universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

„Who is watching us? – Datenschutz als Kunst“

Verfasser

Philipp Fürst

angestrebter akademischer Grad

Magister der Philosophie (Mag. phil.)

Wien, 2008

Studienkennzahl lt. Studienblatt:	A 317 343
Studienrichtung lt. Studienblatt:	Theaterwissenschaft
Betreuer:	Ao. Univ.- Prof. Dr. Rainer Maria Köppl

Vorwort

Wie vielen meiner Kollegen ist auch mir die Themenfindung für meine Diplomarbeit nicht leicht gefallen. Zum einen war es nicht einfach ein Thema zu finden, dass mich selber interessierte und zum anderen musste auch der Professor davon überzeugt werden, ein potentiell interessantes Forschungsgebiet präsentiert zu bekommen. Nach längerem Suchen und diversen Umständlichkeiten fand mein Thema mich: Während des *Ars Electronica Festivals 2007* hatte ich die Möglichkeit die Vortragsreihe der Juristen zum Thema Datenschutz und Überwachung zu hören und auch bei den Diskussionen von Künstlern und Theoretikern dabei zu sein. (An dieser Stelle möchte ich mich bei der netten Dame bedanken die mir auch ohne Anmeldung einen Festival-Pass aushändigte.) Unter den Vortragenden auf diesem Symposium war die Wiener Regisseurin Manu Luksch die ihren Film *Faceless* vorstellte. Im November 2007 bestand auch noch die Möglichkeit einen Workshop mit Manu Luksch in Graz zu besuchen, der sich letztlich als ausschlaggebend erwiesen hatte. Sie hatte sich in London mit dem Datenschutz beschäftigt und wie er auf unseren Alltag einwirkt.

Ich möchte mich an dieser Stelle sehr herzlich bei Manu für die Unterstützung bedanken die sie mir zukommen ließ. Weiters bei Professor Köppl für die Motivation, die hilfreichen Gedankengänge und das Verständnis für die aufgetretene Zeitknappheit.
Ganz besonders möchte ich mich auch bei meinen Eltern, Cilli und Franz bedanken, die mir mein Studium ermöglicht und immer unterstützt haben. Nicht zuletzt möchte ich noch all jenen Danke sagen, die mir als Diskussionspartner, Ideengeber, Motivationsstützen, Korrekturleser und Gleichgesinnte zur Verfügung standen und, wie ich hoffe, es auch gerne getan haben. Herzlichen Dank im Besondern an

Peter, Barbara&Michi, Paul&Francesca, Tom, Lucia, Michi (der große), Babsi, Judith, Lisi, Magdalena, Barbara, Uli.

INHALTSVERZEICHNIS

1. Einführung

Der Begriff der „negativen Utopie“, wie er in George Orwells *1984* beschrieben wird, kommt im heutigen Sprachgebrauch immer öfter vor und das aus gutem Grund. Meldungen von Datenschützern über die gegenwärtige Situation der Überwachung scheinen die Gefahren eines Überwachungsstaates, Kontrollstaates oder Sicherheitsstaates wie ein Damoklesschwert ständig über uns schweben zu lassen: Daten jeglicher Art werden gesammelt, aufgezeichnet, gespeichert und analysiert. In vielen Fällen wissen die Konsumenten das sogar: Kundenkarten werden dazu benutzt, das Einkaufsverhalten auszuwerten, Kundenbewegungen werden über Kameras beobachtet und Online-Geschäfte werden von den Anbietern gespeichert und analysiert, um die Angebote direkt auf den Konsumenten abzustimmen. Dabei werden Daten oft ohne viel nachzudenken weitergegeben. Doch Fragen drängen sich auf: Wer ist im Besitz dieser Informationen? Wie lange werden diese Informationen aufbewahrt? Werden sie gelöscht oder weitergegeben? Gesetze gegen Weitergabe oder langfristige Speicherung dieser Daten existieren zwar, werden aber nur selten exekutiert.

Ein Großteil der Überwachung der heute betrieben wird, besteht darin, Computerdaten zu hacken und Telefone anzuzapfen. Dabei geht es nicht notwendigerweise darum, E-Mails zu lesen oder Gespräche abzuhören (was zu aufwändig und wenig Erfolg versprechend wäre), sondern darum, Kommunikationsprofile der einzelnen Benutzer zu erstellen.[1] Diese sind wesentlich aussagekräftiger als z.B. Transkriptionen von Telefongesprächen. Eigenartig daran ist, dass sich die Menschen gegen diese Art der Überwachung nur wenig wehren und auch nur schwer dazu zu bewegen sind sich diesen Problemen zu stellen.

> „66 Millionen Menschen haben Amazon im letzten Jahr Namen, Adresse, Kreditkarteninfos und persönliche Interessen anvertraut – denn was man anklickt, wird gespeichert. Wer old-school einkauft und in Geschäfte geht, wird dafür gefilmt: In ganz Österreich sind über 250.000 private Überwachungssysteme installiert, die meisten davon illegal. Die Polizei hat trotzdem Zugriff.“[2]

Durch ein Versehen wurden 2006 knapp 23 Millionen Suchanfragen von 650.000 Nutzern eines Internetdienstes publik. Dabei wurde erst wirklich augenscheinlich, wie viele Daten von

[1] Erich Möchel bei der Präsentation von *Faceless* im Top-Kino am 02.05.2008.
Es wurden 2006 allein in Österreich 3.979 Telefonüberwachungen angeordnet. In der Hälfte der Fälle wurde auch der Gesprächsinhalt abgehört. Siehe: Simoner, Michael. „Grobe Mängel beim Lauschangriff“ *Der Standard.* 16. September 2008. S.9.

[2] Reinrecht, Astrid-Marie, Milborn, Corinna in: *Zeitschrift der Österreichischen Liga für Menschenrechte* (ÖLM) Nr. 2/2007: Überwachung. S.15.

Internetanbietern gespeichert werden, und welche Gefahr davon ausgeht, sollten diese Daten in falsche Hände geraten:

> „Da war etwa AOL-Nutzer Nr. 14162375, ein offenbar gehörnter Ehemann. Er suchte nicht nur nach dem Namen seiner Frau, sondern auch nach verschiedenen Methoden, sie zu überwachen – oder gar zu töten. Reportern der New York Times gelang es ohne große Mühe, einige der solchermaßen entblößten Nutzer anhand der ‚anonymen' Suchanfragen namentlich zu identifizieren."[3]

Ein erst kürzlich in den Medien bekannt gewordener Skandal betrifft die Deutsche Telekom: 2006 wurden 17 Millionen Kundendatensätze gestohlen. Diese Datensätze beinhalten Telefonnummern, Handynummern, Adressen, Geburtsdaten und Email-Adressen.[4] Diese Daten wurden bereits im Internet zum Verkauf angeboten.

Benutzer der Internet-Suchmaschine Google sollten sich bewusst sein, dass jede Suchanfrage an die IP-Adresse gespeichert wird. Man hinterlässt „Datenspuren" die durch ihre Zusammenstellung ein komplexes digitales Persönlichkeitsprofil ergeben, bis hin zu: Was wird der Nutzer als nächstes kaufen?

> „Wenn sie wissen was du gestern und vorgestern getan hast, werden sie bald glauben zu wissen, was du morgen tun wirst – und in den meisten Fällen werden sie Recht behalten."[5]

In Kombination mit mehreren Dienstleistungen wie z.B. Google News, Google Finance, Homepage-Generator Google Page Creator, Google Analytics, Google Maps und Google Earth können die Informationen, die mit jeder einzelnen Anfrage eingegeben werden, in Summe ein detailliertes Profil ergeben.

> „Beim Social-Network-Dienst Orkut findet er [der Nutzer; *Anm. Fürst*] neue Freunde. Dazu hinterlegt er ein detailliertes Profil, von der Hautfarbe über den Humor bis hin zur ‚sexuellen Neigung'. So hinterlässt das ganze Leben eine digitale Signatur bei Google."[6]

---

[3] Vašek, Thomas. „Was wird uns da ‚vorgegoogelt'". *P.M*. März 2006. S. 20.
[4] „Telekom-Skandal. Diebe klauten 17 Millionen T-Mobile Kundendatensätze." *Spiegel-Online*. (04.10.2008). (http://www.spiegel.de/wirtschaft/0,1518,581938,00.html) . (05.10.2008).
[5] Programmheft Big Brother Awards 2007.
[6] Bager, Jo. „Der Datenkrake." *c't*. 10/2006. auf: (http://www.heise.de/ct/06/10/168/) (25.09.2008).

Google behauptet Daten anonym zu verwalten und nicht weiterzugeben, benutzt sie aber, um durch Auswertungen von Suchanfragen, Werbungen an den Benutzer anzupassen. Durch das Angebot einer PC-Desktop-Suchmaschine kann Google sogar die privaten Dateien durchforsten und auf den eigenen Servern ablegen. Damit haben auch andere Benutzer Zugriff auf diese Daten.[7]

Die Privatsphäre wird gegen „Komfortgewinn“[8] der Dienste eingetauscht und liefert dem Unternehmen Informationen über unsere „Interessen und Bedürfnisse“.[9] Informationen dieser Art stellen immerhin den wirtschaftlichen Erfolg von Google dar. Als 2006 das US-Justizministerium eine Anfrage stellte, 5.000 Suchanfragen herauszugeben um einen Internet-Filter für Minderjährige zu testen, weigerte sich Google die Daten weiterzugeben und gewann auch vor Gericht. Sollte allerdings eine Anfrage auf Daten in Bezug auf die Terrorabwehr gestellt werden könnte auch Google im Rahmen des *Patriot Act* (Anti-Terror Gesetz der USA) dazu gezwungen werden Informationen Preis zu geben.[10]

> „Das geheime Ziel der Suchmaschinen-Technologie ist es, die wahren Absichten der Nutzer zu erkennen. Das interessiert nicht nur Unternehmen – sondern auch Strafverfolgungsbehörden. Könnte Google vollautomatisch und massenhaft Userprofile erstellen, wäre das für Geheimdienste und Polizei eine Goldgrube: Dann ließen sich potenzielle Terroristen, Amokläufer oder Pädophile anhand ihres ‚Klick-Stroms' routinemäßig aus der Masse der Webnutzer herausfiltern. Die Rasterfahndung im Netz wäre Realität.“[11]

In einem solchen Fall könnten Nutzer voreilig verdächtigt werden: „Für einen Zeithistoriker kann es sogar berufsbedingt notwendig sein, ‚Mein Kampf' zu lesen – voreilige Schlussfolgerungen sollten vermieden werden.“[12]

Ob Google Nutzerprofile wirklich erstellt weiß man nicht, dass es allerdings im Besitz der Möglichkeiten ist, wird nicht angezweifelt.[13]

---

[7] Ebenda
[8] Nentwich/Peissl. In Reiter/Wittmann-Tiwald. 2008 S. 39.
[9] Vašek, Thomas. „Was wird uns da ‚vorgegoogelt'“. *P.M*. März 2006.
[10] Bager. 10/2006.
[11] Vašek. 2006. S. 22.
[12] Peissl, Walter. „Wie (Video-)Überwachung unser Leben verändert.“ S. 136. in: Reiter, Michael / Wittmann-Tiwald, Maria. (Hg.). Goodbye Privacy – Grundrechte in der digitalen Welt. Linde. Wien: 2007. S. 133-139.
[13] Siehe: Vašek. 2006. S.22.

Google wird als die "größte und mächtigste Detektivagentur der Welt"[14], und in Verbindung damit, als „größtes Datenschutzproblem in der Geschichte der Menschheit"[15] bezeichnet. Durch die Unmengen an Daten, die gesammelt werden, besitzt Google sogar die Macht wirtschaftliche Verhältnisse zu beeinflussen.


Problem Datensicherheit

„Google wird wie ein guter Freund"

Die Internet-Suchmaschine wolle User und deren Bedürfnisse so genau kennenlernen wie ein Freund, so die Forschungs-Chefin des Konzerns.

Abb.1: Google – dein „Freund".

Sei es durch Zensur – Google beugte sich der chinesischen Zensur (Nutzer bekommen auf ihre Suchanfragen nur Ergebnisse die vom kommunistischen Regime gebilligt werden) – oder durch Änderungen des Such-Algorithmus die einen Geschäftsmann deshalb bankrott gehen ließ, weil er in der Google-Trefferliste nach hinten rutsche.[16]

Ein weiteres beliebtes Angebot ist Google Earth. Dieses Programm stellt Satellitenbilder der Erde online.[17] Die Qualität der Bilder ist mittlerweile so gut, dass man sich Bilder des eigenen Hauses ansehen und feststellen kann welches Auto vor der Tür steht, oder welche Blumen gerade blühen.

Zu einer heiklen Situation kam es, als sich das Britische Militär beschwerte: Bei irakischen Terroristen wurden Bilder gefunden die von Google Earth stammten, und britische Militärstützpunkte in der Nähe von Basra als Angriffsziel zeigten. Google musste dem Druck der Militärs nachgeben und daraufhin die aktuellen gegen alte Bilder austauschen.[18]

Eine Erweiterung von Google Earth, Google Street View, wirft in der Datenschutzfrage mittlerweile ähnlich hohe Wellen: Für Google Street View fahren Autos, die mit einer 360° Kamera bestückt sind, durch größere Städte. Elf Linsen fotografieren in einem 2 Sekunden-Intervall die Umgebung. Dadurch entsteht im Programm Street View die Möglichkeit jederzeit einen 360° Blick in den abfotografierten Städten zu unternehmen. Das Problem

[14] Siehe: Ebenda. S. 17.
[15] Edward Felten (Princeton University) in: Vašek. 2006. S. 18.
[16] Siehe: Ebenda. S22.
[17] „In 450 Kilometer Höhe kreist der Satellit QuickBird 15-mal täglich um unseren Globus. Pausenlos nimmt er dabei 330 Kilometer lange und 16,5 Kilometer breite Streifen der Erdoberfläche auf. Per GPS wird die geografische Lage der Streifen auf der Erdoberfläche bestimmt. Besonders wichtige Orte werden zusätzlich per Flugzeug aufgenommen." Ebenda. S. 21.
[18] Rötzer, Florian. „Bildbereinigung durch Google Earth". *Telepolis*. (21.07.2007) (http://www.heise.de/tp/r4/artikel/24/24483/1.html) (14.09.2008).

dabei ist, dass der Alltag der Menschen mitdokumentiert wurde: Menschen beim Nasenbohren, beim Urinieren an einen Zaun oder beim Verlassen eines Sexshops (Google liefert zu diesem Shop auch noch zusätzliche Information der Angeboten– von „Lap Dancers" bis zu „Non-Stop Bühnenshows").[19]

Im Internet haben sich schon Communities gefunden, die Bilder von „Merkwürdigkeiten, Peinlichkeiten oder banale[n] Alltagssituationen sammeln."[20] Eine dieser Seiten nennt sich StreetViewFun.com. Die Bilder tragen Untertitel wie „Cutie Jogger with Dog", „Hot Chick, Robot Walk" oder „Timber Creek High School Cheerleader"[21] und lassen Vermutungen zu, welchen Zweck diese Seiten erfüllen, bzw. welche Möglichkeiten Googles Street View zulässt. Andere Blogs verbinden die Fotografien mit Geschichten die völlig aus der Luft gegriffen werden: So können auch Passanten, die z.B. nur an einem Sex-Shop vorbeigehen mittels eines Untertitels zu „Stammkunden" werden. Ob es dabei die Betroffenen in peinliche Situationen bringt ist den Usern meistens egal.

> „Unzähligen Blogs und Webseiten ist's egal. Sie tauschen und verlinken seit Wochen immer mehr Beutestücke. Und so werden aus oft zweideutigen, zufällig aufgenommenen Straßenszenen mithilfe süffisant-suggestiver Kommentare kleine Web-Kurzgeschichten."[22]

In Europa, so Struan Robertson (*Anwalt, IT-Rechtler, GB*), dürfte Googles Street View allerdings illegal sein. Für ihn bedeutet es nichts anderes als eine nicht angekündigte bzw. nicht beschilderte Videoüberwachung.[23]

Sogar in den USA wurde Google bereits wegen Verletzung der Privatsphäre verklagt: Bilder des Hauses eines Paares fanden sich auf Google Street View wieder, obwohl das Haus abseits der öffentlichen Strasse steht und nur über einen Privatweg zu erreichen ist. Google konterte damit, dass Satelliten-Technologie mittlerweile so weit fortgeschritten sei, und absolute Privatsphäre eigentlich nicht mehr existiere.

> „Google's claims to be legally allowed to photograph on private roads stems from its assertion that privacy no longer exists in this age of satellite and aerial imagery."[24]

---

[19] Netzwelt. Online für IT & Consumer Electronics. Woods, Patrick. „Google Street View: Stadtrundfahrt am Bildschirm." (20.06.2007) (http://www.netzwelt.de/news/75729-google-street-view-stadtrundfahrt-am.html) (20.09.2008).
[20] Ebenda.
[21] StreetViewFun. (www.streetviewfun.com) (11.09.2008).
[22] Schmitt, Stefan. „Paradies der Gaffer und Spanner". *Spiegel-Online*. (10.06.2007). (http://www.spiegel.de/netzwelt/web/0,1518,487708,00.html). (15.09.2008).
[23] Robertson, Struan. „Google's Street View could be unlawful in Europe". *The Register-Online*. (05.06.2007). (http://www.theregister.co.uk/2007/06/05/google_street_view_legality_in_europe/). (15.09.2008).

Vint Cerf, der „Erfinder des Internets" und Google-Mitarbeiter, wird in demselben Artikel zitiert: „There isn't any privacy, get over it."[25]

Die einfache Erhältlichkeit von Informationen in unserer Zeit erhöht die Gefahr des Missbrauchs. Darunter fällt vor allem die Zusammenlegung von mehreren Registern. Datensammlungen und Register beinhalten ein Gefahrenpotential das allerdings Problem ist: In den Niederlanden wurde in den 20er und 30er Jahren ein „umfassendes Melderegister" erstellt, das u.a. das Religionsbekenntnis beinhaltete. Nach dem Einmarsch der Nazis wurde dieses Registers benutzt um Juden zu verfolgen.[26] Je mehr Informationen gesammelt werden, je spezifischer sie sind, desto größer ist auch die Gefahr des Missbrauchs, sollten diese Daten in falsche Hände kommen.
Die Zusammenlegung von Registern führt zu einer Gefährdung der Privatsphäre. Eine Effizienzsteigerung lässt sich zwar nicht leugnen, doch „unter Umständen haben Personen Einblicke in die personenbezogenen Daten [...], die diese Daten gar nicht benötigen oder die sie missbräuchlich verwenden könnten;"[27] Dieser Missbrauch wird als „function creep" bezeichnet:

> „Darunter versteht man jenen Prozess, bei dem ein Gegenstand, ein System oder eine Prozedur, die für einen bestimmten Zweck geschaffen wurde, für etwas ganz anderes, niemals Intendiertes, zweckentfremdet verwendet wird."[28]

Eines der großen Probleme, die damit verbunden sind, ist, dass das Internet nicht vergisst! Viktor Mayer-Schönberger (*Professor an der John F. Kennedy School of Government, Harvard University*) hat in seinem Vortrag während des *Good-bye Privacy Symposiums 2007* ein treffendes Beispiel gebracht: Die Lehramtsstudentin Stacy Snyder stellte ein Foto von sich, als Pirat verkleidet, auf ihre MySpace Seite mit dem Untertitel: „Drunken Pirate". Der Dekan der Universität verweigerte ihr daraufhin den Abschluss mit der Begründung, dass ein

---

[24] Musil, Steven. „Google finds no privacy on private roads". *News – Digital Media*. (24.08.2008). (http://news.cnet.com/8301-1023_3-10024294.html?tag=mncol). (20.09.2008).
[25] Cerf, Vint (Internet-Pionier und Mitarbeiter von Google) in: Ebenda.
[26] Mayer-Schönberger, Viktor. „Nützliches Vergessen" (S. 7-16). Reiter/Wittmann-Tiwald. 2008. S. 12.
[27] Nentwich, Michael / Peissl, Walter. Gesellschaftliche Risiken von öffentlichen Registern. In: Reiter/Wittmann-Tiwald. 2008. S. 41.
[28] Peissl, Walter. Technische Aspekte der Videoüberwachung. S. 134f. in: Reiter/Wittmann-Tiwald (Hg.). Goodbye Privacy – Grundrechte in der digitalen Welt. Linde. Wien: 2007. S. 133-139.

solches „Verhalten einer Lehrerin nicht würdig sei.“[29] Auch nachdem sie das Foto wieder von ihrer Seite genommen hatte, konnte sie nicht verhindern, dass dieses Bild bereits im Internet „archiviert und katalogisiert und über Google und Internet Archive weiterhin weltweit für jeden zugänglich war. So sehr Stacy ein Vergessen wollte, so wenig ließ es das Netz zu.“[30]

Dr. Hans Zeger (*Arge-Daten*[31]) formuliert diesen Zustand so: Durch diese Datensammlungen könnten sich „Parallelexistenzen“[32] bilden, von denen die realen Personen nichts wissen (anders als bei SecondLife, studivz, facebook, wo die Informationen selbst weitergegeben werden und man sich dessen auch bewusst ist). In den meisten Fällen weiß der Benutzer allerdings nicht, ob und an wen Daten weitergegeben werden oder ob eine Auswertung vorgenommen wird. Auf derartige Informationen kann aber zugegriffen werden, um „einen Vorwurf zu formulieren.“[33]

> „Wenige wissen dabei über die Konsequenzen: Hier kann jedes Wort, jedes Bild auch gegen die arglosen Mitspieler selbst verwendet, ge-wendet[!] werden.“[34]

Mit der persönlichen Datenfreigabe im Internet scheint man bisher noch sehr freizügig umgegangen zu sein aber was passiert, wenn diese Daten mit Bildern von Videoüberwachungskameras vernetzt werden? Die Kamera ist mehr denn je das Symbol der Überwachung. Warum? Wahrscheinlich weil dieses Kamera-Überwachungsnetzwerk offensichtlicher zu Tage tritt. Vielleicht weil die Angst vor dem Beobachtet-Werden, der körperlichen Präsenz der Überwachung ein unangenehmes Gefühl ist.

> „Kameras sind natürlich so was wie die Ikone der Überwachung, sind sichtbar und ragen in den öffentlichen Raum rein.“[35]

Die Sichtbarkeit der Methode ist es also, die uns verstärkt die Überwachung spüren lässt. Überwachung von E-Mails oder Telefonen wird in den meisten Fällen im täglichen Leben

---

[29] Mayer-Schönberger. in: Reiter/Wittmann-Tiwald. 2008. S. 9. Siehe auch: Brandstetter, Sabine. „Wie Myspace & Co. die Karriere gefährden“. *Die Presse*. (02.20.2008). (http://diepresse.com/home/bildung/unilive/416782/index.do?_vl_backlink=/home/bildung/unilive/index.do) (02.20.2008).
[30] Mayer-Schönberger. in: Reiter/Wittmann-Tiwald. 2008. S. 9
[31] Österreichischer Verein für Datenschutz.
[32] Manu Luksch in: Dax, Patrick. 2007.
[33] Ebenda.
[34] Reiter/Wittmann-Tiwald. Vorwort. in: Reiter/Wittmann-Tiwald. 2008. S.5.
[35] Zurawski, Nils in: Die sichere Stadt (Video) (http://www.zeit.de/video/player?videoID=200707185ecff9) (10.12.2007).

nicht spürbar, ist unsichtbar. Aus diesem Grund stehen Kameras in Diskussionen sehr oft im Vordergrund.

Es mag daran liegen, dass es sich in den meisten Fällen (mittlerweile) um offensichtlich und gut sichtbar positionierte Kameras handelt bzw. „Warnungen" an Eingängen zu überwachten Räumlichkeiten angebracht sind. Diese Maßnahmen, die ihrer Bestimmung nach präventiv zu sein scheinen, sollen illegale Handlungen abschrecken und soziale Störfelder (Vandalismus, Drogendealer, Bettler, Obdachlose, Randgruppen u.ä.) ausschließen. Und trotzdem: Wirken sie noch abschreckend oder haben wir uns bereits so an die Situation gewöhnt, dass wir sie nicht mehr bemerken?

Abb. 2: *Dilbert*: „Gewöhnungseffekt" von Videoüberwachung.

Heute sind sogar fliegende Kameras keine Unmöglichkeit mehr: in England werden mittlerweile „Überwachungsdrohnen eingesetzt, die über sensiblen Stadtteilen kreisen und ‚asoziale Elemente' verfolgen."[36] Die Entwicklung solcher Drohnen wurde auf dem *Chaos-Communication-Camp 2007* (CCC) vorgestellt. Dabei handelt es sich z.T. um umgebaute Modelhubschrauber. Ausgerüstet mit einem GPS-Sender und einer Kamera können dabei Gelände, sowie Stadtgebiete überflogen und Daten weitergeleitet werden. Den Hackern des CCC-Treffen ist allerdings klar mit welchem „Potential" sie hantieren:

> „Man sei sich durchaus bewusst, dass hier im staatlichen wie privaten Bereich eine technische Entwicklung mit Bedrohungspotenzial auf die Gesellschaft zukomme, sagte CCC-Mann Ron zu ORF.at."[37]

[36] Reinrecht, Astrid-Marie/Milborn, Corinna in: Zeitschrift der Österreichischen Liga für Menschenrechte. Überwachung. 02/2007. Druckerei Berger: Wien, 2007. S.15.
[37] Moechl, Erich. „Videodrohnen bald für jedermann". *ORF.at* (13.08.07) (http://futurezone.orf.at/produkte/stories/214259/) (05.09.2008).

Abb.3: Microdrone ausgestattet mit Kamera

Zwischen 2001 und 2004 wurde das Projekt URBANEYE mit Unterstützung der Europäischen Kommission in sieben europäischen Ländern durchgeführt: Österreich, Dänemark, Deutschland, Großbritannien, Ungarn, Norwegen und Spanien. Der Schwerpunkt der Forschung bestand in der Verbreitung von Videoüberwachung und ihrer Handhabung. Das Forschungsteam wurde zu diesem Zweck nicht nur von einem kriminalistischen Standpunkt aus zusammengestellt. Mit dieser Untersuchung sollte ein breites Spektrum abgedeckt werden, das sich zunehmend mit der Stadt, Stadtplanung und den sozialen Aspekten die mit der Überwachung einhergehen, beschäftigen sollte. Die Experten wurden aus den folgenden verschiedenen wissenschaftlichen Sparten rekrutiert: Kriminologie, Philosophie Politikwissenschaft, Soziologie und Stadtplanung.[38]

Im Zeitraum der Untersuchungen des URBANEYE-Projekts wurde die Bedeutung von CCTV[39] in Österreich als „more or less a non-issue“[40] eingeschätzt. Mittlerweile hat sich diese Situation auch in Österreich verändert. War es vor vier Jahren in Österreich noch ein Thema von geringer Aufmerksamkeit, bringt sich die Videoüberwachung auch hierzulande wieder in die Sicherheitsdiskussion ein. Damit sollte eigentlich eine kritische Auseinandersetzung verbunden sein, in der Bevölkerung aber auch beim Gesetzgeber der in vielen Fällen der Technik und Realität nachhinkt. Eine derartig rasche Verbreitung von Videoüberwachung hat sich vor allem aufgrund fehlender gesetzlicher Regelungen und Einschränkungen durchsetzen können.[41]

[38] Siehe: Hempel, Leon/Töpfer, Eric. „CCTV in Europe.“ (August 2004) URBANEYE (http://www.urbaneye.net/results/results.htm) (20.05.2008). S. 1.
[39] CCTV: Closed Circuit Television ist die englische Version der Videoüberwachung.
[40] Ebenda. S. 4.
[41] Siehe: Hempel/Töpfer. 2004. S. 22.

In Großbritannien sind Verbreitung und Einsatz von Videoüberwachung mit 40% erwartungsgemäß am größten. Der Einsatz von Videoüberwachung ist in Österreich, im Vergleich zu den anderen von URBANEYE untersuchten Ländern, mit 18% am geringsten.[42]

Die totale Überwachung – ist sie noch eine Utopie? Während der *Ars Electronica 2007* zum Thema „Good Bye Privacy" stellt die Wiener Filmemacherin Manu Luksch ihren Film *Faceless*[43] vor. Der Film wurde ausschließlich aus CCTV-Material aus London zusammengestellt. Aufgrund des *Data Protection Act 1998* in Großbritannien hat jeder das Recht in Aufnahmen von Überwachungskameras für den Zeitraum, in dem er gefilmt worden ist, nicht nur Einsicht zu nehmen, sondern auch eine Kopie davon erstellen zu lassen.

> „The subject access request letter is to state the place and time of the recording and include a picture of the protagonist, wearing the same clothes if possible, and a cheque for £10 (the maximum fee chargeable)."[44]

Manu Lukschs Arbeitsweise wurde von folgender Fragestellung angeregt: Warum überhaupt in London eine Kamera auspacken, wenn doch über 500.000 CCTV-Kameras installiert sind? Die Idee zum Science-Fiction-Film kam schließlich mit dem Betrachten der ersten angeforderten Bänder. Um die Privatsphäre der anderen Personen zu wahren wurden sämtliche Gesichter von den Betreiberfirmen unkenntlich gemacht (außer das Gesicht jener Person, die die Bänder anfordert). Darauf basiert auch die Geschichte: Die Protagonistin (Manu Luksch) entdeckt eines Tages, dass sie als einzige Person ein Gesicht besitzt.[45]
Diese „gesichtslose Welt" hat keine Vergangenheit und keine Zukunft, sie besteht nur mehr aus *RealTime*, einer Zeit durch die alle und alles miteinander gleichgeschaltet wird:

> „The pulse of real time orients the life of every citizen. Eating. Resting. Going to work. Getting married. Every act is tied to real time. And every act leaves a trace of data. A footprint in the snow of noise. The new machine monitors these data traces. Making sure that all is well."[46]

---

[42] Siehe: Hempel/Töpfer. 2004. S. 4.
[43] *Faceless.* R&D: Manu Luksch. DVD. Amour fou Filmproduktion. 2007. 50 min.
[44] Luksch, Manu. "Manifesto for CCTV Filmmakers" *AmbientTV.net* (http://www.ambienttv.net/content/?q=dpamanifesto) (10.10.2007).
[45] „In an eerily familiar city, a calendar reform has dispensed with the past and the future, leaving citizens faceless, without memory or anticipation. Unimaginable happiness abounds - until a woman recovers her face...". Luksch/Patel. „Faceless: Chasing the Data Shadow." *AmbientTV.* (http://www.ambienttv.net/2007/faceless/chasingthedatashadow2007.pdf) (20.11.2007). S. 74.
[46] *Faceless* (2007): D/R.: Manu Luksch.

East End in London machte 2006 mit einer Überwachungsmethode der besonderen Art und Weise auf sich aufmerksam. Der Wohlfahrtsverband Shoreditch Trust ließ die durch CCTV überwachte Gegend nicht nur von der Polizei beobachten sondern ließ die Überwachung auch von den Bewohnern der Gegend auf ihren TV-Geräten mitverfolgen. Die Initiatoren sprachen von einem „community safety channel".[47] Gegner befürchteten, dass es zu Akten von Selbstjustiz kommen könnte.

Wenn man die (Video-)Überwachung als Gefahr und Einschränkung der persönlichen Freiheit und Privatsphäre sieht, ist es doch paradox zu wissen, dass Hunderttausende von Menschen täglich persönliche Videos ins Internet stellen. Es scheint ein Bedürfnis zu sein nicht nur zu sehen und zu beobachten sondern auch gesehen zu werden. So kann sich auch die Angst vor dem Beobachtet-Werden in die Angst vor dem Nicht-Gesehen-Werden wandeln. Die Kamera und das Bild werden zum Beweis für die Existenz.
Es sollte hierbei aber auch darauf hingewiesen werden, dass sich diese Art von Video im Gegensatz zu den Überwachungskameras auf öffentlichen Plätzen befindet. Nicht nur die Funktion sondern auch die Veröffentlichung des Materials bzw. die Kontrolle darüber stellen gänzlich unterschiedlichen Bereiche dar.
Faceless fungiert als Kunstobjekt, in dem die dominante Allgegenwärtigkeit von Überwachungskameras zur Schau gestellt wird. Es ist ein Versuch, die Bevölkerung darauf hinzuweisen, dass sie – falls sie es vergessen oder verdrängt haben sollte – überwacht wird, auf Schritt und Tritt.

Die Arbeit beginnt mit einer eingehenden Auseinandersetzung von Videoüberwachung und den in Österreich geltenden Gesetzen, mit der Erklärung von grundlegenden Begriffen, sowie der Beschreibung der zuständigen Behörde, der Datenschutzkommission. Diese trifft Entscheidungen über den Einsatz von Videoüberwachungsmaßnahmen, ob und in welcher Form sie angewandt werden dürfen. In ihren Kompetenzbereich fallen z.B. der Einsatz von Kameras bei den ÖBB und den Wiener Linien.
Der zweite Teil beschreibt die Arbeitsweise der Regisseurin Manu Luksch und im Besonderen ihren Film *Faceless*, wie er zustande gekommen ist und auf welchen „Spielregeln" er basiert. Dazu ist es auch notwendig kurz auf das britische Datenschutzgesetz einzugehen. Die Situation die Manu Luksch hervorheben will, nämlich die

[47] Weaver, Matt. „Residents given access to live CCTV footage" (11.1.2006) *The Guardian* (http://www.guardian.co.uk/uk_news/story/0,,1684043,00.html) (11.10.2007).

Überwachungssituation in der wir uns auf Schritt und Tritt befinden, wird durch zwei weitere Beispiele gezeigt: Die Mockumentary Citizen Cam beschreibt 1999 eine fiktive Situation der Videoüberwachung, die 2006 von einer Wohnbaugesellschaft realisiert wurde – einen TV-Kanal der Bilder der Überwachungskameras zeigt, damit die Bevölkerung mithelfen kann, die Überwachung der Polizei selbst fortzusetzen.
Der dritte Teil der Arbeit beschäftigt sich mit den Auswirkungen der Videoüberwachung. Normierung und soziale Kontrolle sind bewiesenermaßen Produkte der Überwachung. Der Mensch, das Individuum passt sich der Norm an um nicht aufzufallen, ist nicht mehr er selbst. Er verliert seine Individualität.

Anmerkung:
Zum Zeitpunkt der Entstehung dieser Arbeit wurde in Österreich das Datenschutzgesetz 2000 (DSG) zum Thema Videoüberwachung novelliert. Nachdem sich dieses Gesetz noch im Zustand der Begutachtung befindet, findet es in dieser Arbeit keine Berücksichtigung.

Für weitere Informationen zum Film, besuchen sie bitte die Webseiten www.amourfou.at und www.ambienttv.net.

2. Gesetzliche Grundlagen des Datenschutzes in Österreich

Die Regisseurin Manu Luksch hat sich mit der britischen Rechtslage (*Data Protection Act 1998*) auseinandergesetzt, um eine Basis für sich und ihr *CCTV-Filmmaker's Manifesto*[48] zu schaffen. Auf den folgenden Seiten wird versucht, das österreichische Gesetz bezüglich der rechtlichen Grundlagen von Videoüberwachung zu untersuchen. Sind wir auf dem Weg zum Überwachungsstaat? Wer überwacht wen und wo? Warum wird überwacht?
Das Problem ist, dass die Videoüberwachung im Datenschutzgesetz (DSG) 2000 für privaten Bereich nicht explizit geregelt ist. Und doch ist die Videoüberwachung ein Eindringen in die Privatsphäre. Dr. Gregor König (*stellvertretender Leiter der Datenschutzkommission*) nennt die im DSG 2000 verabsäumte „Modernisierung" und Anpassung an die Zeit *Technologieneutralität*:

> „Während letztere [herkömmliche Datenermittlung und Datenspeicherung; *Anm. Fürst*] bloß einzelne Aspekte einer Person, meist geordnet in Datenfeldern, zeigt, erfasst das Videobild den Menschen als Ganzes, macht sein Verhalten umfassend transparent und sichtbar."[49]

Mit dem Beitritt zum Europarat 1956 und der Ratifizierung der Europäischen Menschenrechtskonvention (EMRK) am 16. Dezember 1957 ist die EMRK in Österreich im Verfassungsrang. Sie ist in diesem Zusammenhang insofern wichtig, als sie die Grundlage für Gesetze bildet, die vor allem die Wahrung der Privatsphäre festlegen. Sowohl in der EU-Richtlinie 95 als auch im DSG 2000 wird auf sie verwiesen. Im Folgenden wird auch noch das Sicherheitspolizeigesetz (SPG) angesprochen werden. Dieses klärt die Kompetenz der Überwachung durch die Polizei und stellt auch die Regeln für den Einsatz von Lauschangriffen dar. Das Urheberrechtsgesetz wird hier deswegen angeführt, da es Regeln beinhaltet die auch den Bildnisschutz betreffen. Das Hauptaugenmerk wird sich aber auf das österreichische Datenschutzgesetz richten.

[48] Siehe: Anhang.
[49] König, Gregor: „Videoüberwachung und Datenschutz – Ein Kräftemessen" in: Jahnel: *Aktuelle Fragen des Datenschutzrechts*. Facultas, Wien: 2007. S. 109.

2.1. Europäische Menschenrechtskonvention (EMRK):

> Artikel 8 der EMRK
> „Gebot der Achtung der Privatsphäre
> (1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.
> (2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutze der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.“[50]

Im Absatz 1 wird festgehalten, dass jeder das Recht auf Privatsphäre (siehe: § 1 Abs. 1 DSG 2000) besitzt. Die Ausnahmen sind in Absatz 2 der EMRK (siehe: § 1 Abs. 2 DSG 2000) formuliert, in denen das Recht in die Privatsphäre von Betroffenen einzugreifen, eine rechtlichte Basis bekommt. Er regelt somit u.a. jene Situationen, in denen eine Datenanwendung (jede Art der Handhabung von Daten)[51] erfolgen darf.

2.2. EU-Richtlinie 95

Dem DSG 2000 liegt vor allem der Wunsch der EU zugrunde, einheitliche Datenschutzgesetze für die Mitgliedsstaaten zu schaffen. Diese Angleichung mündete in der EU-Richtlinie 95. Sie sollte eine Erleichterung für die EU-Staaten mit sich bringen:

> „Das erklärte Ziel des europäischen Gesetzgebers ist ein möglichst ungehinderter Datenfluß personenbezogener Daten innerhalb der Europäischen Union. Um dies zu erreichen, ohne dass Bürger in Ländern mit hohem Datenschutzniveau auf ihre Rechte verzichten müssen oder es zu einem Datentransfer in Länder mit geringem Schutzniveau kommt, wurde eine DS-RL konzipiert, die den Datenschutz auf hohem Niveau innerhalb der Europäischen Union harmonisiert und gleichzeitig den Export

[50] Internet und Recht. „EMRK”. (www.internet4jurists.at/gesetze/emrk.htm) (05.04.2008).
[51] Unter einer Datenanwendung iSd §4 DSG2000 ist jede „Art der Handhabung von Daten“ zu verstehen, d.h. Verarbeiten und Übermitteln, „Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten.“ (siehe §4 DSG 2000)

personenbezogener Daten aus der Europäischen Union besonders strengen Bedingungen unterwirft."[52]

Diese Richtlinie wurde 1995 verabschiedet, um die Datenschutzgesetze der einzelnen Mitgliedsstaaten der EU zu erneuern und auf einen gemeinsamen Standard zu bringen. Das bis dahin in Österreich gültige DSG war aus dem Jahr 1978, und wurde vom DSG 2000 abgelöst, das etliche Neuerungen beinhaltet, die vor allem ein Augenmerk auf den technischen Fortschritt legten. Die Datenschutznormen wie sie jetzt ausgeübt werden, haben auch eine Verstärkung der Betroffenenrechte mit sich gebracht (*Recht auf Löschung, Richtigstellung, und Beschwerde* (§§ 26 und 31)).

In den meisten Fällen wurde auf die EU-RL 95 (die in Abs. 1 direkt auf die EMRK als Stütze verweist) zurückgegriffen, das *Recht auf Sicherheit* wie es in Artikel 5 EMRK festgehalten ist, wurde jedoch nicht in das DSG 2000 übernommen. Das ist ein wesentlicher Punkt, da diese Möglichkeit somit nicht als Begründung für eine Überwachung und Registrierung einer Datenanwendung angegeben werden kann.

Die Datenschutzbeauftragte der Regierung, Dr. Waltraut Kotschy (1994), lehnte eine Erneuerung des Datenschutzes in Österreich ab.[53] Die EU-Richtlinie 95 verlangte aber eine Umsetzung bis zum 24.10.1998.[54] Nach Fertigstellung und Inkraftsetzung des DSG 2000 ist „ein im Kern völlig neues DSG"[55] entstanden, dass es trotzdem verabsäumt hat wesentliche technische Neuerungen in den Gesetzestext aufzunehmen.

2.3. Allgemeines Bürgerliches Gesetzbuch (ABGB)

Das ABGB konstituiert die allererste Grundlage zum Datenschutz: Persönlichkeitsrechte sind absolute Rechte und daher auch schützenswürdig.[56]

§ 16 ABGB

> „§ 16. Jeder Mensch hat angeborne[!], schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten. Sclaverey[!] oder Leibeigenschaft,

[52] Mayer-Schönberger. *Das Datenschutzgesetz 2000*, Linde: Wien, 1999. S. 14
[53] Siehe: Ebenda. S. 11. Die Beauftragte für Datenschutz in Österreich (Waltraut Kotschy) meinte, Österreich sei eine Datenschutzhochburg und brauche kein neues Datenschutzgesetz (1994).
[54] Siehe: Ebenda. S. 11
[55] Ebenda. S. 12
[56] Dittrich, Robert. *Manz Taschenbuchkommentar* ABGB, Manz: Wien, 2005. S. 12.

> und die Ausübung einer darauf sich beziehenden Macht, wird in diesen Ländern nicht gestattet.“[57]

Das Datenschutzrecht hat seinen Ursprung im ABGB. In den Erläuterungen zum § 16 ABGB steht folgendes:

> „ISd §16 angeboren ist das Recht auf Wahrung der Geheimsphäre. Es schützt sowohl gegen das Eindringen in die Privatsphäre der Person als auch gegen die Verbreitung rechtmäßig erlangter Informationen aus der u[nd] über die Geheimsphäre.“[58]

Der Oberste Gerichtshof (OGH) kommt in einem später angeführten Beispiel auf den § 16 ABGB zurück um einen Rechtsstreit wegen Videoüberwachung in einem Mietshaus beizulegen.

2.4. Sicherheitspolizeigesetz (SPG)

Die Zulässigkeit von Videoüberwachung im sicherheitspolizeilichen Bereich wird im SPG geregelt, genauer gesagt im § 54 Abs. 6 und 7 SPG.

> „§ 54 SPG Abs. 6:
> (6) Ist auf Grund bestimmter Tatsachen, insbesondere wegen vorangegangener gefährlicher Angriffe, zu befürchten, dass es an öffentlichen Orten (§ 27 Abs. 2)[59] zu gefährlichen Angriffen gegen Leben, Gesundheit oder Eigentum von Menschen kommen wird, dürfen die Sicherheitsbehörden zur Vorbeugung solcher Angriffe personenbezogene Daten Anwesender mit Bild- und Tonaufzeichnungsgeräten ermitteln. Sie haben dies jedoch zuvor auf solche Weise anzukündigen, dass es einem möglichst weiten Kreis potentieller Betroffener bekannt wird.“[60]

Der Hinweis auf Ankündigung der Überwachung soll zusätzlich darauf einwirken, dass das gelindeste Mittel angewandt wird. Eingriffe der Sicherheitspolizei müssen außerdem der *Verhältnismäßigkeit* (§ 54 Abs. 4a SPG) entsprechen. Das bedeutet, dass Bild- und

[57] Internet und Recht. „ABGB“. (http://www.internet4jurists.at/ges/abgb.htm) (05.04.2008).
[58] Rummel, Peter. *Kommentar zum Allgemeinen Bürgerlichen Gesetzbuch*. Manzsche Verlags-und Universitätsbuchhandlung: Wien, 2000. S. 61.
[59] § 27. (1) Den Sicherheitsbehörden obliegt die Aufrechterhaltung der Ordnung an öffentlichen Orten. Hiebei haben sie auf das Interesse des Einzelnen, seine Grund- und Freiheitsrechte ungehindert auszuüben, besonders Bedacht zu nehmen.
(2) Öffentliche Orte sind solche, die von einem nicht von vornherein bestimmten Personenkreis betreten werden können.
[60] Internet und Recht. „SPG“. (http://www.internet4jurists.at/ges/spg2008.htm) (05.04.2008).

Tonaufzeichnungen nur zulässig sind, „wenn die Begehung von mit beträchtlicher Strafe bedrohten Handlungen (§ 17) zu erwarten ist." Das SPG betrifft das DSG 2000 insofern, als es die Überwachung im öffentlichen Raum abdeckt, der für private Überwachung rechtlich nicht zulässig ist.

Das SPG wurde vor allem mit einer groß angelegten Polizeiaktion im Jahr 1999 in Verbindung gebracht. Es war dies der erste „große Lauschangriff" der Polizei der durch das SPG erst möglich gemacht wurde. Es musste „zwangsläufig" ein Erfolg sein um die Notwendigkeit und Wirkung eines derartig starken Eingriffs in die Privatsphäre auch unter Beweis zu stellen. Dieser Lauschangriff wurde unter dem Namen „Operation Spring" bekannt.
Angelika Schuster und Tristan Sindelgruber hinterfragen in dem gleichnamigen Film *Operation Spring*[61] die Methoden der Polizei während dieser Aktion. Der Prozess fand gegen mehr als 100 angeklagte Nigerianer statt. Die Anklage wegen Drogenhandel wurde mit der Begründung geführt, „unbekannte Mengen an unbekannten Orten an unbekannte Menschen" verkauft zu haben.[62] Während der Prozesse kamen Zweifel an der Rechtmäßigkeit der Anklagen auf.

> „Schon bald kam der Verdacht einer Vergeltungsaktion der Polizei auf. Mehrere der verhafteten Personen waren an Demonstrationen nach dem Tod des Schubhäftlings Marcus Omofuma beteiligt. War diese bildliche Übereinstimmung eindeutig, so bedurfte sie auf dem Beweismaterial von geringer Bildqualität der Interpretation."[63]

Bild- und Tonträger, die von sehr schlechter Qualität waren wurden als eindeutige Beweismittel vorgelegt. Ein gerichtlich nicht vereidigter Übersetzer entschied selbst über „wichtige Textpassagen" und ordnete auch die Stimmen den einzelnen Personen zu.
An diesem Beispiel ist zu erahnen wie die Vernetzung von Datenbanken funktionieren kann: Bilder von z.B. Demonstrationen werden in Verbindung mit anderen Ermittlungen in Verbindung gebracht, um die Beweislast zu erhöhen und den Beschuldigten zu misskreditieren.

[61] *Operation Spring*. R: Angelika Schuster / Tristan Sindelgruber. Schnittpunkt Filmproduktion. DVD-Der Standard-Edition. 2005. Österreich. 94.min.
[62] Siehe: Kamalzadeh, Dominik. „Plädoyer für den Zweifel." *Der Standard.* 24.09.2005.
[63] Ebenda.

Die Polizei konnte sich der Blöße aber nicht hingeben, durch den Lauschangriff kein brauchbares Material erlangt zu haben. Sie musste mit diesem Lauschangriff ein Exempel statuieren das diesen, und weitere Eingriffe dieser Art rechtfertigen konnte.

2.5. Urheberrechtsgesetz (UrhG)

Im Urheberrechtsgesetz deckt der § 78 den Bereich der Videoüberwachung ab:

> „Bildnisse von Personen dürfen weder öffentlich ausgestellt noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden, wenn dadurch berechtigte Interessen des Abgebildeten [...] verletzt würden.“[64]

Die „Verletzung berechtigter Interessen“ findet nicht statt, da diese Bilder im Normalfall nur einem beschränkten Personenkreis zugänglich sind. Weiters sind sie nicht als „Veröffentlichung der Bildnisse Dritter anzusehen“.[65] Der § 78 UrhG ist also im Bereich des Bildnisschutzes *nicht* anzuwenden.

In der Literatur wird das Urheberrechtsgesetz selten in Verbindung mit dem Datenschutz verwendet. Ein Problem ortet Dr. König aber im Bereich der WebCam-Anwendungen, da diese Bilder einer breiten Öffentlichkeit zugänglich gemacht werden würden. Die rechtliche Situation führte er aber nicht weiter aus.[66] Auch auf der Homepage der DSK befinden sich dahingehend ebenfalls keine Verweise.

2.6. Datenschutzgesetz 2000 (DSG 2000)

Der Schutzbereich des Datenschutzgrundrechts ist in § 1 DSG 2000 beschrieben:

Grundrecht auf Datenschutz

> „§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das

[64] Internet und Recht. „Urheberrecht“. (http://www.internet4jurists.at/gesetze/bg_urhg2a.htm#§_78.) (05.04.2008).
[65] Siehe: König, Gregor. *Videoüberwachung*. Verlag Österreich. Juristische Schriftenreihe Bd. 179: 2001. S. 179ff.
[66] Siehe: Ebenda. S. 180.

> Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind."

Damit ein Sachverhalt in den Bereich des DSG fällt, müssen folgende Voraussetzungen gegeben sein:[67]

1. Die Daten müssen „personenbezogen" sein (Siehe Kap. 3.4.2. Personen-bezogene Daten).
2. Die Daten müssen einem Geheimhaltungsanspruch zugänglich sein (d.h. nicht öffentlich verfügbare Daten).
3. An den Daten muss ein subjektives Geheimhaltungsinteresse der Betroffenen bestehen (z.B. medizinische Daten, Polizeiakten, Finanzakten, ...).
4. Das Geheimhaltungsinteresse muss objektiv schutzwürdig sein.

3. Anwendung des Datenschutzgesetzes in Österreich

3.1 Datenschutzkommission (DSK)

Um den Wildwuchs von Datenanwendungen einzudämmen und eine Kontrollinstanz zu schaffen, sieht die EU-Richtlinie die Installation einer Institution vor, die eine Kontrollfunktion ausführt (Art. 28 Abs. 1 der RL 95/46/EG). Sie besagt, dass es

> „[...] in jedem Mitgliedsstaat der Europäischen Union ‚eine oder mehrere Behörden' geben [muss], die zur Überwachung der Einhaltung der nationalen Datenschutzgesetze berufen sind."[68]

Die DSK ist eine eigenständige Behörde, die keinem Amt unterstellt ist.[69]

> „Die Mitglieder der Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden."[70]

[67] Siehe: Kunnert, Gerhard. „Big Brother in U-Bahn, Bus und Bim". *juridikum* 2006/01, S. 44.
[68] Datenschutzbericht 2007. (www.dsk.gv.at). S. 70.
[69] Die Ansiedlung der DSK im Bundeskanzleramt lässt allerdings Datenschützer daran zweifeln ob sie wirklich als vollständig unabhängige Institution arbeitet.
[70] §37 Abs. 1 DSG 2000.

„[I]hre Mitglieder sind unabhängig, ihr Vorsitzender ist Richter [Mitglied des Berufsstandes; siehe 3.1.1].“[71]

3.1.1. Gliederung der DSK

Die DSK selbst besteht aus 6 Mitgliedern und 6 Ersatzmitgliedern, die vom Bundespräsidenten ernannt werden. Die jeweiligen Mitglieder (und Ersatzmitglieder) werden von folgenden Institutionen vorgeschlagen:[72]

Präsident des Obersten Gerichtshofes (OGH) → 1 richterliches Mitglied
Länder → 2 Mitglieder
Bundeskammer für Arbeiter und Angestellte → 1 Mitglied
Wirtschaftskammer Österreich → 1 Mitglied
Bundesregierung aus dem Kreis der Bundesbeamten → 1 Mitglied

Die derzeitigen Mitglieder sind:[73]

- Dr. Anton Spenling, Vorsitzender (richterliches Mitglied)
- Dr. Waltraut Kotschy, geschäftsführendes Mitglied
- Mag. Helmut Hutterer
- Dr. Claudia Rosenmayer-Klemenz
- Dr. Ludwig Staudigl
- Mag. Daniela Zimmer

3.1.2. Aufgaben der DSK

Die Aufgaben der DSK bestehen im Wesentlichen[74]

- In der Führung des Datenverarbeitungsregisters (DVR):

  Meldepflichtige Anwendungen müssen dem DVR, als Teil der DSK, gemeldet werden. Zu diesem Zweck hat die DSK eigens Formulare erstellt, um die Anmeldung zu erleichtern.

[71] Datenschutzbericht 2007. S. 10.
[72] Siehe: Ebenda.
[73] Siehe: (www.dsk.gv.at) (05.04.2008).
[74] Siehe: Ebenda.

- In der Funktion als Stammzahlenregisterbehörde:

  „Die DSK vergibt Stammzahlen, um eine eindeutige Identifikation von natürlichen Personen im Bereich des E-Governments sicherzustellen. Sie stellt auch deren rechtmäßige Verwendung sicher.“[75]

- In Kontrollbefugnissen und Beschwerdenannahmen

  lt. §30 DSG 2000 kann sich jeder

  > „[...] wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters [...] an die Datenschutzkommission wenden.“[76]

3.1.3. Recht auf Auskunft, Beschwerde und Löschung

Ein Betroffener hat das Recht beim Auftraggeber einer Datenanwendung Auskunft über ihn gesammelten Daten zu erlangen. Dieses Recht beinhaltet auch Informationen, ob diese Daten weitergegeben worden sind und an wen. Wird die Auskunft verweigert, kann man bei der DSK Beschwerde einreichen.
Liegt eine Verletzung des Rechts auf Auskunft vor, wird von der DSK die eingegangene *Beschwerde* überprüft. Im Falle einer Beschwerde gegen einen Auftraggeber des öffentlichen Bereichs, kann man bei der DSK auch das Recht auf *Löschung* und *Richtigstellung* einfordern. Ist die *Beschwerde* gegen einen Auftraggeber des privaten Bereichs gerichtet, so sind dafür die Zivilgerichte zuständig. Die DSK ist in diesen Fällen nur dann zuständig, wenn

> „[...] der Betroffene seine Beschwerde gegen einen Auftraggeber des öffentlichen Bereichs richtet, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist. [...] (§1 Abs. 5 DSG 2000).“[77]

Die DSK ist berechtigt, in die Datenanwendungen von öffentlichen und privaten sowie gemeldeten und nicht gemeldeten Datenanwendungen Einsicht zu nehmen und Kopien zu erstellen.

[75] Stammzahlenregister. (www.stammzahlenregister.gv.at/) (01.04.2008).
[76] Mayer-Schönberg. 1999. S. 100.
[77] (www.dsk.gv.at/dskd.htm) (05.04.2008).

3.1.4. Datenschutzbericht

Der Datenschutzrat hat in der DSK beratende Funktion und ist verpflichtet regelmäßig einen Datenschutzbericht zu veröffentlichen.
Durch vermehrte Anfragen, damit verbundenem erhöhten Arbeitsaufwand und personeller Unterbesetzung kann die DSK ihren Aufgaben nicht mehr vollständig nachkommen. Die DSK kritisiert diesen Zustand auch im Datenschutzbericht 2007 dahingehend, dass sie der „Prüfung von Datenanwendungen vor Ort“[78] nicht nachkommen kann. Sie bemängelt auch, dass „[...] die faktische Nicht-Ausübung dieser Kontroll-Kompetenz an sich schon als mangelnde Aufgabenerfüllung angesehen werden [muss]“.[79]

3.1.5. Zulässigkeitsprüfung

Die DSK hat bei Eingang eines Formulars für Datenanwendungen innerhalb von 2 Monaten zu prüfen, ob die Anwendung durchgeführt werden darf oder nicht. Dr. Gregor König hat den Aufgabenbereich der DSK zur Zulässigkeitsprüfung in 4 Punkte eingeteilt:[80]

1. Ist Zweck und Inhalt der Datenanwendung von den rechtlichen Befugnissen des Auftraggebers gedeckt?
2. Ist die Grundrechtseinschränkung verhältnismäßig?
3. Sind die schutzwürdigen Geheimhaltungsinteressen der Betroffenen gewahrt?
4. Sind die allgemeinen Datenschutzgrundsätze eingehalten?

Nur bei positiver Bearbeitung aller Punkte ist eine Überwachungsanlage zulässig. Dabei gilt der Grundsatz: „Je intensiver der Eingriff, desto schwerer muss der Anlass für die Überwachung wiegen.“[81]

[78] Datenschutzbericht 2007, S. 25 (siehe auch: §30 Abs. 2 und 3 DSG 2000).
[79] Ebenda.
[80] König, Gregor in: Jahnel. 2007. S. 125.
[81] Wiederin, Ewald. Videoüberwachung und Grundrechte. S. 123. in: Reiter/Wittmann-Tiwald. 2007. S.117-123.

3.2. Videoüberwachung

> „Positiv und ‚videospezifisch' formuliert kann man sagen, dass §1 Abs 1 DSG 2000 jedermann im Prinzip einen grundrechtlichen Anspruch darauf einräumt, dass sein in der Öffentlichkeit gezeigtes Verhalten nicht [*Herv. Fürst*] ‚videoaufgezeichnet' wird."[82]

Der Versuch durch Videoüberwachung Vandalismus zu bekämpfen hat in den letzten Jahren stark zugenommen. Sucht man allerdings im DSG 2000 einen Paragrafen über Videoüberwachung, so sucht man umsonst. Dieser Punkt wurde nicht ausgearbeitet bzw. sind die Formulierungen so allgemein gehalten, dass sie sogar für Juristen nicht immer eindeutig sind.[83] Nachdem die DSK über Registrierungen entscheidet, musste sie selbst eine Richtlinie für Videoüberwachung erstellen:

> „Mangels einschlägiger detaillierter gesetzlicher Regelungen war es notwendig, Leitlinien für die Registrierung von Videoüberwachungsmeldungen zu entwickeln, um dem DVR [Datenverarbeitungsregister; siehe Kap.3.1.2. *Anm. Fürst*] Anhaltspunkte dafür zu geben, wann es registrieren darf und wann ein ablehnender Bescheid für die Beschlussfassung durch das Kollegium der DSK vorzubereiten ist."[84]

Um eine Kamera mit Aufzeichnungsfunktionen aber auch verwenden zu dürfen, bedarf es der Bestätigung der DSK. Sie trifft die Entscheidungen, ob ein Eingriff berechtigt oder überhaupt notwendig ist bzw. wie stark in die Privatsphäre von Betroffenen eingegriffen wird. Die DSK kann zuerst Vorschläge für Maßnahmen unterbreiten die einen geringeren Eingriff darstellen. Dies kann dazu führen, dass sie z.B. den Einsatz von Kameras ablehnt, da bisher keine anderen Schutzmaßnahmen ergriffen wurden, die einen weniger starken Eingriff darstellen. Dazu sind unter anderem der Einsatz von Wachpersonal oder einer zusätzlichen versperrbaren Tür (bei vermehrtem Auftreten von Einbrüchen und Diebstählen) u.ä. zu zählen.

Die Formulare wurden aufgrund der Erfahrung im Umgang mit Anwendern erstellt. Sie sollen das Anmeldeverfahren beschleunigen und den Anwendern die Möglichkeit geben an die nötigen Informationen zu gelangen. Wegen der vielen eingehenden Anfragen hat die DSK

[82] Kunnert, Gerhard. 2006/01, S. 46.
[83] Siehe: König. 2001. S. 109: „[...] Videoüberwachung und –aufzeichnung seien schon deshalb kein datenschutzrechtliches Problem, weil sie im DSG nicht explizit geregelt sind. Gerade darin liegt aber [...] das größte der zahlreichen damit verbundenen Probleme."
[84] Datenschutzbericht 2007. S. 61.

Online-Formulare erstellt, um die Registrierung zu erleichtern.[85] Dr. Hans Zeger sieht aber gerade darin, in der Vereinfachung der Meldepflicht über Online-Formulare, die Gefahr des Wildwuchses von Überwachungskameras.[86]

Nachdem die DSK jene Instanz ist, die über den Einsatz von Videoüberwachung entscheidet, wird im Folgenden die Definition von „Videoüberwachung" wiedergegeben, wie sie im Datenschutzberichtes 2007 zu finden ist:

> „Unter ‚Video*überwachung'* wird die Beobachtung, d.h. die systematische und längerdauernde visuelle und allenfalls auch akustische Kontrolle einer Örtlichkeit mit Hilfe von Videokameras verstanden."[87]

Da nicht jede Kamera den Zweck der Überwachung erfüllt, gibt es natürlich Abstufungen bzw. Anlagen, die von der Registrierung ausgenommen sind.
Das DSK unterscheidet hierbei zwischen WebCam-Anwendungen (Anwendungen ohne Kontroll- bzw. Überwachungszweck), Überwachung durch *real time monitoring* (RTM – Videoüberwachung ohne Aufzeichnung bzw. Speicherung der Daten) und Überwachung durch Aufzeichnung (Videoüberwachung mit dem Ziel der Aufzeichnung).

WebCam-Anwendungen sind sehr einfach und im Prinzip überall möglich. Sie werden für Panoramabilder, an Flugplätzen, Baustellen, und auch in Wirtshäusern benutzt. Man kann also den Wirtshausbetrieb von zuhause aus mitverfolgen, wer trinkt was und wie viel. Nachdem hierbei keine Aufzeichnung erfolgt, sind derartige Anwendungen legal. Allerdings bräuchte es nur einen User, der diese Bilder speichert, um die Anwendung theoretisch meldepflichtig zu machen. Das Problem dabei ist aber das Fehlen der nötigen Kontrollmöglichkeiten. „Mit der digitalen Aufzeichnung von Daten wird es heikel", wird die Wiener Anwältin Margot Artner im Standard zitiert.[88] Es besteht vor allem die Möglichkeit des Missbrauchs und der Verwendung der Daten außerhalb ihres ursprünglichen Zusammenhangs (*function creep*). Die Homepage *globocam.de* zeigt alleine für Österreich über 1900 WebCam-Anwendungen an.

---

[85] Siehe: (www.dsk.gv.at) (04.04/2008). (Die Novelle zum DSG 2000 sieht im §50 eine Kennzeichnungspflicht vor.).
[86] Vortrag: Dr. Hans Zeger: Überwachungsunion Europa (Wien, 08.05.2008).
[87] Datenschutzbericht 2007. S. 64 (Betonung DSK).
[88] Haupt, Cornelia: „Schadenersatz für indiskrete Webcams" (http://weblog.derdetektiv.at/categories/35-Videoueberwachung) (08.02.2008).

Abb. 4: WebCam-Anwendung [*Grafik Fürst*]

Videoüberwachung, die nur am Monitor, also live und ohne zusätzliche Speicherung, abläuft und von einem Menschen überwacht wird, kann man keinen Informationseingriff unterstellen. Die Bahnsteigüberwachung der Wiener Linien wäre ein derartiger Fall.

> „Schon infolge der begrenzten Leistungsfähigkeit des menschlichen Gehirns, ist ein menschliches Aufsichtsorgan genötigt, sich bei der Überwachung auf die Wahrnehmung ‚abweichenden' bzw. ‚auffälligen' Verhaltens zu beschränken."[89]

Abb. 5: Real-Time Monitoring [*Grafik Fürst*]

Die Überwachung durch Video*aufzeichnung* stellt in jedem Fall eine Datenanwendung dar und ist der DSK zu melden.

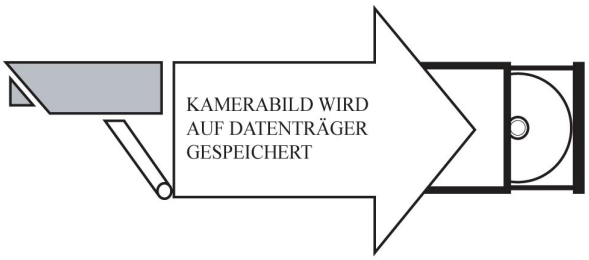


Abb. 6: Videoaufzeichnung und Speicherung [*Grafik Fürst*]

[89] Kunnert. 2006/01. S. 47.

Zudem stellen technische Zusatzmaßnahmen eine „Überhöhung“ dar, die außerhalb des menschlichen Vermögens liegen. Das bedeutet, ein Eingriff ist gegeben sobald

- die Daten gespeichert,
- ein Teleobjektiv, oder
- ein Zoomobjektiv verwendet werden.

Da sich Tele- und Zoomobjektiven außerhalb des Wahrnehmungsvermögens der Betroffenen befinden, ist sogar das Fehlen von Aufzeichnung ein Eingriff.[90]

3.2.1. Zweck der Videoüberwachung

Der Zweck der Videoüberwachung liegt in der Datenermittlung. Datenschutzrechtlich relevant sind Daten aber erst ab dem Zeitpunkt, an dem ein Personenbezug besteht d.h. ihre Identität bestimmt werden kann.[91]
Dem Zweck der Videoüberwachung wird bei der Entscheidung, ob eine Meldepflicht besteht oder nicht, große Bedeutung zugemessen (§ 4 Z 7 und § 7 Abs. 1 DSG 2000).
Es gibt folgende Hauptgründe für den Einsatz von Videokameras, die durch die Meldungen und Anfragen von der DSK angegeben werden:

- Schutz des Eigentums des Auftraggebers (Vandalismus, Diebstahl) – *Eigenschutz.*
- Schutz der Mitarbeiter des Auftraggebers – *Verantwortungsschutz.*
- Schutz von anderen Personen (als Mitarbeitern) gegen strafrechtliches Verhalten oder sonstige Verfahren – *Fremdschutz.*

Der hier angeführte „Schutz“ wird „sowohl als Generalprävention, also Verhinderung, als auch Spezialprävention, also Verfolgung, verstanden.“[92] Der Zweck der Überwachung ist von besonderer Bedeutung, da sie, sofern öffentliche Bereiche abdeckt werden, ausschließlich von der Sicherheitspolizei durchgeführt werden darf und damit in den Bereich des SPG fällt. Überwachung im öffentlichen Raum fällt immer unter *Fremdschutz.* Der Private ist allerdings

[90] Siehe: Kunnert. 2006/01.
[91] Siehe: Steiner/Andreewitch. „Videoüberwachung aus datenschutzrechtlicher Sicht.“ *Medien und Recht.* 2006/02, S. 80.
[92] Datenschutzbericht 2007. S. 64.

weder berechtigt den öffentlichen Raum zu überwachen noch kann er *Fremdschutz* als Zweck für die Installation von Kameras anführen.

3.2.2. Personenbezogene Daten

Von besonderer Bedeutung für die Anwendung von Videoüberwachung ist die Definition von „personenbezogenen Daten". Schon die Möglichkeit (nicht deren Ausführung) Gesichtszüge auf den Aufnahmen zu erkennen stellen personenbezogene Daten dar.

> „Für das Vorliegen einer ‚Verarbeitung personenbezogener Daten' kommt es nicht darauf an, ob die aufgenommenen Personen tatsächlich identifiziert werden; es genügt vielmehr, dass diese grundsätzlich identifizierbar sind. [...] ‚Identifizierbar' sind Daten auch dann, wenn nicht der Aufnehmende, sondern nur ein Dritter (z.B. eine Sicherheitsbehörde) voraussichtlich in der Lage sein wird, eine Identifikation erfolgreich vorzunehmen."[93]

Durch die Speicherung von Daten können die zusätzlich gewonnen Informationen über Ort und Zeitpunkt eine Identifikation darstellen und damit auch unter den Begriff *personenbezogen* fallen.

3.2.3. Sensible Daten

Die DSK hat festgehalten, dass Videoaufzeichnungen prinzipiell *sensible Daten* ermittelt. Unter sensiblen Daten versteht man *besonders schutzwürdige Daten,* die Aufschluss über „rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben"(§ 4 Abs. 2 DSG 2000) einer Person geben. Somit unterlägen sie der Vorabkontrolle durch die DSK (ff § 17 DSG 2000).[94]

Nachdem der Zweck der Videoüberwachung meistens auf genau diese Informationen (Verdächtige identifizieren zu können) abzielt, sind ein Großteil der Überwachungsbilder als sensible Daten einzustufen.

[93] Datenschutzbericht 2007. S. 65.
[94] Siehe: Steiner/Andreewitch. 2006/02, S. 82.

3.2.4. Datenanwendungen[95]

Die Ermittlung von Daten stellt einen „Eingriff in das Grundrecht auf Datenschutz dar“ und ist nur unter der Berücksichtigung auf §1 DSG 2000 erlaubt (dazu zählen lebenswichtige Interessen; Zustimmung des/der Betroffenen; Wahrung überwiegender berechtigter Interessen;).
Die Meldepflicht ist auf Datenanwendungen beschränkt. Der §16 ff DSG 2000 besagt folgendes: der Tatbestand einer Datenanwendung

> „[...] liegt vor, wenn die zur Erreichung des Zwecks der Datenanwendung vorgenommen Verarbeitungsschritte ‚zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen’ [...] Nur die Videoüberwachung mit Daten*aufzeichnung* ist demgemäß eine ‚Datenanwendung’.“[96]

Hierbei ist anzumerken, dass bei digitaler Bildaufzeichnung auf jeden Fall eine Datenanwendung vorliegt. Bei analogen Aufzeichnungen ist dies nur der Fall, wenn sie als „‚Datei’ organisiert ist“.[97] Eine Datei im Sinne des §4 Z 6 DSG 2000 ist eine „strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind.“[98]

3.2.5. Ausnahmen

Die Zustimmung der DSK eine Videoüberwachung auch wirklich anzuerkennen, wird zum einen vom Zweck und zum anderen von der Zulässigkeit abhängig gemacht. Der § 1 Z 2 DSG 2000 besagt:

> „(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zu Wahrung überwiegender berechtigter Interessen eines anderen zulässig, [...]“[99]

Dies bedeutet, dass entweder die *Zustimmung* aller Betroffenen vorhanden sein muss oder *lebenswichtige Interessen* gewahrt werden müssen. Bei *Wahrung überwiegend berechtigter Interessen* ist weiters zu prüfen, ob das angegebene *berechtigte Interesse* auch vorliegt. Im § 1

[95] Siehe: Kapitel 2.1.
[96] Datenschutzbericht 2007. S. 65.
[97] Datenschutzbericht 2007. S. 65.
[98] §4 Z 6 DSG 2000.
[99] Mayer-Schönberger. 1999. S. 53.

Z 2 DSG 2000 wird zu diesem Punkt noch angefügt, dass „der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden [darf]“.[100] Dieses *Verhältnismäßigkeitsgebot*[101] regelt, ob *berechtigtes Interesse* des Auftraggebers über den Interessen des Betroffenen d.h. dessen Recht auf Geheimhaltung seiner Daten überwiegt. Gibt die DSK dem Antrag statt, dürfen personenbezogene Daten ermittelt werden.

3.2.5.1. Verhältnismäßigkeitsgebot

Dieses Interesse muss vor einer Zusage zu einer Datenanwendung geprüft werden. Das *Verhältnismäßigkeitsgebot* (§ 1 Abs. 2 DSG) steht hier an oberster Stelle: Dabei wird abgewogen, ob der Eingriff in die Privatsphäre eines Betroffenen schwerer wiegt als das Interesse des Anwenders.

Für die private Videoüberwachung ist zudem die „gesamte Rechtsordnung“ als Entscheidungsgrundlage heranzuziehen.

> „Für die Videoüberwachung zu nicht-behördlichen Zwecken (und daher insbesondere auch für jede Datenermittlung mit Hilfe von Videokameras durch Private) gilt nicht der strenge Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 für Grundrechtseingriffe – mangels konkreter gesetzlicher Ermächtigungen kann sich die Berechtigung zu einem Grundrechtseingriff diesfalls auch aus einer Gesamtschau der Rechtsstellung des Auftraggebers in der Rechtsordnung ergeben.“[102]

Die Entscheidung, ob die Videoüberwachung für private Zwecke zulässig ist hängt davon ab

> „[...] ob in der konkreten Fallkonstellation der mit der Videoüberwachung verfolgte Zweck nach objektiven Kriterien als vorrangig gegenüber dem Datenschutzinteresse der von der Überwachung Betroffenen zu werten ist.“[103]

3.2.6. Einteilung des Raumes

Hier ergibt sich ein weiteres Problem, dass einer genaueren Definition bedarf: der *öffentliche Raum*. Folgende Unterteilungen werden vom DSK verwendet:[104]

[100] Siehe: Mayer-Schönberger. 1999. S. 53.
[101] Datenschutzbericht 2007. S. 66.
[102] Ebenda. S. 66.
[103] Ebenda. S. 68.

- *Öffentlicher Raum*: ist jener Bereich, in dem sich jedermann grundsätzlich unbeschränkt aufhalten darf und eine Zutrittkontrolle rechtlich nicht – oder nur aus besonderem Anlass – zulässig ist. Dies betrifft etwa Straßen, Plätze, die freie Natur etc.
- *Beschränkt öffentlicher Raum*: ist jeder Bereich, in dem zwar ein privatrechtliches Verfügungsrecht über die Örtlichkeit besteht, die Berechtigung des Zutritts jedoch nicht auf von vornherein bestimmt Personen (z.B. „Schüler der Schule", „Patienten" etc.) beschränkt ist.
- *Nicht-öffentlicher Raum*: Zutritt nur für bestimmte Personen wie Mitarbeiter
- Privater Raum: ist rein privaten, insbesondere Wohnzwecken vorbehalten.

Man muss, ungeachtet dieser Einteilung, festhalten, dass das Recht auf Privatsphäre im öffentlichen Raum trotzdem aufrechterhalten bleibt. Die DSK hat unter Anwendung des § 1 DSG 2000 festgestellt, dass die

> „[...] Geheimhaltung keineswegs auf den innersten Kreis einer privaten, der Öffentlichkeit verborgenen Lebensgestaltung beschränkt [ist]. Vielmehr umfasst dieser Anspruch auch Äußerungen der privaten Lebensgestalt die sich in einer öffentlichen oder teilöffentlichen Sphäre abspielen."[105]

Die Privatsphäre kann und muss also auch im öffentlichen Bereich respektiert und eingehalten werden, d.h. sie ist nicht ausschließlich auf den Privatraum beschränkt.

3.2.7. Meldepflicht

Der Meldepflicht unterliegen nur *Datenanwendungen*. Die Video*aufzeichnung* ist eine Datenanwendung (§ 4 Z 7 DSG 2000) und somit meldepflichtig.
Wird die Videoüberwachung zum Zweck der Strafverfolgung, also nicht für „rein persönlich oder familiäre Tätigkeiten" (§§ 17 und 45 DSG 2000) eingesetzt, stellt sie ebenfalls eine Datenanwendung dar und unterliegt der Meldepflicht. Diese darf aber erst nach einer Vorabkontrolle der DSK in Betrieb genommen werden. Werden *sensible Daten*

[104] Datenschutzbericht 2007. S. 67.
[105] Kunnert, Gerhard. 2006/01, S. 44.

aufgezeichnet, unterliegen sie ebenfalls der Vorabkontrolle der DSK.[106] Ist der Zweck der Strafverfolgung nicht gegeben und ist die Datenanwendung eine „rein persönliche“ (Filmen auf Privatfeiern, Urlaubsvideos, etc.) so ist sie nicht meldepflichtig. Die Abgrenzung zu „rein persönlichen Tätigkeiten“ ist allerdings nicht detailliert festgehalten.

Das DSG sieht zusätzliche Unterscheidung zwischen analoger und digitaler Aufzeichnung. Während die digitale Aufzeichnung meldepflichtig ist, gilt die analoge Aufzeichnung nur dann als Datenanwendung, wenn die als *Datei* d.h. nach mindestens einem Suchkriterium geordnet ist.[107]

Gregor König geht in dieser Hinsicht noch weiter, wenn er behauptet, dass eine Videoüberwachung prinzipiell im Hinblick auf eine Beweisführung, also eine Weitergabe an eine Behörde ausgerichtet ist, und somit meldepflichtig ist.[108]

Die Meldung zur Registrierung umfasst laut § 19 DSG 2000 folgenden Angaben:

> „Diese [Meldung] hat – wie bisher – den Namen und die Anschrift des Auftraggebers, die Registernummer des Auftraggebers, den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten, die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise – einschließlich allfälliger ausländischer Empfängerstaaten – sowie die Rechtsgrundlagen der Übermittlung und – soweit eine Genehmigung der Datenschutzkommission notwendig ist – die Geschäftszahl der Genehmigung durch die Datenschutzkommission zu enthalten.“[109]

Aufgrund des fehlenden Gesetzestextes bzgl. Videoüberwachung herrscht unter den Betreibern von Überwachungsanlagen Unklarheit. Zum einen werden Anlagen überhaupt nicht registriert und zum anderen werden Anträge für Anlagen eingereicht, die nicht meldepflichtig sind. Die DSK geht bei manchen Anträgen aber auch davon aus, dass die Registrierung nicht-meldepflichtiger Anlagen als eine Art Qualitätsmerkmal der jeweiligen Betreiberfirma gelten soll.

---

[106] Anwendungen die der Vorabkontrolle unterliegen dürfen nicht sofort nach Abgaben der Meldung sondern erst nach Prüfung durch die DSK in Betrieb genommen werden. (§ 18 Abs. 1 DSG 2000)

[107] Die DSK kam im Falle einer einzelnen handgeführten Kamera mit analoger Magnetaufzeichnung, die durch handschriftliche Aufzeichnungen unterstützt (Ort und Datum) wurde, zu dem Schluss, dass hierbei weder eine „automationsunterstütze Verarbeitung“ vorlag noch das Kriterium der Strukturiertheit erfüllt wurde. (Steiner. Andreewitch. 2006. S. 81ff).

[108] König, Gregor, 2001. S. 122.

[109] Mayer-Schönberger, 1999. S. 28.

Private Bildaufnahmen, Bildaufnahmen für touristische Zwecke, Verkehrsstrom-Analysen, künstlerische oder kommerzielle Film- und Fotoherstellung die nicht zum Zweck der Identifikation der Abgebildeten hergestellt werden, unterliegen nicht der Meldepflicht.

Wird als Grund für die Überwachung der *Schutz vor bestimmten Gefahren* angegeben, so muss der Auftraggeber die Notwendigkeit eines solchen Eingriffs auch glaubwürdig darstellen. In speziellen Räumlichkeiten wie in Banken oder Museen ist der Grund der *erhöhten Gefährdung* zum Beispiel durchaus gegeben.

Ein Problem es allerdings bei der Überwachung von Verkaufsräumen, Eingangsbereichen von Wohnhäusern und Wohnungen sowie Gebäudefassaden. Die DSK versucht die jeweiligen Situationen individuell abzuwägen und nach dem „Prinzip des gelindesten (Eingriffs-) Mittels“[110] zu lösen. Haustorüberwachungen, die Teile des Gehsteiges (öffentlicher Raum) mitüberwachen, sind „nur im Ausnahmefall zulässig d.h. nur im absolut unvermeidlichen sachlichen und räumlichen Ausmaß.“[111] Die Überwachung öffentlicher Räume stellt ein Monopol der Sicherheitsbehörden dar, die dem Privaten als Zweck gänzlich untersagt ist. *Verantwortungsschutz* und *Eigenschutz* können aber in Bereichen des Privatbesitzes geltend gemacht werden, der an öffentlichen Raum angrenzt.

Die von der DSK durchgeführten Registrierungsverfahren haben an folgenden Örtlichkeiten Zustimmung gefunden:[112]

- Kassensaal einer Bank (ES, VS)
- Öffentlich zugänglicher Teil eines Museums (ES)
- Eingang und Verkaufsraum eines Juweliergeschäftes (ES)
- Lager von Waffen- und Munitionshersteller (ES)
- Fahrzeuge von Unternehmen des öffentlichen Verkehrs (ES, VS)
- Bahnhöfe bzw. Stationsgebäude/anlagen an öffentlichen Verkehrslinien (ES, VS)
- Fassaden von denkmalgeschützten Gebäuden, die an öffentlichen Plätzen angrenzen (ES)

(ES – Eigenschutz, VS – Verantwortungsschutz)

[110] Datenschutzbericht 2007. S. 68.
[111] Ebenda.
[112] Siehe: Ebenda. S. 69.

3.2.8. Kennzeichnung

Das DSG 2000 sieht, aus Mangel an klaren Richtlinien, keine direkten verpflichtenden Kennzeichnungen videoüberwachter Bereiche vor.[113] Im § 24 DSG findet sich allerdings ein Hinweis darauf:

> „§24. (1) Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise
> 1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und
> 2. über Namen und Adresse des Auftraggebers,
>
> zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegt.“[114]

Das Kapitel „Videoüberwachung“ des Datenschutzberichtes 2007 erwähnt diese Hinweispflicht aber nicht. Es wäre allerdings schon alleine im Sinne einer Präventivmaßnahme sinnvoll, überwachte Bereiche zu kennzeichnen. Es wäre darauf hinzuweisen, dass überwacht wird und wo überwacht wird. Hinweisschilder findet man u.a. vor dem Eingang von Supermärkten und – wo sie v.a. in Wien präsent sind – bei den Eingängen zu den U-Bahnen. Diese Hinweisschilder und Kameras sind so anzubringen dass sie gut sichtbar sind. Die Arge-Daten formuliert es in dem Artikel „Überwachungskameras in Wiener U-Bahn“ so:

> „Wenn daher Überwachung für einen konkreten Ort notwendig sein sollte, sollte dies entsprechend angekündigt werden, der überwachte Bereich auch entsprechend gekennzeichnet werden und auch angegeben werden, wer verantwortlich zeichnet und wo man seine Informationsrechte nach dem Datenschutzgesetz wahrnehmen kann.“[115]

Die Untersuchungen von URBANEYE ergaben, dass im Durchschnitt 51% aller Überwachungsanlagen in den untersuchten Ländern, nicht gekennzeichnet wurden (in Österreich und Ungarn über 80%).[116] Ähnlich bedauerlich verhielt sich auch die

---

[113] Das DSG 2000 enthält dazu keine Angaben. Verweise darauf aber in: *Die Presse* (2.2.2005) Nowak/Fritzl/ Stöger. „Prokops Pläne: Massive Ausweitung der Videoüberwachung“. Darin wird festgehalten dass in der Novelle des DSG 2000 „Videoüberwachung eines öffentlichen Ortes mit Hinweisschildern angekündigt werden muss.“ Und *Die Presse* (19.10.2007) Wetz, Andreas: „Boom bei Spionagekameras“: „Weiters müssen Betreiber von Überwachungsanlagen Kunden und Passanten ausdrücklich darüber informieren, dass sie gefilmt werden. Allerdings: Geschieht dies nicht, hat das vor Gericht kaum Konsequenzen.“
Der Autor des Artikels vom 19.10.2007 bestätigte dem Autor dieser Arbeit dies auch telefonisch.

[114] Mayer-Schönberger. 1999. S. 90.

[115] Arge-Daten: „Überwachungskameras in Wiener U-Bahn Zügen“ (vom 12.04.2005). (http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=18195sst) (05.04.2008).

[116] Siehe: Hempel/Töpfer. 2004. S. 7.

Auskunftsbereitschaft: Im europäischen Schnitt wurden 43% der Anfragen, wer denn eigentlich der Besitzer sei, abgelehnt.[117]

> „Die Geheimhaltung der Videoüberwachung war am schlimmsten in Österreich, Deutschland und Ungarn, wo in 55% bis 87% der Fälle ein Interview verweigert wurde [...]."[118]

3.2.9. Aufbewahrungsdauer

Im DSG 2000 findet sich kein exakter Anhaltspunkt, der die Dauer bzw. die Löschung von Daten vorsieht. Bei Expertengesprächen der Österreichischen Juristenkommission zum Thema „Sicherheit im öffentlichen Raum" 2006 wird auf die Richtlinie von 48 Stunden hingewiesen, wie sie auch für die Einsätze unter dem SPG gilt. Die DSK gibt in ihren Bescheiden den Zeitrahmen vor, und kann ihn auch individuell variieren.
Dr. Bernd-Christian Funk (*Institut für Staats- und Verwaltungsrecht, Juridicum, Universität Wien*) sieht die Gefahr darin, dass es keine eindeutige gesetzliche Grundlage gibt. Damit verbunden ist die Ungewissheit, was mit aufgezeichnetem Bildmaterial überhaupt passiert.[119] Wer kontrolliert wann und ob Daten gelöscht werden? Diese Unsicherheit brachte Dr. Hannes Tretter (*Ludwig-Boltzmann Institut für Menschenrecht Wien, Universität Wien*) auf den Punkt:

> „Ich weiß nicht, wo Daten und Bildaufzeichnungen, auch wenn sie offiziell nach 48 Stunden gelöscht werden, versteckt werden, wo sie weitergeleitet werden, wo irgendwelche Datenmengen weggeschnitten werden, um irgendwie in einem anderer Zusammenhang wieder aus dem Koffer hervorgezaubert zu werden."[120]

Bei diesen Gesprächen forderte Dr. Andreas Kletečka (*Rechtswissenschaftliche Fakultät, Privatrecht, Universität Salzburg)*, eine verpflichtende Buchführung für diese Daten, um auch dokumentieren zu können was damit passiert.[121] In England wurde dazu eine praktische Richtlinie erstellt aus dem DPA heraus erstellt, der die Rechte und Pflichten der Betreiberfirmen deutlich macht: Der *Code of Practice* (Siehe: Kap. 6).

---

[117] : Hempel/Töpfer. 2004. S. 6.
[118] Ebenda. S. 6. Wien wurde mit rund 55%, Berlin mit 72% und Budapest mit 87% angeführt.
[119] Österreichische Juristenkommission (ÖJK) (Hg.). *Grundrechte in der Informationsgesellschaft*. Mai 2001. Neuer Wissenschaftlicher Verlag: Wien, 2001. S. 19.
[120] Tretter, Hannes. in: Ebenda. S. 48.
[121] Kletečka, Andreas. in: Ebenda. S. 60.

4. Entscheidungen des DSK und des OGH

Die folgenden Beispiele sollen veranschaulichen wie die Entscheidungen des DSK und des Obersten Gerichtshofes (OGH) die Videoüberwachung regeln. Sie reichen vom Eigentumsschutz bei den Wiener Linien bis zur privaten Überwachung der Grundstücksgrenze wegen Belästigung durch die Nachbarn.

4.1. Wiener Linien[122]

Seit Beginn des U-Bahnbetriebes in Wien wurden die Bahnsteige mittels Fixkameras überwacht. Das primäre Ziel der Videoüberwachung dient der Betriebssicherheit, wobei sich dieses „Sicherheitssystem“ auch international bewährt hat. Bis 2005 erfolgte keine Aufzeichnung der Bilder. Seit diesem Zeitpunkt überwachen die Wiener Linien auch U-Bahnen und Straßenbahnzüge. Die Kameras sind Kuppel- bzw. Dome-Kameras mit hoher Auflösung.

Abb. 7: Dome-Kameras (U2 Station Praterstern)

Die Daten dieser Kameras werden aber nicht wie die Bilder der Bahnsteigüberwachung von einem Mitarbeiter (*real-time-monitoring*) beobachtet, sondern auf einer Festplatte gespeichert. Diese Daten inkludieren Ort und Zeit. Es kann nicht beobachtet und sofort eingegriffen werden, sondern dient nur der Aufklärung von z.B. Vandalenakten. Werden keine „Störungen“ gemeldet, werden die Daten nach 48 Stunden überspielt und somit wieder gelöscht.

[122] Siehe: Kunnert, Gerhard. 2006/01.

„Läuft der Test erfolgreich, werden Schritt für Schritt weitere U-Bahn-Züge und Straßenbahnen mit Kameras bestückt sowie entsprechende Aufzeichnungsmöglichkeiten geschaffen. Neben der Videoüberwachung in den U-Bahn-Fahrzeugen liefern derzeit rund 1.000 Videokameras Livebilder von den Bahnsteigen, Gängen und Rolltreppen auf die Monitore der Stationsüberwachung und der zentralen Leitstelle."[123]

Planungen für neue U-Bahn-Stationen sind begleitet von der Modernisierung der Kameras. Die zukünftigen Überwachungskameras sollen, trotz der ungeklärten rechtlichen Situation, schwenkbar sein und über eine Zoomfunktion verfügen.[124]

4.1.1. Anträge bei der DSK

Im Jahr 2005 wurden von den Wiener Linien zwei Anträge eingereicht: Der erste Antrag zur Videoüberwachung wurde mit der Begründung eingereicht, dem „[...] Zwecke der Erholung der Sicherheit ihrer Mitarbeiter sowie der Fahrgäste und die Eindämmung von Vandalismusschäden"[125] zu dienen. Diesem Antrag gab die DSK befristet bis zum 30. Juni 2009 auch statt. Bis dahin muss ein Erfahrungsbericht von den Wiener Linien vorgelegt werden, um Vergleiche mit nicht-videoüberwachten Stationen ziehen zu können.
Der Begründung der Wiener Linien, warum Videoaufzeichnungsgeräte installiert werden sollen („Schutz des Eigentums" und „Schutz der Fahrgäste"), kann Dr. Gerhard Kunnert (*BKA-Verfassungsdienst*) rechtlich nicht viel abgewinnen:

- Schutz des Eigentums:

  „Nicht unmittelbar einsichtig erscheint es demgegenüber, aus dem Eigentumsrecht bzw. der bloßen Möglichkeit dessen Verletzung eine Befugnis zur Erhebung personenbezogener Daten auch gegenüber Unbeteiligten bzw. im Verhältnis zur Gesamtmenge der Fahrgäste abzuleiten. Diese wäre wohl einen unverhältnismäßige Überdehnung des Eigentumsrechts. Ähnliches gilt für Zweck des Mitarbeiterschutzes."[126]

- Schutz der Fahrgäste:

[123] Wiener Linien. „Bericht 2005". S. 45. (www.wienerlinien.at) (12.03.2008).
[124] Siehe: Kunnert. 2006/01. S. 42.
[125] Bescheid der DSK vom 21.03.2007 (www.ris2.bka.gv.at/Dsk/) (05.04.2008).
[126] Kunnert. 2006/1. S. 48.

> „Die Zuständigkeiten der Wiener Linien konzentrieren sich auf die Gewährleistung der Betriebsicherheit.“[127] Daraus ergibt sich für Kunnert nicht zwingend die Befugnis zur Ermittlung personenbezogener Daten.

Es ist auch zu bedenken, dass Vandalismusschäden und der Versuch diese durch Videoüberwachung einzudämmen, nur von geringem Erfolg ist. Einerseits sind Vandalismusschäden nicht-rational, d.h. aus einer emotional aufgeladenen Stimmung heraus (z.B. Beschädigungen durch Sportfans). In einem solchen Fall ist die präventive Wirkung nicht vorhanden.[128] Personen, die Beschädigungen aus einer rationalen Überlegung heraus begehen, können sich im Normalfall durch Vermummung der Identifikation durch die Kameras entziehen.[129]

Die Aufzeichnung des Videomaterials hält Randalierer nicht ab. In dieser Hinsicht ist die Echtzeitübertragung von Bildern die einzige Möglichkeit, um sofort zu reagieren und im Notfall einzugreifen.

Für die Wiener Linien ist somit der Fall der Videoaufzeichnung – laut Kunnert – nicht das „gelindeste Mittel“. Die damit verbundene „Vorbeugung gegen Sachbeschädigung“ stellt keinen „festgelegten, eindeutigen Zweck“ einer Datenverwendung iSd § 6 DSG 2000 dar.[130]

> „Dieses Zahlenmaterial weist für die Jahre 2003 und 2004 Reparaturkosten von etwa 200.000 Euro für etwa 500 Fälle von Vandalismus aus, wobei zusätzlich von der Antragstellerin bemerkt wurde, dass nicht alle Fälle von Vandalismus sich in Zahlen niederschlagen, da nicht alles repariert wird (z.B. zerkratzte Fensterscheiben). Weiters wurden Beispiele angeführt, in welchen Vandalismus einhergeht mit echter Gefährdung von Fahrgästen und Personal, wie das Bestreichen von Glasscheiben mit Flußsäure.“[131]

Der zweite Antrag versuchte die rechtlichen Möglichkeiten der Datenweitergabe an die Exekutive auszuloten. Das Innenministerium und die Stadt Wien hatten dieses Sicherheitspaket bereits besiegelt: Das erklärte Ziel war es damit den Drogenhandel in öffentlichen Verkehrsmittel zu erschweren bzw. verfolgen zu können. Die DSK wies diesen Antrag ab, mit der Begründung, dass

---

[127] Kunnert. 2006/1. S. 42.

[128] Siehe: Müller, Henning Ernst. „Zur Kriminologie der Videoüberwachung“ in: *Monatsschrift für Kriminologie und Strafrechtsreform*. 2002/1. S. 33-46.

[129] Siehe auch: Stemmer, Martina: „Alles unter Kontrolle“ *Der Standard* (16.10.2007) bzgl. der Videoüberwachung aufgrund von Vandalismusschäden im Museumsquartier Wien: „Sind Sprayer wirklich so blöd, unmaskiert eine videoüberwachte Fassade zu besprühen? Ja, behauptet Waldner [MQ-Chef].“

[130] Kunnert, Gerhard. 2006/01 S. 50.

[131] Bescheid der DSK zur Aufnahme der Videoüberwachung der Wiener Linien vom 21.06.2005 (Rechtsinformationsservice des Bundeskanzleramtes: (www.ris2.bka.gv.at) (31.03.2008)).

> „[...] zwar eine Übermittlung von Videoaufzeichnungen an die Kriminalpolizei als Ausfluss der Ausübung des jedermann [...] zustehenden Anzeigerechts in Betracht käme, keinesfalls aber eine Übermittlung für sicherheitspolizeiliche Zwecke auf Aufforderung der Behörde.“[132]

Die Gewährleistung der Sicherheit und Ordnung ist außerdem nicht die Aufgabe der Wiener Linien. Aus diesem Grund mussten die Wiener Linien bereits aufgeklebte Hinweisplaketten mit der Aufschrift „Dieser Zug wird für ihre *Sicherheit* videoüberwacht“ entfernt bzw. mit solchen Plaketten überklebt werden, die nur darauf hinweisen, dass überwacht wird (siehe Abb. 8.).

Abb.8: Aufkleber der Wiener Linien zur Kennzeichnung der Videoüberwachung ihrer Züge[133]

Auf der Basis von Dr. Kunnert kritisiert auch die Arge-Daten die Videoüberwachung der Wiener Linien.

> „Die Wiener Linien sollten ihr millionenschweres Projekt stoppen. Bisher waren die Kosten für die vier Straßenbahn- und U-Bahnzüge noch vergleichsweise gering, eine flächendeckende Umrüstung würde erhebliche Mittel verschlingen, Gelder die etwa im Rahmen der Beschleunigung der Züge oder auch in der Hebung der Hygienestandards in den Wartebereichen besser investiert wären.“[134]

[132] Kunnert. 2006/01. S. 43 ff.
[133] Programmheft der „Big Brother Awards 2007“.
[134] Arge-Daten: „Videoüberwachung durch Wiener Linien zulässig?“ (26.06.2006) (www2.argedaten.at) (20.03.2008).

4.2. Videoüberwachung der ÖBB

Seit der Einführung der Kameraüberwachung der ÖBB ist der Bestand von 896 stationären Kameras (Mai 2007) auf 1860 Kameras erhöht worden.[135] Damit sollen die Haltestellen und Bahnhöfe überwacht werden. Bis zur Europameisterschaft im Juni 2008 sollte die Zahl der Kameras auf 2000 erhöht worden sein.[136] Ähnlich wie die Wiener Linien sind auch die ÖBB darauf bedacht, Vandalismusschäden durch den Einsatz von Videokameras einzudämmen, und nach eigenen Angaben mit gutem Erfolg: 50 Schnellbahnzüge, die mit Kameras überwacht werden, weisen weniger oft Beschädigungen auf.[137] Darüber hinaus fühlen sich einer Studie zufolge „83% aller Befragten in videoüberwachten Zügen sicherer“[138] und sind für einen verstärkten Einsatz.[139] In einem Jahr wurden von der Polizei ca. 140 Ansuchen auf Aushändigung der Videobänder gestellt. Die tatsächliche Erfolgsquote ist den ÖBB allerdings nicht bekannt.[140]

Bahnhofüberwachung durch Videokameras wurde Anfang Mai 2007 zum ersten Mal großflächig eingesetzt. Die überwachten Bahnhöfe sind u.a. Baden, Mödling, Linz, Graz, Leoben, Klagenfurt und Lienz.[141] Der Plan der ÖBB ist es bis 2011 in ganz Österreich 160 Bahnhöfe und 170 Garnituren („Talent“-Züge)[142] mit Überwachungsanlagen auszustatten.[143]

Der im Mai 2008 fertig gestellte Bahnhof am Prater soll laut Angaben bis zu 100 Kameras aufweisen. Thomas Berger, ein Sprecher der ÖBB, betont aber dennoch, dass die Videoüberwachung „nur als Teil des Sicherheitsgesamtpaketes gesehen werden [darf].“[144] Es ginge bei der Überwachung vielmehr um Abschreckung von Kriminellen.

Die folgende Abbildung ist eine Grafik mit den Kameras im Erdgeschoss des neuen Nordbahnhofes (Praterstern, Wien). Auffällig sind dabei nicht nur die vielen Kameras sondern auch, dass es keine Sitzbänke in der Wartehalle gibt.

---

[135] Austria Presse Agentur. „Ausbau der Videoüberwachung bei ÖBB“ *APA* (http://www.oebb.at/euro2008/de/Aktuell/2008/05/06/3207162881/index.jsp) (14.05.2008).
[136] Ebenda.
[137] „Was bringen Videoüberwachungen?“ *ORF.at* (http://oesterreich.orf.at/wien/stories/270105) (14.05.2008).
[138] Katja Blum (Pressesprecherin der ÖBB) in: „Videoüberwachung – Wiener Linien: ‚Vandalismus kommt nicht mehr vor'“ (25.07.2008) *Der Standard*. (http://derstandard.at/?id3234049) (13.05.2008).
[139] Ebenda.
[140] Austria Presse Agentur. 2008.
[141] ÖBB-Sprecher Nikolaus Käfer in: „ÖBB starten Videoüberwachung“ *Die Presse*. (01.05.2007).
[142] Austria Presse Agentur. 2008.
[143] „Was bringen Videoüberwachungen?“ *ORF.at* (http://oesterreich.orf.at/wien/stories/270105) (14.05.2008).
[144] Austria Presse Agentur. 2008.

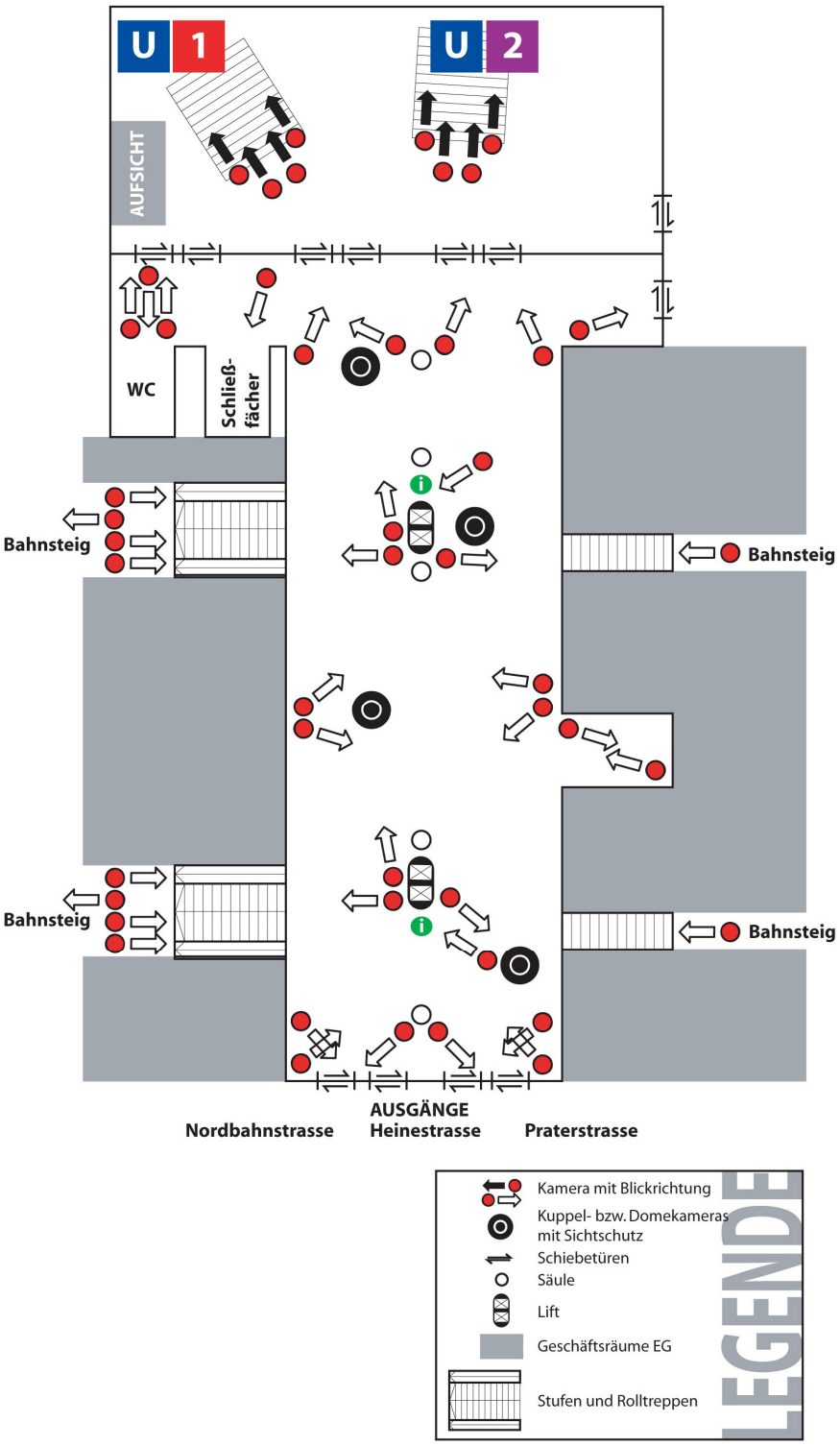


Abb.9: Grafik der Überwachungskameras in der Eingangshalle Nordbahnhof [*Grafik Fürst*]

4.3. Mistkübelüberwachung in Wien

In der Öffentlichkeit schlug der positive Bescheid zur Mistkübelüberwachung in Wien einigermaßen große Wellen, vor allem deswegen, weil die DSK der Kontrolle durch Videoüberwachung zugestimmt hat. Am 6. Februar 2008 wurde beschlossen, dem Antrag auf Videoüberwachung von Garagen, Liften und Müllräumen von Wiener Wohnen (Städtische Gemeindebauverwaltung Wien) stattzugeben. In den Gesprächen vor dem Antrag war von 15 Gemeindebauten die Rede. Nachdem die DSK aber mehr Unterlagen über Vandalismusschäden verlangte, wurden nur 8 Gemeindebauten beantragt und davon nur 7 bewilligt,[145] da „eine bestimmte Gefährdung nachzuweisen [ist].“[146] Die DSK will damit Vergleichsflächen schaffen und somit feststellen, ob

> „[...] Videoüberwachung überhaupt ein geeignetes Mittel zur Bekämpfung von Vandalismusschäden ist und daher der damit verbundene Eingriff in das Grundrecht auf Datenschutz gerechtfertigt ist.“[147]

Wiener Wohnen begründete den Antrag damit, dass Vandalismusvorfälle in Liften bzw. um Einbrüche in der Garage des Gemeindebaus reduziert werden soll. Außerdem soll damit auch der so genannte „Mülltourismus“ aus Niederösterreich eingedämmt werden.[148]
Wiener Wohnen legte dem Antrag eine Auflistung und Kosten der Schadensfälle der Jahre 2005 und 2006 bei. Die Dokumentation muss fortgeführt und am 31. Dezember 2009 vorgelegt werden. Bis zu diesem Termin wurde die Videoüberwachung zeitlich beschränkt. Diesen Bericht nimmt die DSK als Basis für die Entscheidung, ob die Videoüberwachung aufgrund mangelnder Resultate eingestellt wird, oder ob sie fortgesetzt und eventuell erweitert werden kann.
Den Anlagen wurden allerdings Einschränkungen gemacht insofern, als sie Hauseingänge und Stiegenhäuser nicht überwachen dürfen, da „diesbezüglich keine wesentlichen Schadensfälle im Antrag ausgewiesen waren.“[149] Garagen, Müllräume und Aufzüge wurden nur unter der Voraussetzung bewilligt, dass „keinesfalls Wohnungseingänge von der Videoüberwachung

[145] Marits, Mirjam: „ ‚Big Brother’: Gemeindebau-Videoüberwachung fix“ (18.02.2008) *Die Presse* (http://diepresse.com/home/panorama/oesterreich/363821/print.do) (07.04.2008).
[146] Waltraud Kotschy zit. in: Springer, Gudrun: „ ‚Kamera läuft’ in acht Wiener Gemeindebauten“ *Der Standard* (27.03.2008).
[147] „Bekanntmachung Wiener Wohnen“ (www.dsk.gv.at/Bekanntmachun_wienerwohnen.htm) *DSK.* (20.02.2008).
[148] „Das neue ‚Mist-TV’ im Gemeindebau.“ *Der Standard* (19.02.2008).
[149] (www.dsk.gv.at/Bekanntmachung_wienerwohnen.htm) (20.02.2008).

mit erfasst sein dürfen, da dies einen unverhältnismäßigen Eingriff in die Privatsphäre darstellen würde.“[150]

Die aufgezeichneten Daten werden nur kontrolliert, wenn von den Bewohnern Vandalenakte oder Einbrüche gemeldet werden, bzw. dürfen nur weitergegeben werden, falls eine „gesetzliche Verpflichtung zur Ausfolgung des Bildmaterials, z.B. an Strafverfolgungsbehörden, besteht.“[151] Den Mietern steht eine 24-Stunden Hotline zur Verfügung, bei der sie Beschwerden einbringen können. Um Missbrauch vorzubeugen sind ausschließlich 5 Personen von Wiener Wohnen dazu berechtigt, sich das Videomaterial anzusehen, und allenfalls der Polizei zu übermitteln. Die Daten dürfen 72 Stunden lang aufbewahrt werden. Wird in dieser Zeit ein Vorfall gemeldet, werden die Aufnahmen ausgewertet. Andernfalls werden sie nach Ablauf dieser Zeit gelöscht.[152] Um Missbrauch durch die Mitarbeiter vorzubeugen wird „genau dokumentiert wer wann Einsicht genommen hat.“[153] Dem SP-Wohnungsbaustadtrat Michael Ludwig geht es jedoch nicht nur um die Reduktion von Schadensfällen, sondern auch um die Kontrolle von „Angsträumen“.[154]

Die DSK hat den Antrag für die 7 Bauten genehmigt ohne jedoch weitere Angaben zu machen wie viele Kameras dort aufgestellt werden dürfen.[155]

Die Genehmigung erfolgte für diese Bauten:[156]

Lechnerstraße 2-4 (3. Bezirk)

Rosa-Hochmann-Ring 3 (11. Bezirk)

Am Hofgartl 3-7 sowie 8-10 (11. Bezirk)

Weiglgasse 8-10 (15. Bezirk)

Markgraf-Gerold-Gasse 18 (22. Bezirk)

Rennbahnweg 27 (22. Bezirk)

„Mieterecho“, eine Plattform die 2007 gegründet wurde, befürwortet den Einsatz von Videoüberwachung in den Gemeindebauten. Sie hofft, dass die Überwachung eine abschreckende Wirkung hat. Die Probleme, die diese Plattform allerdings jetzt schon sieht, ist die Kostenabwälzung auf die Mieter, sollte diese Überwachung auf alle Gemeindebauten

[150] (www.dsk.gv.at/Bekanntmachung_wienerwohnen.htm) (20.02.2008).
[151] Ebenda.
[152] „Das neue ‚Mist-TV’ im Gemeindebau.“ *Der Standard* (19.02.2008).
[153] Hanno Csisink (Ludwig-Sprecher). in: Marits. (25.03.2008).
[154] Ludwig, Martin. in: Springer. (27.03.2008).
[155] Springer. (27.03.2008).
[156] „Das neue ‚Mist-TV’ im Gemeindebau“ *Der Standard* (19.02.2008).

ausgedehnt werden.[157] Derzeit übernimmt die Stadt die Kosten von 400.000€ für die Überwachungsanlage.[158]

4.4. OGH-Urteile

4.4.1. Videoüberwachung im Mietshaus[159]

Das folgende Beispiel betrifft Videokameras in einem Mietshaus und wurde durch ein OGH-Urteil gelöst: Ein Mieter klagte die Hauseigentümerin da sie vor ihrer Wohnungstür eine Kamera installiert hatte, die auch den Eingang zu seiner Wohnung mitfilmte. Die Hauseigentümerin berief sich auf ihr Recht auf Eigenschutz, während der Kläger sich in seiner Privatsphäre verletzt fühlte. Der OGH entschied, dass ein berechtigtes Interesse des Bewohners besteht, beim Betreten und Verlassen seiner Wohnung nicht permanent überwacht zu werden. Der Hauseigentümerin wurde allerdings erlaubt neuralgische Punkte, wie z.B. die Hauseingangstür oder den Abgang zum Keller, mit Kameras zu versehen um das Recht auf Eigenschutz zu wahren.
In einer Erläuterung des § 16 ABGB, so wie auch vom OGH festgestellt wurde, ist es „einem Mieter zumutbar und dient seinem Schutz, dass jedenfalls der Eingang zu einem Miethaus durch Bewegungsmelder und Videokameras gesichert wird.“[160]

4.4.2. Kameraattrappe

Ein weiterer Fall betrifft die Aufstellung einer Kameraattrappe in einem Siedlungsgebiet:
Vom Balkon eines Privathauses aus wurde eine Kamera, die weder angeschlossen noch betriebsbereit war, auf den Nachbargarten gerichtet. Der Nachbar klagte und verlangte, dass die Kamera entweder entfernt oder so fixiert werde, damit sie seinen Garten nicht mitüberwacht. Der Beklagte verteidigte die aufgestellte Kamera mit dem Verdacht, dass die

[157] Marits. (25.03.2008).
[158] Hanno Csisink (Ludwig-Sprecher) in: Ebenda.
[159] Siehe: Kletečka, Andreas. in: ÖJK, 2006. S. 35 (OGH Entscheidung 6 Ob 2401/96y = SZ 70/18 =immolex 1997/71).
[160] Kletečka, Andreas. in: ÖJK, 2006. S. 34. *und*: Dittrich, Robert. *Taschenbuchkommentar ABGB*, Wien: Manz, 2005. S. 12 (Erläuterungen zum §16 ABGB).

Nachbarn Müll über den Zaun in seinen Garten werfen würden.[161] Sein Argument war nicht der Schutz vor „verbrecherischen Eindringlingen“[162], sondern er wollte seine Nachbarn abschrecken und ihnen ein Gefühl geben beobachtet zu sein. Der OGH kam hier zu dem Schluss, dass die Kamera, das Nachbargrundstück nicht mitfilmen darf. Dabei ist es egal, ob sie in Betrieb ist oder nicht, weil der Nachbar ja auch keine Möglichkeit zur Kontrolle hätte. Der OGH konstatiert auch, dass das Schutzbedürfnis von Siedlungshäusern nicht mit dem von Botschaften, Konsulaten oder Banken gleichzusetzen ist bei denen derartige Maßnahmen üblich sind.[163]

[161]Röhsner, Georg. „Schon eine Attrappe kann zu viel sein“ *Die Presse* (31.03.2008) (www.diepresse.com) (01.04.2008).
[162] Kletečka, Andreas. in: ÖJK, 2006. S. 37.
[163] Siehe: Ebenda. S. 37 (OGH Entscheidung 7 Ob 89/97g = JBl 1997, 641).

5. MANU LUKSCH

Die Künstlerin Manu Luksch, eine gebürtige Wienerin (1970), wanderte 1998 nach London aus. Dort gründete sie ein Jahr später mit ihrem Partner Mukul Patel die Plattform AmbientTV.net. Diese versteht sich als Plattform für unabhängige, interdisziplinäre Projekte die sich kritisch mit sozialer und technischer Infrastruktur auseinandersetzen vor allem in Bezug auf Datenaustausch, Privatheit und Überwachung[164] (Installationen, Dokumentationen, Tanz, Klang- und Videokompositionen und Live-Manipulationen[165]). Als Künstlerin**,** die „außerhalb des Rahmens und des gewohnten Umfeldes arbeitet“,[166] hat sie seit 2002 in mehreren Projekten versucht, Datenspuren nachzuverfolgen, die im alltäglichen Leben hinterlassen werden.[167] Das Ziel dieses Projektes war, jene zu beobachten, die uns beobachten („to watch those who watch us“[168]). In einem Projekt wurde der Versuch deutlich gemacht, in dem das Logo des TIA (*Total Information Awareness*) der DARPA (*US Defence Advanced Research Projects Agency*) der US Regierung, verändert wurde. Luksch gründete zu diesem Zweck das AIS (*Ambient Information Systems*) und ersetzte das Motto des ursprünglichen TIA Logos „Scientia est potentia“ („Wissen ist Macht“) durch „Quis custodiet ipsos custodes“ („Wer überwacht die Überwacher“). Diese veränderten Logos wurden auf T-Shirts gedruckt und verkauft.[169]

Abb.10: *Ambient Information Systems*.

[164] AmbientTV.net (http://ambienttv.net/content/?q=about) (10.10.2008).
[165] AmbientTV.net. (http://www.ambienttv.net/akha/vb/us.html) (14.05.2008).
[166] AmbientTV.net. (http://www.ambienttv.net/content/?q=manuluksch) (10.06.2008).
[167] Luksch, Manu/Patel, Mukul. “Faceless: Chasing the Data Shadow.” *AmbientTV.* (http://www.ambienttv.net/2007/faceless/chasingthedatashadow2007.pdf) (20.11.2007). S. 73.
[168] Ebenda.
[169] AmbientTV.net. (www.ambienttv.net/3/spyschool/5/index.html) (10.06.2008).

Mit einem weiteren Projekt, der Projektreihe *Spy School* (seit 2002), wurde der Grundstein für Lukschs Film *Faceless* gelegt.

> „*Faceless* is a CCTV science fiction fairy tale set in London, the city with the greatest density of surveillance cameras on Earth.“[170]

Dabei wurde der *Data Protection Act 98* (DPA)[171] praktisch getestet und die ersten Videomaterialien von CCTV-Kameras angefordert. Der DPA entspricht dem österreichischen Datenschutzgesetz (DSG 2000), ist aber in wichtigen Punkten, wie z.B. der Videoüberwachung, dem österreichischen Gesetz voraus. In Großbritannien ist aufgrund der enorm verbreiteten Anwendung von Videoüberwachung diese Regelung schon 1998 in das Datenschutzgesetz aufgenommen worden. Österreich hinkt dieser Situation noch hinterher, wird aber im Rahmen einer Gesetzesnovelle, die im Herbst 2008 kommen soll, nachziehen. Datenschützer kritisieren aber auch die Vorlage als immer noch unvollständig und nicht zeitgemäß.

5.1. Arbeitsweise von Manu Luksch

Das besondere Interesse von Manu Luksch liegt bei „‚moving' images“[172] und vor allem deren Entwicklung im digitalen, vernetzten Zeitalter. Charakteristisch für ihre Arbeit und Arbeitsweise sind die Überschreitung und Vermischung der Grenzen zwischen „linear and hypertextual narration“[173], zwischen Einzelarbeiten und multiplen Autorenschaften, postproduzierten und selbst generierenden Bildern.[174] Manu Lukschs Interesse als

[170] Luksch/Patel. 2007. S. 73.
[171] Der DPA ist das britische Datenschutzgesetz.
[172] AmbientTV.net. (www.ambienttv.net/content/?q=manuluksch). (28.04.08).
[173] AmbientTV.net. (http://www.ambienttv.net/content/?q=manuluksch) (28.04.2008). (Die Unterscheidung zwischen linearer und hypertextualer Erzählung ist jener, der zwischen dem Text eines Buches und dem einer Internetseite mit verschiedenen Links besteht. In letzterem kann sich der „Leser“ seine Geschichte selber zusammenstellen, d.h. er entscheidet selber über die Linearität. Ein solches Beispiel hat Manu Luksch in ihrem Projekt *Orchestra of Anxiety* verwirklicht. Als Instrument wurde eine Natodraht-Harfe hergestellt. Es wurde ein 2,5 Meter hoher Metallrahmen konstruiert und anstelle der Saiten wurde Natodraht eingezogen. Der Spieler zupft mit Metallhandschuhen und verlängerten Metallfingern die Saiten. Durch ein computergesteuertes Interface werden dadurch verschiedene akustische und visuelle Effekte ausgelöst. Siehe: Luksch, Manu: Einreichung Projekt 2007-1 Orchestra of Anxiety (http://netznetz.net/wiki/Einreichung_Projekt_2007-1_Orchestra_of_Anxiety) (28.04.2008).
[174] Siehe: (www.ambienttv.net/content/?q=manuluksch) (28.04.08). In der Aktion “Broadbandit Highway” hackte sich Manu Luksch in video-streams von Verkehrsüberwachungs-WebCams auf der ganzen Welt, stellte sie in einem 24 Stunden, 7 Tage die Woche, Road-Movie neu zusammen. „The live, self-generative version of Broadbandit Highway was online at www.ambienttv.net/broadbandit until the last traffic surveillance webcam

Filmemacherin konzentrierte sich vor allem auf CCTV-Überwachungsanlagen in London. Dies gilt vor allem in Bezug auf das Projekt *Spy School* und den Film *Faceless*. Zum einen weil sie sich mit Überwachung und der Situation als Bürger, als Person, als Individuum beschäftigt und zum anderen weil es ein Medium darstellt mit dem man als Künstler auch arbeiten kann.

Die Gesamtzahl an Kameras in Großbritannien beläuft sich auf vermutlich 4,2 Millionen, davon sind nur ca. 3 Millionen registriert, die restlichen 1,2 Millionen sind illegal. Mit einer geschätzten Anzahl von 500.000 Kameras gilt London als die am intensivsten überwachte Stadt weltweit. Man nimmt an, dass man bei einem Spaziergang durch London mindestens 300 Mal von einer CCTV-Kamera gefilmt wird.[175]

Die Regisseurin sah sich in London mit einer für sie eigenartigen Situation konfrontiert: Eine Überwachungskamera gegenüber ihrer Wohnung war so installiert, dass bei geöffneter Tür in die Wohnung gefilmt werden konnte. Aufgrund dieses beängstigenden Zustands begann sie sich mit der rechtlichen Situation von Überwachungskameras auseinanderzusetzen. Während ihrer Recherchen über den britischen DPA fand sie heraus, dass ein Bürger das Recht hat, in Informationen Einsicht zu nehmen die über ihn aufgezeichnet wurden und auf Wunsch auch eine Kopie verlangen kann.

Die Möglichkeit, vorhandene Kameras zu nutzen, nahm die Regisseurin schließlich zum Anlass, einen Film zu machen, der die Aufdringlichkeit und „Eindringlichkeit", sowie die Allgegenwärtigkeit der Überwachung durch Kameras bewusst werden lassen sollte. Durch die eigene Erfahrung und in Gesprächen mit Datenschützern und Aktionsgruppen kam ihr der Gedanke, dass man in einer Stadt, in die über so viele Kameras beinahe flächendeckend eingesehen wird, auf eine eigene Kamera verzichten könnte.[176]

---

from the original list of web addresses went offline. The movie was ongoing without repetition of sequences for about 5 years." AmbientTV.net. (http://www.ambienttv.net/2001/broadbandit/disturb/cam26.html). (15.05.2008).

[175] Threard, Yves. „Society under surveillance". (15.10.2007) *Le Figaro* (http://www.lefigaro.fr/debats/2006/11/08/01005-20061108ARTWWW90245-society_under_surveillance.php) (12.02.2008).

[176] Siehe: Manu Luksch in: Dax, Patrick: „Filme machen mit Überwachungskameras. Interview mit Manu Luksch." (03.05.2008) *Futurezone ORF.at* (.http://futurezone.orf.at/it/stories/275169/) (03.05.2008).

5.2. Spy School

Spy School ist eine durch die Anschläge auf die Twin Towers von 9/11 inspirierte Reihe von Aktionen und Workshops, die sich vor allem mit den Nachwirkungen dieser Anschläge beschäftigen. Damit sollte insbesondere die Aufmerksamkeit des Einzelnen geschärft werden wie stark die Überwachung schon fortgeschritten ist und wie wenig man selber über die tatsächliche, wie auch die rechtliche Situation, in der sich ein Bürger befindet, weiß. Mit *Spy School* wies Luksch auf die Überwachung durch Videokameras, Abhören von Telefongesprächen, Erhöhung der Sicherheitsstandards, etc. hin.

Spy School hat den DPA auf seine Tauglichkeit getestet: In diesem Projekt versuchte Manu Luksch zum ersten Mal an CCTV-Videos zu gelangen. Diese Versuche bildeten daraufhin die Grundlage für ihr *Manifesto for CCTV-Filmmakers*. Manu Luksch hat aufgrund der Informationen, die sie dem DPA entnommen hat, entdeckt, dass die Betreiberfirmen von CCTV-Anlagen, gesetzlich dazu verpflichtet sind, Kopien von Bändern herzustellen und zu versenden, wenn Betroffene sie schriftlich dazu auffordern.
Letztlich ging es Luksch um die rechtlichen Möglichkeiten, Kopien zu erlangen und zu erfahren, ob die gesetzlichen Auflagen von den „Videooperators" erfüllt werden bzw. wie kooperationsbereit die Firmen in dieser Hinsicht sind.

Der erste Teil von *Spy School* fand im Rahmen einer Party statt: Es wurden Informationen wiedergegeben, die sich laut der Beschreibung aus Telefongesprächen, Radiosendungen, geflüsterten Gesprächen und Videoüberwachung zusammensetzten –

> „Raiding the spectrum, The Spy School gathers information, throws it in to the mix, and sends it back out through the airwaves. Radio-talk, phone-talk, cctv, your whispered conversations and surreptitious glances, captured, reconfigured, rebroadcast. You'll hear yourself echoed on the soundtrack, find that your're dancing to your own projected image – you may arrive at the party to find you're already there. The Spy School infiltrates scenes with its human avatar, wired for sound and image and feeding the DJ and VJ with angles on the party-goers. And there's a performer on the floor, ranging through moves and masks – but no one's quite sure who's watching who."[177]

[177] AmbientTV.net. (www.ambienttv.net/3/spyschool/1/index.html). (24.05.2008).

Auf dieser Party wurde CCTV-Material (das von Luksch angefordert wurde und z.T. im Vorhinein choreographiert wurde) auf eine Leinwand projiziert, auf der auch die Partygäste zu sehen waren: Die Gäste wurden während ihres Besuches beobachtet, belauscht und gefilmt und versorgten somit DJ und VJ mit Live-Material. Damit sollte eine Beklommenheit unter den Partygästen geschaffen werden. Es sollte ein Bewusstsein dafür entstehen, dass sie jederzeit und an jedem Ort abgehört werden können, ohne zu wissen wer sie belauscht oder warum sie beobachtet werden.

Nachdem für die Regisseurin die rechtliche Komponente dieses Projekts im Vordergrund stand, traten die visuellen Charakteristika zunehmend in den Hintergrund. Der Interessensschwerpunkt wurde vom „Bildmaterial als Träger von rechtlichen Eigenschaften“[178] bestimmt, besonders deshalb weil das Gesetz diesen Film erst ermöglicht hat. Dieser Prozess wurde von der Fragestellung beeinflusst, die sich der rechtlichen Struktur unserer Gesellschaft annimmt:

> „Ich wollte die Frage stellen, was denn so ein Gesetz eigentlich wert ist. Gesetze symbolisieren, wie sich eine demokratische Gesellschaft arrangiert und Kompromisse formuliert. Es haben bestimmte Parteien Grund zu überwachen, und es haben Parteien, die überwacht werden, bestimmte Grundrechte. Man nimmt dann an, dass das über das Gesetz geregelt wird. Damit wird ja auch beschwichtigt. Mir geht es darum, zu zeigen, wie sehr die Gesetzeslage und das Bewusstsein der Situation der technologischen Realität unseres Alltags hinterherhinkt.“[179]

Das bedeutet, dass der Film nicht nur im Plot seine Kritik an das System richtet, sondern schon durch die Art des Material, wie es zustande gekommen und beschafft wurde, Kritik an der Situation ausübt.

[178] AmbientTV.net. (www.ambienttv.net/3/spyschool/1/index.html). (24.05.2008).
[179] Luksch/Patel. 2007. S. 74.

6. *Data Protection Act* (DPA)

6.1. *Codes of Conduct*

Die Möglichkeit an CCTV-Material heranzukommen, wurde gesetzlich durch eine Novelle des DPA 98 im Jahr 2001 ermöglicht. Diese Novelle basiert auf einer EU-Richtlinie, die festlegt, dass Informationen, die auf „systematische Art über ihn [den Bürger; *Anm. Fürst*] aufbewahrt werden, "[180] demselben auch zugänglich gemacht werden müssen. Dabei sind die *Human Rights (EMRK)*, Privat- und Strafrecht als Grundlagen sowie der *Code of Practice*[181] (als eine nicht verpflichtende) Richtlinie anzunehmen. Der *Code of Practice* hält fest, wie sich die Rechte und Pflichten von CCTV-Betreibern allgemein und im Falle von polizeilichen Ermittlungen gestalten. Die Überwachungsanlagen werden ja nicht nur von staatlichen Behörden geführt, sondern sehr oft von privaten Firmen. Um dem Wildwuchs von CCTV-Systemen eine Richtlinie zu geben, wurde der *Code of Practice* installiert. Darin ist vorgeschlagen, Aufzeichnungen über die Handhabung mit dem jeweiligen Material zu führen, sozusagen eine Art Buchführung, wie sie auch von Dr. Andreas Kletečka gefordert wurde (siehe: S. 37).

In Österreich gibt es eine derartige Grundlage nicht, da der Einsatz von Videoüberwachung noch nicht einmal im Datenschutzgesetz geregelt ist.[182] Firmen können sich freiwillig den Regeln der *Codes of Conduct* verpflichten, dafür erhalten sie im Gegenzug „Erleichterung bei den Meldeverfahren [...] und bei internationalen Datentransfers."[183]: Nachdem im Europäischen Binnenmarkt 25 durchaus unterschiedliche Datenschutzgesetze zum Einsatz kommen, „fordern große Konzerne seit einigen Jahren eine verstärkte Selbstregulierung im Datenschutz."[184] Das bedeutet, dass sie die Regeln des Datenschutzes mehr oder weniger selbst bestimmen können und damit auch die jeweiligen Datenschutzkommissionen umgehen können.

---

[180] Dax. 2008.
[181] *Code of Practice* (Version 2008): (http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf) (24.04.2008).
[182] Im Herbst 2008 soll ein Antrag bezüglich einer DSG 2000 Novelle eingebracht werden, der auch einen Paragraphen für die Verwendung von Videoüberwachung ins DSG beinhaltet.
[183] Ebenda.
[184] Knyrim, Rainer. „5 Jahre Datenschutzrecht in Österreich. Bestandsaufnahme und Lösungsansätze für aktuelle Probleme. *Medien und Recht*. 7/2005. S. 419.

„Ein Ansatz [für die Selbstregulierung; *Anm. Fürst*] sind die ‚*Codes of Conduct'*, mit denen der Gedanke eines einheitlichen europäischen Datenschutzrechts verwirklicht werden soll."[185] Dies geschieht um den konzernweiten Austausch zu erleichtern bzw. Informationen mit Geschäftspartnern auf der gleichen Ebene führen zu können, ohne dafür die eventuell strengeren Richtlinien eines Partnerkonzerns in einem anderen Land übernehmen zu müssen.

6.2. *Code of Practice* (COP)

Der *Code of Practice* (COP) wird vom *Information Commissioner's Office* (ICO – entspricht der DSK) herausgegeben. Damit ist keine gesetzliche Verpflichtung für Betreiber von CCTV-Anlagen verbunden. Er stellt eine Anleitung und Richtlinie für jene dar, die eine CCTV-Anlage installieren wollen. Im COP wird aber auch gewarnt, dass bei Abweichungen von diesem Code, obwohl er rechtlich nicht bindend ist, erhöhtes Risiko besteht, gegen das Gesetz zu verstoßen. Dabei bringt er nicht nur die gesetzlichen Richtlinien mit ein, sondern gibt auch Überlegungen und Denkanstösse, ob eine Anlage errichtet werden soll, wie sie geführt werden und welchem Zweck sie dienen soll. Ebenso wird die Frage gestellt, ob die Notwendigkeit, eine CCTV-Anlage zu errichten wirklich besteht. Das ICO versucht dabei auf andere Schutz- und Sicherungsmöglichkeiten hinzuweisen („You should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals."[186]). Den einzelnen Kapiteln werden zu den betreffenden Themen Fragenkataloge hinzugefügt.

Der COP an sich deckt die Verwendung von CCTV-Anlagen und solchen Systemen ab, die Bilder zur Personenidentifikation liefern[187] und ist primär auf Organisationen, Firmen und Geschäfte als Anwender ausgelegt. Mobil-Telefone und Digitalkameras werden weder vom DPA, noch vom COP erfasst, ebenso wenig wie private Filmaufnahmen oder Attrappen.[188]

Die Anwendungen von CCTV-Kameras müssen jährlich gemeldet und registriert werden. Damit sollen Überlegungen verbunden sein, die den Denkprozess über die Notwendigkeit des

[185] Weichert, Thilo. zit in: Knyrim. 2005. S. 419.
[186] *Code of Practice*. (http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf) (24.04.2008). S. 6.
[187] Siehe: Ebenda. S. 5.
[188] Ebenda. S. 5.

Systems anregen sollen.[189] Im günstigsten Fall werden die Anlagen stillgelegt, oder aber sie laufen als illegale Anwendung weiter. Der Versuch, über eine bürokratische Hürde die Anzahl der Überwachungskameras zu reduzieren, funktioniert allerdings nicht.
Besondere Aufmerksamkeit kommt hier der Aufbewahrungspflicht zu: In Österreich ist die „Standard-Löschungsfrist" bei meist 48 Stunden angesetzt. In Großbritannien hat der Bürger das Recht, innerhalb von 40 Tagen Anspruch zu erheben, in Daten einzusehen.

7. Materialsammlung

Der Gesetzestext des DPA hält fest, dass CCTV-Material angefordert werden kann und wie es einzufordern ist: Ein Betroffener sendet innerhalb von 40 Tagen der Aufzeichnung eine schriftliche Anfrage, einen so genannten *subject access letter*, an jene Betreiberfirma, die Daten über die Person aufgezeichnet hat. Die Firmen sind verpflichtet die Aufzeichnungen zu kopieren, Dritte zu löschen und dem Antragsteller eine Kopie zuzusenden. Kameras müssen so gekennzeichnet sein, dass sie dem Bürger die Möglichkeit geben, sich an die Betreiberfirmen wenden um in diese Daten einsehen zu können.
Luksch stieß allerdings kontinuierlich auf Widerstand, als sie versuchte an Kopien zu gelangen. Viele Betreiber von Überwachungsanlagen ignorierten ihre Anfrage bzw. wiesen sie ab, zum einen, weil sie von dieser Verpflichtung tatsächlich nichts wussten und zum anderen weil sie es auch nicht wissen wollten. Solche Anfragen verursachen allerdings nicht nur zusätzlichen Personalaufwand. Die Kosten für die Unkenntlichmachung anderer Personen müssen von der Betreiberfirma übernommen werden. Demjenigen, der die Bänder anfordert, dürfen laut DPA maximal 10£ verrechnet werden.
Vor allem kleinere Firmen, wie Bäder und Trafiken, mussten durch zusätzliche Verweise auf den Gesetzestext auf ihre Verpflichtung (auf schriftliche Anfragen hin Kopien der Videos zu erstellen und zu senden) hingewiesen werden. Manu Luksch führt in ihrem *Manifesto for CCTV Filmmakers* auch die einzelnen Passagen aus dem Gesetzestext an und empfiehlt diese Passagen dezidiert anzuführen, wenn ein *subject access letter* (schriftliche Anfrage)versendet wird. Der COP konstatiert zwar, dass die Dauer der Aufbewahrungspflicht im DPA nicht eindeutig angegeben ist, sie ergibt sich allerdings aus dem Recht, dass der Betroffene ausüben

[189] Siehe: *Code of Practice*. S. 8

kann, nämlich Einsicht nehmen bzw. eine Kopie zu verlangen. Daraus ergibt sich eine Mindestaufbewahrungszeit von 40 Tagen, in denen die schriftliche Anfrage zu erfolgen hat.

> „Individuals whose images are recorded have the right to view images of themselves and, unless they agree otherwise, to be provided with a copy of the images. This must be provided within 40 calender days of receiving a request. You may charge a fee of up to £10 (this is the current statutory maximum set by Parliament)."[190]

In Österreich gibt es zurzeit eine Löschungspflicht für Aufnahmen von Überwachungskameras, die von der DSK in einem Bescheid dem Antragsteller vorgibt. Die Wiener Linien dürfen z.B. Material bis zu 48 Stunden lang speichern, danach muss es gelöscht werden.

Der *subject access letter* sollte, um einen einigermaßen reibungslosen Ablauf sicher zu stellen, laut *Manifesto* folgende Informationen enthalten:

- Datum, Zeit und Ort des Aufenthaltes im Sichtfeld einer CCTV-Anlage
- Foto (evtl. mit Kleidung, die zum Zeitpunkt der Datenaufzeichnung getragen wurde)
- evtl. eine Personenbeschreibung.

Der COP formuliert es auf diese Weise:

> „Those who request access must provide you with details which allow you to identify them as the subject of the images and also to locate the images on your system."[191]

Ein Beispiel für eine Anfrage gibt Luksch in ihrem Artikel für das *Goodbye Privacy Festival* der Ars Electronica an:

> „I wish to apply, under the Data Protection Act, for any and all CCTV images of my Person held within your system. I was present at (place) from approximately (time) onwards on (date).
> *(from the template for 'subject access requests' used for Faceless)*"[192]

[190] *Code of Practice*. S. 15.
[191] Ebenda. S. 16.
[192] Luksch/Patel. 2007. S. 73.

7.1. Rückmeldungen

Der Regisseurin ging es nicht nur darum den Film *Faceless* zu schaffen, sondern den Gesetzestextes einer praktischen Untersuchung zu unterziehen. Damit sollten Grenzen im DPA sichtbar gemacht und seine Lücken aufgedeckt werden. Wie schon erwähnt, wurden nicht alle Anfragen positiv beantwortet. Negative Rückmeldungen auf Bildanfragen wurden mit unterschiedlichen Ausreden zurückgesendet: Entweder waren die CCTV-Systeme angeblich nicht in Betrieb oder nicht funktionstüchtig.

> „I can confirm there are no such recordings of yourself from that date, our recording system was not working at that time. (11/2003)"[193]

Manchmal wurde Material mit der Argument verweigert, es könne aufgrund „menschlichen Versagens" nicht ausgehändigt werden.

> „As I had advised you in my previous letter, a request was made to remove the tape and for it not to be destroyed. Unhappily this request was not carried out and the tape was wiped according with the standard tape retention policy employed by (*deleted*). Please accept my apologies for this and assurance that steps have been taken to ensure a similar mistake does not happen again. (10/2003)"[194]

Es konnte auch passieren, dass die schlechte Qualität der Bilder als Ablehnungsgrund genannt wurde bzw. so viele Menschen auf den Bildern waren, dass die Person der Regisseurin (Anfragestellende) nicht erkennbar war. Bei vielen Absagen wurde auch auf technische Gebrechen und vorzeitige Löschung verwiesen. Lukschs Arbeit, das Gesetz zu testen, ist zusätzlich durch eine bestimmte Rückmeldung auf eine Anfrage bekräftigt worden: Es wurde entdeckt, dass seit 2 Jahren installierte Kameras entweder nicht in Betrieb genommen waren oder nie funktioniert hatten.[195]

> „Upon receipt of your letter [...] enclosing the required £10 fee, I have been sourcing a company who would edit these tapes to preserve the privacy of other individuals who had not consented to disclosure. […] I was informed […] that all tapes on site were blank. [...W]hen the engineer was called he confirmed that the machine had not been working since installation.

[193] Luksch/Patel. 2007. S. 74.
[194] Ebenda. S. 75.
[195] Diskussion im Top Kino (04.05.2008). Manu Luksch, Hans Zeger (Arge-Daten), Doris Kaiserreiner (Quintessenz). Moderation: Ingrid Brodnig (Falter).

> Unfortunately there is nothing further that can be done regarding the tapes, and I can only apologise for all the inconvenience you have been caused. (11/2003)"[196]

Davon ausgehend lässt sich schließen, dass viele der installierten Kameras nicht funktionstüchtig sind bzw. die Wirkung der Kameras auf einem Abschreckungseffekt beruht.[197] Es wurde schon erwähnt, dass die Verpflichtung der Übersendung einer Kopie besteht. Weiterführend bedeutet das auch, dass die Funktionstüchtigkeit der Kamera und des Systems sicher zu stellen ist. Werden Anfragen also aufgrund von qualitativ schlechtem Bildmaterial abgewiesen, ist dieser Zustand gesetzeswidrig.

Insgesamt wurden nur ungefähr 7% der von der Regisseurin gestellten Anfragen positiv beantwortet.[198] Die Gründe dafür wurden schon erwähnt und lagen laut Auskunft der Betreiberfirmen an technischem wie auch menschlichem Versagen. Betroffene die auf dem Material zu sehen waren, außer der Regisseurin, mussten von den Betreiberfirmen unkenntlich gemacht werden. Dies fand hauptsächlich durch Ausschwärzen von Gesichtern statt. Diese Eingriffe sind sehr kostspielig, deshalb wurde auch versucht, der Anfragenden die Kosten zu verrechnen bzw. wurden die Kosten als Grund vorgeschoben, dem *subject access letter* nicht Folge zu leisten. Größere Firmen, wie z.B. Banken, verweigerten der Regisseurin die Aushändigung von Material, die durch ein, wie Luksch es nennt, gesetzliches „Schlupfloch" begründet wurden:

> „I should point out that we reserve the right, in accordance with Section 8(2) of the Data Protection Act, not to provide you with copies of the information requested if to do so would take „disproportionate effort". (12/2004)"[199]

Banken kann man allerdings zugute halten, dem Kunden gegenüber verpflichtet zu sein, eine erhöhte Wahrung bezüglich der Achtung der Privatsphäre sicher zu stellen.

Wie der „unverhältnismäßige Aufwand" ausgelegt wird, liegt aber an und für sich bei den Firmen selbst, die die Kosten für die Anonymisierung von Dritten natürlich miteinberechnen müssen. Die Überwachungsfirma muss dafür aufkommen, nachdem diese Kosten nicht auf den Anforderer abgewälzt werden können. Es darf dem Betroffenen hierfür eine maximale Kostenentschädigung von £10 verrechnet werden.

---

[196] Luksch/Patel. 2007. S. 75.
[197] Dax. 2008.
[198] Siehe: Ebenda. Daraufhin angesprochen wie viele Briefe sie gesendet habe, konnte die Regisseurin allerdings keine genaue Zahl nennen. Disskussion im Top Kino (04.05.2008).).
[199] Luksch/Patel. 2007. S. 76.

An einem besonderen Beispiel, das Luksch auch immer wieder „anerkennend“ in Vorträgen erwähnt und hervorhebt, kann man die unterschiedlichen Auffassungen von „unverhältnismäßigem Aufwand“ erkennen: Eine Firma hatte diesen Aufwand und die Mühen (des Personals) nicht gescheut, indem auf mehreren hundert auf Papier ausgedruckten Foto-Stills die Anonymisierung auf besondere eifrige Art und Weise vorgenommen wurde, denn ähnlich wie in den Anfängen des Films als die einzelnen Frames noch händisch koloriert wurden und die Zensur auch zur Schere griff, wurden auf den Stills/Frames die Manu Luksch zugesandt bekam die Gesichter Dritter händisch mit einer Nagelschere ausgeschnitten bzw. zensuriert.[200]

Abb.11: *Faceless*: TC: 29:53. (©Amour Fou)[201]

Abb.12: *Faceless*. TC 30:00. (©Amour Fou)

[200] Luksch/Patel. 2007. S. 76

[201] „Faceless“ - ein Film von Manu Luksch (c) Amour Fou Filmproduktion / Ambient Information Systems 2007. Sämtliche Film-Stills unterliegen dem Copyright von Amour Fou.

Durch den Fall *Durant vs. Financial Service Authority*[202] 2003 wurde der Begriff „personal data“ neu definiert. Da das britische Recht auf Präzedenzfällen aufbaut, erschwerte die Entscheidung des Gerichts die Material-Sammlung erheblich. Es genügte nicht mehr, nur von den Kameras erfasst zu werden. Es musste mittlerweile Information „of a ‚biographical nature'“[203] gegeben sein, um das Recht auf eine Kopie erwirken zu können. Für die Betreiber von Überwachungskameras änderte sich wenig. Für die Betroffenen wurde die bürokratische Hürde, von seinem Recht gebrauch zu machen, erhöht. Bei einer Diskussion deutete Manu Luksch an, dass der Film *Faceless* in seiner jetzigen Form nicht zustande gekommen wäre, wenn dieses Gesetz früher als 2003 in Kraft getreten wäre.[204]

7.2. Weitergabe von Bildmaterial

Der *Code of Practice* gibt Betroffenen das Recht auf Material bzw. Kopien, sofern sie durch eine schriftliche Anfrage (*subject access letter*) angefordert werden. Die Weitergabe von Bildmaterial an Medien ist allerdings verboten. Die Polizei kann dieses Material allerdings verlangen.

> „[...] but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet. Images can be released to the media for identification purposes; this should not generally be done by anyone other than a law enforcement agency.“[205]

Überwachungsvideos sollten auf Anraten des COP also nur von der Polizei, weitergegeben werden. Sicherheitsbehörden können diese Bilder zum Zweck der Personenidentifikation

[202] Mr. Smith klagte seinen Arbeitgeber Barclay (Finanzdienstleister). Die Klage wurde abgewiesen. Daraufhin wollte Mr. Durrant[!] seinerseits Informationen über einen Antrag des DPAs über den Kläger bei der Financial Service Authority einholen. Dieser Antrag wurde beim Berufungsgericht mit der Begründung der Irreführung abgewiesen („a misguided attempt to use the machinery of the DPA. […] Data only falls within the scope of the DPA where the information is biographical in a significant sense, where it has the individual as its focus and that the personal data is information that affects the privacy of the individual, either in a professional, or business capacity.“). Siehe: Glotel. (http://www.glotel.com/content_dynamic/display_news.asp?id=357&session_id=%7B475418E6-B310-410F-9A92-EF1B0424B173%7D). (1.10.2008).

[203] Ebenda. S. 77. (Dieser Begriff beinhaltet die medinzinischen Daten, Einkommen, Steuerpflicht, Bankinformationen und Informationen sonstiger Ausgaben von Bürgern.) Siehe: Glotel. Glotel Plc. (http://www.glotel.com/content_dynamic/display_news.asp?id=357&session_id=%7B475418E6-B310-410F-9A92-EF1B0424B173%7D). (1.10.2008).

[204] Diskussion im Top Kino (04.05.2008)

[205] *Code of Practice*. S. 13

allerdings an die Medien senden. Den Betreibern ist nicht gestattet „Versteckte Kamera“ zu spielen und die „Hoppalas“ zu Unterhaltungszwecken an die Medien zu senden.

7.3. Materialqualität

Nachdem in Großbritannien die Videoüberwachung schon seit 25 Jahren eingesetzt wird, ist auch anzunehmen, dass sich die Technik nicht immer auf dem neuesten Stand befindet. Dadurch ergeben sich auch Differenzen in der Qualität des Materials: Die Videos wurden zum Teil auf VHS-Kassetten geliefert, einige auf CDs und in einem Fall sogar als auf Papier ausgedruckte Stills.[206]

Die Regisseurin kommentiert auch die schlechte Bildqualität: Durch die veraltete Technik, die immer noch zum Einsatz kommt und wenig gewartete Anlagen, können Personen zum Teil nicht eindeutig identifiziert werden. Dieser Zustand ist positiv, insofern als die Überwachung nicht funktioniert, aber auch negativ aufzufassen, da die Kameras trotzdem nicht entfernt werden. Ob eine Kamera funktioniert oder nicht, ist dem Betroffenen nicht bewusst – er fühlt sich somit auch von einer Attrappe beobachtet. Hierbei drängt sich natürlich die Frage auf, warum diese Anlagen nicht abmontiert werden.

> „Die Bildqualität war generell eher schlecht. Bei manchen Aufnahmen hat es so ausgesehen, als ob Taubenkacke auf der Linse war. Die Kameras wurden wahrscheinlich seit Jahren nicht gewartet. Bilder von neueren Systemen waren hingegen kristallklar.“[207]

Ein Zuseher stellte der Regisseurin nach einer Vorstellung sogar die Frage, ob denn dieser „nostalgic look” bewusst verwendet wurde.[208]

Dabei stellt sich dann die Frage, ob der Zweck eines Videoüberwachungssystem überhaupt noch gegeben ist, wenn es nicht funktioniert. Des Weiteren ist es eine gesetzliche Verpflichtung und ist ebenso im DPA festgehalten, dass installierte Kameras eigentlich zu funktionieren haben:

[206] Siehe: Dax. 2008.
[207] Ebenda.
[208] Siehe: Ebenda. S. 4.

> „Many data requests had negative outcomes because either the surveillance camera, or the recorder, or the entire CCTV system in question was not operational. Such a situation constitutes an illegal use of CCTV: the law demands that operators comply with the DPA by making sure […] equipment works properly. (CCTV Systems and the Data Protection Act 1998)"[209]

Nachdem dies nicht immer der Fall ist, läst sich also auch in Großbritannien auf mangelnde Kontrollausübung der britischen Datenschutzbehörde schließen. Ein Problem das sich zusätzlich ergibt ist, dass auch Attrappen disziplinierenden Effekt haben. Der Betroffene hat im Normalfall ja keine Möglichkeit festzustellen, ob die Kamera funktioniert oder nicht.

> „The view of the camera's eye is expected to be felt by the subjects regardless of the operation or even the existence of a CCTV system."[210]

8. *Faceless*

In den vier Jahren des Datensammelns wurde klar, dass sich ein „normales", im Vorhinein geschriebenes Drehbuch in einem kontinuierlichen Prozess des Umschreibens und Anpassens befinden würde. Das war dem Zustand zuzuschreiben, dass einige der Bänder und Kopien von geplanten und durchgeführten Szenen aus schon genannten Gründen nicht erhältlich waren.
Abgesehen von Manu Luksch, mussten sämtliche anderen Personen die auf den Videoaufnahmen zu sehen waren, aufgrund des DPAs, von den Betreiberfirmen unkenntlich gemacht werden. Ausschließlich Manu Luksch forderte für dieses Projekt Material an, deshalb blieb sie in *Faceless* auch die Einzige deren Gesicht zu erkennen ist. Aus dieser Tatsache heraus entstand letztendlich (und zwangsläufig) auch die Idee einer „gesichtslosen" Welt.[211] Der Titel und ein Großteil der Idee des Drehbuchs sind davon abgeleitet. Die CCTV-Operatoren hatten bei Aushändigung des Materials zwar die Gesichter Dritter ausgelöscht, den Timecode aber mitkopiert. Der Timecode muss bei jeder Kamera mitlaufen. Das Kamerabild wird mit der Aufnahmezeit (Uhrzeit) synchronisiert. Damit werden Ort und Zeit kontrolliert und Bilder können einem exakten „Datum" zugeordnet werden (WER, WO und WANN). In den Kopien die Manu Luksch erhalten hat, war nicht nur der Timecode der

[209] Luksch/Patel. 2007. S. 74
[210] Hempel/Töpfer. 2004. S. 19.
[211] Luksch/Patel. 2007. S. 73.

Kamera mitkopiert worden, sondern in manchen Fällen auch der Timecode der Kopiermaschine. Die Zahlen sind zu einem bestimmenden Teil des Bildes geworden.

Abb.13: *Faceless*. TC: 10:15. (©Amour Fou).

Das Prinzip des Filmes basiert auf dem Austausch des Filmteams gegen Datenkontrolleure: Die Kameras wurden gegen das CCTV-System ausgetauscht, der Kameramann durch den Videooperator, der Script-Writer durch einen Anwalt, und das Script selbst durch das Gesetz.[212] Durch ihre Arbeit an den Projekten von *Spy School* erarbeitete sie eine Anleitung (*Manifesto for CCTV-Filmmakers*) für Regisseure die ihrer Idee folgen wollen. Dazu gehören Informationen wie z.B. nur CCTV-Systeme zu verwenden die auch unter den DPA fallen.[213] Die Ausnahmen wurden in einem negativen Anforderungsbescheid folgendermaßen definiert:

> „[…] our CCTV system is no longer covered by the DPA [because] we:
> -only have a couple of cameras
> -cannot move them remotely
> -just record on video whatever the cameras pick up
> -only give the recorded images to the police to investigate an incident on our premises (05/2004)"[214]

Die Aufnahmen kamen nicht in chronologischer Reihenfolge zustande. Das bedeutet, dass der Timecode in den verschiedenen Einstellungen nicht kontinuierlich abläuft, sondern Zeitsprünge (Jahr, Monat, Tag, Uhrzeit) aufweist. Nachdem der Timecode in den Bilder meist sehr prominent ist (siehe Abb.13), stellte dies die Regisseurin vor ein „zeitliches" Problem:

[212] Siehe: AmbientTV.net. (www.ambienttv.net/content/?q=node/426). (05.05.2008).
[213] CCTV-Systeme sind Kameraverbände ab einer bestimmten Größe. Einzelne Kameras gelten nicht als CCTV-System und fallen daher auch nicht unter den DPA.
[214] Luksch/Patel. 2007. S. 77.

Luksch hatte sich beim Schnitt für den Film vorwiegend mit der Story auseinandergesetzt und war nach stunden- und tagelangen Materialscreenings für den Timecode in den Aufnahmen „blind“ geworden. In den Testscreenings wurde den Timecodes allerdings mehr Bedeutung zugemessen und es wurde ein tieferer Sinn dahinter vermutet, als von der Regisseurin beabsichtigt war. Zu diesem Zweck konstruierte sie für den Film eine eigene Zeit: *RealTime*.

> „In the luminous world of the new machine each moment of time saturates each consciousness. **There is no memory, no anticipation. There is no past, so there can be no guilt or regret, and no future, therefore no anxiety or fear.** [*Herv. Fürst*] RealTime, the perfect and perpetual present is the heartbeat of the healthy universe.“[215]

RealTime entstand, um den variierenden Timecode eine neue Rolle zu verleihen bzw. die originale Bedeutung, Ort und Zeit miteinander zu verbinden, auszulöschen. Dem Timecode sollten sehr wohl eine diegetische Rolle zukommen, allerdings in einem arbiträren Format, verschlüsselt wenn man so will. Das kann man in vielen anderen (Science-Fiction) Filmen beobachten, wenn jemand über eine Kamera verfolgt wird. Dass der Timecode dabei immer im Bild ist, verstärkt das Gefühl des Beobachtet-Seins der Protagonistin, und versetzt den Blick des Zusehers in den des Beobachters – des Videooperators.

Der Verlust der Vergangenheit und der Zukunft zugunsten einer „perfekten Gegenwart“ führt zum Verlust der Identität der Bewohner. Die Gesellschaft wird von der *New Machine* reguliert, dem Takt der Maschine angeglichen und der Norm unterworfen.

Für Luksch war es wichtig, herauszuarbeiten, dass es nicht mehr nur um die Kontrolle des Raumes geht.[216] Wenn die Zeit nicht mehr erfahrbar ist, kann sich auch keine Persönlichkeit entwickeln.[217] Deshalb haben die Figuren in *Faceless* keine Geschichte und kein Gesicht, weil sie in der *RealTime* gefangen sind als Sklaven der „perfekten und ewigen Gegenwart“.

> „The film plays in an eerily familiar city, where the reformed RealTime calendar has dispensed with the past and the future, freeing citizens from guilt and regret, anxiety and fear. Without memory or anticipation, faces have become vestigial – the

[215] *Faceless*. TC: 11:00-13:00..
[216] Walter Peissl unterscheidet zwischen „Kontrolle“ und „Überwachung“. „Kontrolle“ ist der Abgleich zwischen einem „Ist-Wert“ und einem normgebenden „Soll-Wert“. „Überwachung betont zusätzlich den zeitlichen Aspekt. Überwachung kann als Abfolge von Kontrollakten verstanden werden.“ Das bedeutet, dass der Zeitfaktor für die Überwachung eine besondere Bedeutung besitzt. (Peissl, Walter. Überwachung und Sicherheit: Eine Fragwürdige Beziehung. S. 81. in: Nentwich/ Peissl (Hg.). Technikfolgenabschätzung in der österreichsichen Praxis. Verlag der Österreichischen Akademie der Wissenschaften, Wien: 2005. (S. 73-90).
[217] Manu Luksch: Diskussion im Top Kino (04.05.2008).

> population is literally faceless. Unimaginable happiness abounds – until a woman recovers her face…"[218]

Der Film *Faceless* hat nur eine Protagonistin (Manu Luksch) die Gefangene dieser Zeit ist. Es wurden Zukunft, Gegenwart und Vergangenheit ersetzt, durch die „perfekte Zeit" – *RealTime*. Mit der Auslöschung der Zeit gehen sowohl die Emotionen verloren, als auch die Individualität des Einzelnen, der dadurch sein Gesicht verliert. Es wird eine Norm etabliert, die jede Abweichung von Aufsehern verfolgen und korrigieren lässt. Die Abnorm ein Gesicht zu haben ist strafbar. Die Protagonistin selbst ist eine jener Personen die Datenströme für die Maschine analysieren. In ihren Träumen bricht sie aus der *RealTime* aus – sie weicht ab. Als sie ihr Gesicht entdeckt, bastelt sie sich eine Maske um es wieder zu verdecken. Es fällt ihr schwer, diese Abweichung zu akzeptieren und diese Situation treibt die Handlung voran. Durch einen Brief wird sie aufgefordert ihren Träumen und Gefühlen, abnormen Dingen in ihrer Welt, zu folgen.

Die Bilder im Film laufen stakkatoartig ab, (ähnlich wie die abgefilmten Fotografien in *La Jetée* – siehe unten) sie „fließen" nicht. Bildstörungen, Flimmern und Verzerrungen markieren Szenen- und Kamerawechsel. Abgesehen von der unterschiedlichen Qualität der Bilder, umfasst das Farbspektrum des Materials monochrome, farbige, als auch von der Regisseurin nachgefärbte Bilder.
Unterschiedlichen Personengruppen differenzieren sich durch die verschiedenen Formen der „Ausschwärzungen" (Masken), die Manu Luksch im Nachhinein zusätzlich vorgenommen hatte: Die „Aufseher der Maschine" werden durch schwarze rechteckige Masken verdeckt, „normale Bürger" (wie Luksch selbst zu Beginn und am Ende des Filmes) haben ovale Masken (Schwarzschattierungen) und die „spectral children", die nicht von der Maschine synchronisiert wurden, haben bunte Masken.
Sämtliche Szenen und Einstellungen sind mit dem Timecode der CCTV-Kameras versehen, die auch im Bild zu sehen sind. Die Protagonistin bricht mehrmals aus der *RealTime* aus und träumt. Die Träume der Protagonistin (*flashforwards*) zeigen nie das ganze Bild, und auch nie einen Timecode. Sie sind durch Kameramasken (in der Postproduktion) verdeckt. Der einzige „Zeit-Raum" in dem keine Datenaufzeichnung in diesem Sinne erfolgt ist jener in ihren Träumen.

[218] Luksch/Patel. 2007. S. 74.

Nachdem keine eigene Kamera verwendet wurde, ist die mise-en-scene ohne zusätzliche Requisiten oder Beleuchtung ausgestattet. Ein Film-Set gab es nicht. Die Einstellungen sind an die Kamera gebunden: In einigen wenigen Fällen war die Kamera beinahe auf Augenhöhe (je nach Raumhöhe), die meiste Zeit allerdings befand sie sich in einer Vogelperspektive (*God's Eye View*). Damit verbunden bedeutet das auch, dass die meisten Bilder in einer Totalen sind. Die Bilder selber sind starr. Bewegung oder Zoom kommen nur durch Montage im Bild zustande, d.h. es wird ein nur Bildausschnitt gezeigt. Der Schwenk/Zoom geschieht im Bild selbst.

Der Timecode wirkt als Variable eines nicht näher zu bestimmenden Zeitablaufes. Er dient als Variable für die ständig mitlaufenden Symbole der Kontrolle, die Zeit und Ort des Geschehens festhalten.

In *Faceless* wird der Plot von einer auktorialen Stimme wie bei Chris Marker begleitet.[219] Die Stimme der Erzählerin nimmt in *Faceless* allerdings eine undurchschaubare Stellung ein. Sie ist nicht an eine festgelegte Erzählposition gebunden. Anders hingegen bei Marker, bei dem sich die Stimme des *voice-overs* von Anfang an allwissend präsentiert („omniscient narrator").

Der Film braucht die Narration um das Geschehen zu kommentieren, da die Bilder sonst nicht verständlich wären. Ein Passant, der in Wirklichkeit mit einem Zettel in der Hand nach dem Weg fragte, wurde durch das *voice-over* im Film zu einem Aufseher mit Pistole.[220]

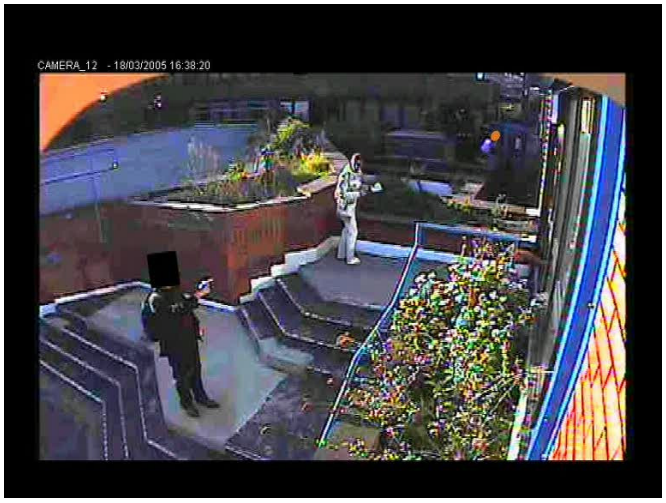


Abb.14: *Faceless*. TC: 25:40. (©Amour Fou).

[219] Diskussion im Top Kino (04.05.2008).
[220] Ebenda.

Es ist nicht klar, ob die Erzählerin als allwissender Erzähler agiert, aus der Sicht der Frau oder eines Aufsehers erzählt, oder aus der Position der *New Machine*. Daraufhin angesprochen wollte die Regisseurin keine klare Antwort geben. Ihr gefällt der Gedanke, dass es für den Zuseher unklar bleibt, für wen die Stimme steht: Sie sollte durch die verschiedenen Positionen „schwimmen", nicht unbedingt einer Person oder einem Erzähler zuordenbar sein.[221] Der Stimme würde man, ähnlich wie den Kameras, die „Allwissenheit", den Blick von oben unterstellen. Der Zuseher wird verunsichert, zum einen von der teilweisen Sonorität und andererseits von einer versteckten, unterdrückten Emotion der Erzählerstimme.
Das v*oice-over* wurde von der schottischen Oscar-Preisträgerin Tilda Swinton gesprochen.

Die Geschwindigkeit mit der die Bilder abgespielt werden variiert, was man an den mitlaufenden Timecodes ablesen kann. Die Regisseurin verlangsamt und beschleunigt das Bild, schneidet Bilder heraus, um die gewünschte Wirkung zu erzielen bzw. die gewünschten Bilder zu bekommen. Um z.B. die Illusion des Laufens zu erhalten, wurden Bilder später in der Szene beschleunigt – die Geschwindigkeit der Bewegung blieb gleich, der Timecode steigert sich rasant. Die Szene in der die Protagonistin ihr Gesicht in einer Spiegelung bemerkt, dauert ein paar Sekunden. Der Timecode gibt in diesem Fall aber die Dauer der „Dreharbeiten" wider.
Die Bildkompositionen besteht zum Teil aus Montagen in den Bildern selber: Mehrere Bilder im Bild, wie bei Überwachungsmonitoren, bekommen die Funktion, den Zuseher auf die Situation aufmerksam werden zu lassen, dass auch sie sich in der Position des Videooperators befinden.

Abb.15: *Faceless.* TC: 13:41. (©Amour Fou).

[221] Diskussion im Top Kino (04.05.2008)..

8.1. Plot

„A NEW TIME
THE NEW MACHINE
AMIDST WHICH SURVIVES
A SINGULAR DREAM."[222]

In einer nicht näher definierten Zukunft, kontrolliert eine Maschine Gesellschaft und Zeit. Sie verfolgt die Datenspuren der Bevölkerung und gibt einen Rhythmus vor, dem sich die Gesellschaft unterzuordnen hat, ein Takt, der den Tages- und Lebensablauf kontrolliert: „Eating, drinking, resting, going to work, getting married... every act is tied to *RealTime*. And every act leaves a trace of data. A footprint in the snow of noise."[223]

Die Maschine, von der Bevölkerung dazu bemächtigt die Vergangenheit auszulöschen um ihren eigenen Schuldgefühlen zu entkommen, löscht auch die Geschichten der Menschen aus die fortan in der eigens für sie geschaffenen *RealTime* leben. Die Datenspuren, die von Menschen zurückgelassen werden, werden beständig aufgezeichnet, notiert, gespeichert und analysiert. Damit geben sie der Maschine Information und Kontrolle. Der Verlust der Vergangenheit bringt den Verlust der Identität und somit den Verlust des Gesichtes mit sich. Die Überwachung ist mittlerweile soweit fortgeschritten, dass wir uns nicht soweit von der *New Machine* entfernt wähnen sollten. Die Metapher der *New Machine*, die Datenspuren sammelt, ist keine Metapher mehr – sie ist Realität. Luksch bringt damit ihre Sichtweise auf den Punkt: Das Filmmaterial stammt zum Teil aus choreographierten Aktionen, entstanden aber auch aus Situationen alltäglicher Besorgungen. Luksch zeigt hier, in Form eines Filmes der der Realität entspringt, die beängstigende Tatsächlichkeit der Überwachung, an jedem Ort und jeder Zeit. Das Wissen über die Vergangenheit bedeutet Kontrolle über die Zukunft. Dieser Thema wurde schon in George Orwells *1984* geprägt: „'Who controls the past,' ran the Party slogan, 'controls the future: who controls the present controls the past.'"[224]

Kein einziger Schritt bleibt dabei unbemerkt und wird auch nicht gelöscht, es wird nichts vergessen.

[222] *Faceless*. TC: 0:15.
[223] *Faceless*. TC: 9.10.
[224] Orwell, George. *Nineteeneightyfour*. Signet Classics. USA, 1977. S. 34.

8.2. Ideen und Einflüsse

Die Idee, Videobilder von Überwachungskameras zu verwenden und zu einem Film zusammenzustellen, wurde 1983 schon von Michael Klier umgesetzt. Sein Film *Der Riese*[225] hat allerdings weder Hauptdarsteller, noch einen Plot. Er verwendete Überwachungsvideos quer durch Deutschland und stellte sie zusammen. Er zeigt Flughäfen, Städte, Einkaufszentren, Banken u.v.m. und so gut wie keine Personen – „almost totally dehumanized". Auch dieser Film gilt als Mischung zwischen Science-Fiction und Dokumentation.[226]

> „Durch die Verknüpfung verschiedener Aufnahmen im realitischen[!] Stil entsteht der Eindruck eines zentralen Überwachungsapparates als anonymes, mächtiges Subjekt, das allgegenwärtig alles sieht, aber selbst nicht gesehen werden kann."[227]

Harun Farocki hat mit seinem Film *Gefängnisbilder*[228] ein ähnliches Experiment gemacht. Farocki zeigt die Tristesse des Gefängnislebens, in der die Zeit nicht vergeht. In der die Ereignislosigkeit das größte Problem darstellt.
Die Wärter können jederzeit Moment in alle Winkeln der Vollzugsanstalt blicken, jeden Gefangenen beobachten, wo er sich befindet und was er gerade macht. Die Kamera ist das Medium, das die Abweichung von der Norm sichtbar macht.[229]

> „Neben neuen Gefängnisbauten schafft diese Wirklichkeit auch ein neues Bild- und Blickregime. Farocki rückt dies in eine Tradition, das Gefängnis als Labor menschlichen Handelns zu verstehen, als anthropologische und technische Versuchsanstalt, in der das Verhalten des Menschen ebenso wie die Möglichkeiten seiner Manipulation und Konditionierung getestet werden."[230]

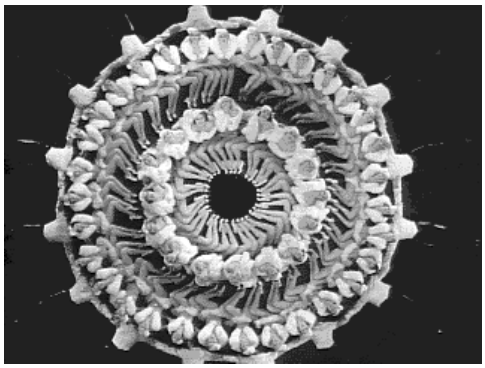
Lukschs Inspirationen für Choreographie und Plot gingen, wie sie selbst sagt, von Busby Berkelys Tanzchoreographie und Chris Markers Film *La Jetée* aus.[231]

---

[225] *Der Riese*. R: Michael Klier. 1983. Deutschland.
[226] Siehe: (http://www.thekitchen.org/MovieCatalog/Titles/DerRiese.html) (26.05.2008).
[227] Wolf, Reinhard. „Der Riese". (http://www.medienkunstnetz.de/werke/der-riese/) (10.10.2008).
[228] *Gefängnisbilder*. R: Harun Farocki. 2000. Deutschland. Dokumentarfilm.
[229] Siehe: „Dokumentarfilmzeit: Gefängnisbilder". (05.04.2007). (http://www.3sat.de/3sat.php?http://www.3sat.de/specials/11034/index.html) (28.05.2008).
[230] Pantenburg, Volker. „Gefängnisbilder". (09.10.2008) (http://www.kunst-der-vermittlung.de/artikel/filmbeschreibung-gefaengnisbilder/) (18.10.2008).
[231] Manu Luksch: Diskussion im Top Kino (04.05.2008).

Busby Berkeley (1895-1976):

Berkeley war Tänzer, Schauspieler und wurde später Theaterregisseur und Choreograph. Berühmt wurde er vor allem durch den Einsatz der Vogelperspektive, die seine kaleidoskopartige Choreographie, die sich in einer geometrischen Dynamik zeigte, erst zum Ausdruck brachte. Damit schuf er eine neue visuelle Sprache für das Kino.[232]



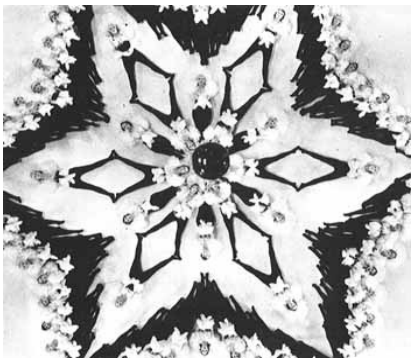


Abb.16: (links): *Young and Healthy* (1933). Busby Berkeley.

Abb.17: (rechts): "Dancers create geometric patterns in Busby Berkeley's *Dames* [1934]".

Die Tanzsequenzen in *Faceless* entstanden in Anlehnung an die Vogelperspektive der Kamera in Berkeleys Tanzszenen. Er machte sich den *Bird's Eye-View* (God's Eye POV) zunutze und filmte die Tänze in einigen seiner Filme von oben und zeigte damit eine neue, bisher kaum genutzte Möglichkeit der Darstellung von Choreographie im Film.

Abb.18: *Faceless*. TC: 6.00f. (©Amour Fou).

Francesco Casetti bezeichnet diese Einstellung als „unreal objective shot" der auf die Draufsicht der Kamera auf die Tänzer in Berkeley verweist.[233]

[232] Siehe: Billman, Larry. *Film Choreographers and Dance Directors*. McFarland&Company: London, 1997. S.233.

[233] Casetti, Francesco. In Warren Buckland (www.warrenbuckland.com) (18.10.2008).

La Jetée

Abb. 19: *La Jetée*. TC: 26'

Faceless orientiert sich in seiner Idee und seinem Aufbau an Chris Markers *La Jetée*. Für diesen Film verwendete Marker abgefilmte Photographien.[234] *La Jetée* hat nicht die abrupten, stakkatoartigen Bildabläufe, sondern führt ruhiger durch den Film. Die Filme ähneln sich aber nicht nur in der Form, sondern auch im Inhalt. Der erste Satz in *Faceless*, gleicht mit nur geringen Änderungen dem ersten Satz in Markers *La jetée*:

> „This is a story of a man marked by an image from his childhood."

Faceless:

> „This is a story of a woman haunted by an echo of a memory, a dislocated dream in which the past telescopes into the future."

Beide Filme handeln von einer Zeit, in der die Menschheit durch gravierende Eingriffe reduziert lebt. Bei *La Jetée* ist es die Zeit nach dem 3. Weltkrieg, bei *Faceless* ist es die Installation der *New Machine*, die durch die *RealTime* die Bevölkerung „versklavt". *La Jetée* dekonstruiert Zeit, indem der Protagonist Zeitreisen unternimmt. Sein Blick in die Zukunft bzw. der Wunsch in die Vergangenheit zurückzukehren und der Gegenwart zu entfliehen, führen allerdings unweigerlich zu seinem Tod. Catherin Lupton beschreibt den Protagonisten in *La Jetée* folgendermaßen:

> „The man finally realizes that there is no escape from Time[!], and that the image that had haunted him since childhood was that of the moment of his own death."[235]

[234] Auf den Filmplakaten von *La jetée* (IMDB) wird Chris Marker, mit *La jetée,* als der gedankliche Vater von Terry Gilliams *12 Monkeys* (1995) geführt: „The film that inspired 12 MONKEYS" bzw „The brilliant inspiration for ‚12 Monkeys' " (http://www.imdb.com/title/tt0056119/) (10.07.2008).

[235] Lupton, Catherin. Christ Marker. Memories of the Future. Reaktion Books. London, 2005. S. 89.

Abb. 20: *La Jetée*. TC: 26'

Die Protagonisten der beiden Filme verbindet eine emotionale Bindung an die Vergangenheit. In *La Jetée* wird der Protagonist auf Zeitreisen geschickt, „only because he was glued to an image of his past."[236] *Faceless* hingegen schafft Zukunft und Vergangenheit ab, um sie durch den Takt der *RealTime* zu ersetzen. Es sind die Erinnerungen der Frau an ein Kind – ihr Kind – die sie erwachen lassen und ihre Reise bis ins Zentrum der *New Machine* führen. Dort erwartet sie zwar nicht der Tod, ihre Reise als Mensch, der sich seiner Individualität bewusst ist, wird allerdings durch die Reintegration in die *RealTime* beendet.


Abb.21: *Faceless*. TC: 45:46. (©Amour Fou).

[236] *La jetée*. R: Chris Marker. Timecode: 7:48. (Siehe auch: http://www.youtube.com/watch?v=3RvmJan17q8) (10.06.2008).

8.3. Interpretationen

Faceless verwendet wie in George Orwells *1984* ebenfalls einen totalitären Staat als Hintergrund der, verbunden mit der „Zeitkontrolle", auch eine sprachliche Verstümmelung zur Folge hat: *Newspeak* in *1984* verfolgt den Zweck bestimmte Gefühle und Gedanken zu verdrängen um nur noch die vom Staat verfolgten Gedanken denken zu können („The purpose of Newspeak was [...] to make all other modes of thought impossible."[237]). Die Protagonistin in *Faceless* erhält einen Brief der ihr helfen soll, zu verstehen was mit ihr vorgeht. Die Emotionen, die sie dabei verspürt, kann sie nicht verstehen, es sind Worte aus einer vergangenen Zeit. Die Emotionslosigkeit die mit der Ges(ch)ichtslosigkeit einhergeht, kommt als Kontrollmechanismus in dem Film *Equilibrium* (R.: Kurt Wimmer (2002)) zur Anwendung. Durch die Einnahme von Emotionshemmern werden Gefühle unterbunden. Individualität muss rationalem Denken und der Konformität weichen, um Krieg, Angst und Verbrechen zu auszumerzen. Der Vorläufer und geistiger Vater von Orwells *1984* ist *Wir* (1920) von Jewgenij Samjatin, dessen Protagonist, D 503, Ingenieur ist und im Takt einer Maschine arbeitet, die wie in *Faceless* alles kontrolliert und nach „mathematischen Gesetzen" organisiert. Die Häuser bestehen aus Glasfassaden, in die jeder einsehen kann. D 503 erlebt wie seine Liebe zur „mathematischen Harmonie"[238] zu bröckeln beginnt. Dafür entdeckt er die Abweichung von der Masse durch die Liebe zu einem Menschen, der ihm die Phantasie wiedergibt.

In den hier angeführten Beispielen wird (mathematische) Rationalität als einziger Weg zu Harmonie beschrieben. Und in allen Beispielen wird den Protagonisten durch ihre „Abnorm" und ihr Außenseitertum, abseits einer aufgezwungenen Lebensweise, das Leben in vollem Umfang bewusst (durch Emotionen, Vergangenheit, Erinnerung, Liebe, dem Denken außerhalb der Norm). Dieses Wissen und die Existenz dieser Personen sind systembedrohend: In *Wir*, *1984* und *Faceless* scheitern die Protagonisten kurz vor ihrem Ziel, sie sterben allerdings nicht, sondern werden gezwungen wieder an dieses System zu glauben. Dem

[237] Orwell, George. *Nineteeneightyfour*. Signet Classics: USA, 1977. S. 299f.

[238] Die Synchronisation der Bevölkerung in die *RealTime*, dem „hehren Zweck dienend" die Harmonie, geistige Ruhe und Frieden zu erhalten, ähnelt der *24. Geschichte* in Stanislaw Lems *Sterntagebücher*: Ijon Tichy, der Raumfahrer, kommt auf den Planeten der Indioten. Dort wurde eine Maschine programmiert, welche den Menschen die Verantwortung abnehmen und dem Planeten zu Harmonie verhelfen soll. Die Maschine sieht den Menschen in seiner Form als „Abartigkeit" an, beginnt den Menschen zu beseitigen und „verarbeitet" ihn zu „runden durchsichtigen Scheiben". Diese werden dann in der „vollendeten Harmonie" der Maschine auf dem Planeten aufgestellt. Die Indioten verlieren ihr Leben um einer „mathematischen Harmonie", zu dienen die ihnen eine Maschine vorgegeben hat. *Faceless* funktioniert ähnlich: Um dem schlechten Gewissen der Vergangenheit und der Angst vor der Zukunft zu entkommen, unterwirft sich die Bevölkerung der Maschine, die ihnen Probleme und Verantwortung abnimmt, und sie zu „hohlen Gefäßen" macht.

Ingenieur D 503 in *Wir* wird durch eine Operation die Phantasie entfernt. Winston Smith wird in *1984* solange gefoltert bis er wieder an Big Brother und dessen Unfehlbarkeit glaubt und in *Faceless* wird die Protagonistin ohne es wirklich zu wissen, wieder in jene Zeit integriert (*RealTime*), vor der sie geflüchtet ist.

8.4. *Manifesto for CCTV Filmmakers* vs. *Dogma 95 Manifest*

Das *Manifesto for CCTV-Filmmakers* ist in Diskussionen des Öfteren mit dem *Dogma-Manifest* verglichen worden. Manu Luksch sieht dabei aber gravierende Unterschiede: Ihr Manifest sei weniger eine Restriktion für Filmemacher, sondern vielmehr sollte es ein Werkzeuges schaffen, mit dem sich neue Möglichkeiten überhaupt erst eröffnen. Es werden klare Regeln für den Umgang geschaffen, die allerdings nicht freiwillig sondern durch den DPA limitiert sind. Sie sollen aber als Chance, und nicht als Einschränkung wahrgenommen werden.[239] Während *Dogma*-Regeln bewusst Einschränkungen vornehmen, wird das *Manifesto* von äußeren Einflüssen beschnitten (Gesetz, Kooperation der Betreiber, etc.).

Es sind durchaus Ähnlichkeiten in den Regelaufstellungen der beiden Manifeste festzustellen, allerdings gelten grundsätzlich verschiedenen Voraussetzungen: Das Credo der *Dogma*-Filmemacher ist die Reduktion des Films auf das Wesentliche, die Forderung nach der „Keuschheit der filmischen Erzählung“[240]:

Dogma 95 Manifest[241]

,,I swear to submit to the following set of rules drawn up and confirmed by DOGME 95:

1. Shooting must be done on location. Props and sets must not be brought in (if a particular prop is necessary for the story, a location must be chosen where this prop is to be found).
2. The sound must never be produced apart from the images or vice versa. (Music must not be used unless it occurs where the scene is being shot).
3. The camera must be hand-held. Any movement or immobility attainable in the hand is permitted. (The film must not take place where the camera is standing; shooting must take place where the film takes place).

[239] Diskussion im Top-Kino (04.05.2008).
[240] Maneljuk, Tina. „Thomas Vinterberg.“ *Film-zeit.de* (Juni 2007) (http://www.film-zeit.de/home.php?action=result&sub=person&info=long&person_id=1489&PHPSESSID=73.) (20.05.2008).
[241] Dogma 95. „The Vow of Chastity“. (http://www.dogme95.dk/menu/menuset.htm) (21.05.2008).

4. The film must be in colour. Special lighting is not acceptable. (If there is too little light for exposure the scene must be cut or a single lamp be attached to the camera).
5. Optical work and filters are forbidden.
6. The film must not contain superficial action. (Murders, weapons, etc. must not occur.)
7. Temporal and geographical alienation are forbidden. (That is to say that the film takes place here and now.)
8. Genre movies are not acceptable.
9. The film format must be Academy 35 mm.
10. The director must not be credited.

Furthermore I swear as a director to refrain from personal taste! I am no longer an artist. I swear to refrain from creating a "work", as I regard the instant as more important than the whole. My supreme goal is to force the truth out of my characters and settings. I swear to do so by all the means available and at the cost of any good taste and any aesthetic considerations.
Thus I make my VOW OF CHASTITY."
Copenhagen, Monday 13 March 1995'

Das *Manifesto for CCTV Filmmakers* hingegen verweist auf die Möglichkeit, ohne eigene Kamera Filme zu machen, „as a possibility of empowering the director".[242] In der Einleitung zu ihrem *Manifesto* (Version 2004) bezeichnet Luksch den Filmemacher als Symbiont, einen Nutznießer des Überwachungsnetzwerkes, und hält Grundlegendes fest:

> *„ the filmmaker as symbiont:*
> *opportunistic infections of the surveillance apparatus*
> MANIFESTO FOR CCTV FILMMAKERS declares a set of rules, establishes effective procedures, and identifies further issues for filmmakers using pre-existing CCTV (surveillance) systems as a medium in the UK. The manifesto is constructed with reference to the **Data Protection Act 1998** [*Herv. Luksch*] and related privacy legislation that gives the subjects of data records (including CCTV footage) access to copies of the data. The filmmaker's standard equipment is thus redundant; indeed, its use is prohibited. The manifesto can easily be adapted for different jurisdictions."[243]

Durch die Arbeit mit CCTV-Material und den Umstand, dass ein Versuch mit diesem Material eine geschlossene Handlung zu zeigen, noch nicht unternommen wurde, war der Arbeitsprozess stark von einem „learning by doing" Prinzip geprägt.
Während eines Workshops in Graz im November 2007 wurde versucht, das *Manifesto* auf das österreichische Datenschutzgesetz anzuwenden. Es erwies sich schwieriger als erwartet. Diese „einfache Adaption" (siehe Zitat oben.) des *Manifestos* auf andere Datenschutzgesetze stellt sich allerdings als nicht so einfach heraus: Dieser Umstand rührte daher, dass

[242] Manu Luksch. Diskussion im Top-Kino (04.05.2008).
[243] *Manifesto for CCTV Filmmakers.* (siehe: Anhang).

Videoüberwachung im DSG 2000 nicht behandelt ist. Während des Versuchs, das *Manifesto* zu adaptieren, blieben daher viele Fragen zwangsläufig unbeantwortet.

Im Folgenden wird das *Manifesto* zitiert wobei die einzelnen Paragrafen des DPA ausgespart werden. Eine vollständige Version des *Manifestos* befindet sich im Anhang.

Das Manifest ist unterteilt in sechs Punkte:[244]

1. General
   The filmmaker is not permitted to introduce any cameras or lighting into the location.

2. Script
   A protagonist („data subject“) is required to feature in all sequences.

3. Location
   The filmmaker is to choose locations covered by multiple cameras operated by a large business, private security firm or public authority – or, if operated by a small retailer, cameras that can be panned or zoomed remotely. Locations may be mobile (e.g., public bus).

   For every camera, the operator's name and contact details are to be noted.

4. Footage Requests
   After each shoot, the filmmaker is to send a written request („subject access request letter“) to the CCTV operator („data controller“) to ensure that the data recovery process can be initiated while the recordings are still archived. (Mandatory retentions periods vary.)

   The subject access request letter is to state the place and time of the recording and include a picture of the protagonist (wearing the same clothes if possible) and a cheque for £10 (the maximum fee chargeable). Letters should be sent by a secure system that provides evidence of delivery. (Some data controllers may require the notarisation of the letter to legally establish identity.)

   The filmmaker is to allow a maximum 40 days after sending the data request for an initial response.

   The filmmaker is to establish a set of rules for handling the various formats in which the data may be sent (video tape, DVD-video, digital files encoded with proprietary codecs, hard copies of frames, etc.).

5. Sound
   CCTV systems are not permittet to record sound. The filmmaker is to establish a set of rules for the soundtrack (if any) of the movie.

[244] *Manifesto for CCTV Filmmakers.* (siehe: Anhang).

6. Distribution
   Footage received is subject to complex copyright issues. The filmmaker is to take legal advice and establish a strategy.

Weiters gibt es zu diesen sechs Punkten noch zwei Anmerkungen:[245]

> „The documented activity of the protagonist must qualify as personal or sensitive data. The filmmaker is to establisch this by locating a CCTV camera and circumscribing the field of action for the actors relative to it, so that incidents of biographical relevance (i.e., that reveal personal data) occur in the frame.
>
> All people other than the protagonist ("third parties") will be rendered unidentifiable on the data obtained from the CCTV operators. Typically, operators blur or mask out faces of third parties. The filmmaker is to consider the visual impact of this manipulation, and to establish a rule for the handling of footage delivered with ineffectual masking or blurring – for example, reporting the offence."[246]

Die Regeln sind eher Vorschläge, bzw. eine Bedienungsanleitung, um rechtlich abgesichert zu sein. Luksch rät aber trotzdem die Zuhilfenahme eines Anwaltes.

8.5. legal readymades – found footage – video sniffing

Luksch wendet für ihr Material den Terminus „*legal readymades* (‚objet trouvé')"[247] an. Der Begriff entspricht dem klassischen Gedanken Marcel Duchamps, ein Objekt dem Kreislauf „industrieller Realität"[248] zu entnehmen um es dem ursprünglichen Bereich völlig fremden Kreislauf, nämlich dem der Kunst zuführt.

> „Die Idee war die, ein Objekt zu finden, das vom ästhetischen Blickwinkel aus keinerlei Anziehung hatte. [...] Daß[!] die meisten meiner Ready-mades

[245] Diese Version des *Manifesto* wurde während eines Workshops in Graz im November 2007 ausgehändigt.
[246] AmbientTV.net. *Manifesto for CCTV-Filmmakers*. (http://lo-res.org/~manu/manifestocctvfilmmakers2004.mp4) (02.10.2008).
[247] Luksch/Patel. 2007. S. 74. Das „objet trouvé" (*found footage*) stellt im Falle Lukschs aber nicht nur das Rohmaterial dar, das in ein Kunstobjekt umgewandelt wird. Seine Bedeutung geht darüber hinaus: Die Bilder dieses Mediums existieren teilweise unter sozialen und rechtlichen Bedingungen, mit einem rechtlichen Überbau. (siehe: Ebenda. S. 74).
[248] Siehe: Daniels, Dieter. *Vom Readymade zum Cyberspace*. Kunst/Medien: Interferenzen. Hatje Cantz Verlag: Ostfildern-Ruit, 2002. S. 47.

> Massenprodukte waren und dupliziert werden konnten, ist ein weiterer wichtiger Unterschied.“[249]

Für Luksch stellen die *legal readymades* ein „rechtliches Fertigprodukt“ dar. Sie behandelt dieses Produkt wie Duchamp, und auch Michael Klier zuvor[250], indem sie die Bilder dem Kreislauf der Sicherheits- und Überwachungsbranche entnimmt. [251]
Die Verwendung von *legal readymades* in *Faceless* ähnelt den Bildern, die in *found footage* Filmen zum Einsatz kommen. Der Unterschied besteht allerdings darin, dass diese Bänder „live“ sind und erst durch den DPA zustande kommen konnten. Vor allem der rechtliche Hintergrund unterscheidet diese beiden Formen: Dieses „Fertigprodukt“ basiert auf dem Gesetz und Manu Luksch hat dieses Material legal, also rechtlich korrekt, erworben, daher auch *legal readymades*.

Lukschs Idee hat Nachahmer gefunden, die sich aber weniger „strikt“ an ihr *Manifesto for CCTV-Filmmakers* halten. Als Weiterentwicklung der Idee, Material von Überwachungsanlagen anzufordern, wurde Bildmaterial von wireless-Überwachungskameras abgefangen und aufgezeichnet. Für diese Art der Materialbeschaffung wird der Terminus *video sniffing*[252] verwendet. *Video sniffing* ist außerdem billig und erfordert kein großartiges technisches Vorwissen.

> „Video sniffing encourages people low on resources, but high on imagination, to create their own media. Our mission is to capture the live feed from the network of CCTV cameras that stand sentry over so many shops and street corners in Britain. […]“[253]

Ist keine Einverständniserklärung der Betroffenen (Besitzer als auch Gefilmte) vorhanden, ist *video sniffing* eigentlich illegal. Nachdem allerdings nur wenige Signale gesichert sind und es an und für sich keine Möglichkeit gibt festzustellen, ob jemand das Signal abfängt, relativiert sich auch die rechtliche Situation.

---

[249] Duchamp, Marcel zit. In: Kunstwissen.de. (http://www.kunstwissen.de/fach/f-kuns/o_mod/ducham1.htm) 18.10.2008).
[250] „Klier setzt dabei ganz auf den Readymade-Effekt des unveränderten Materials, das [...] provokant auf die Allgegenwart von Überwachung aufmerksam macht [...].“ Daniels. 2002. S 42.
[251] Siehe: Luksch, Manu: Einreichung Projekt 2007-1: *Orchestra of Anxiety* (http://netznetz.net/wiki/Einreichung_Projekt_2007-1_Orchestra_of_Anxiety) (28.04.2008).
[252] *Video-Sniffin'*. (04.07.2006) (http://mediashed.org/videosniffin) (am 10.04.2008).
[253] Dodson, Sean. „The secret art of video sniffing. Real-life stars of CCTV.” (25.04.2008) *Guardian-Online*. (http://arts.guardian.co.uk/filmandmusic/story/0,,2275895,00.html) (05.05.2008).

> „[…] The handheld receiver allows us to scan, or 'sniff', wireless transmissions and view them on the screen without the owner's knowledge or consent."[254]

Von Rechts wegen sollten derartige Möglichkeiten durch Verschlüsselungen oder Absicherungen ausgeschlossen werden. Graham Harwood, Mitglied der Künstlergruppe *Mongrel*,[255] präsentierte 2007 auf dem Symposion der Ars Electronica *Goodbye Privacy 2007*, ein Projekt, das von Jugendlichen gestaltet wurde, die normalerweise nur auf der Straße „rumhängen". Sie wurden aufmerksam als sie im Internet auf den Begriff *video-sniffin'* stießen, „a term given to the practice of picking up the public signals being broadcast by wireless CCTV."[256]

the commercial[257] ist ein von Mediashed[258] ausgehendes *video-sniffin'* Projekt. Die Ausgangsposition bzw. Fragestellung war dieselbe, die sich Manu Luksch gestellt hatte: „Why would you want to buy some video equipment when there are already so many cameras around for you to use?"[259]

Die Jugendlichen suchten sich eine High Street, in der sie ca. 24 Kameras vorfanden, und baten dann die Besitzer der Geschäfte, ob sie vor den Kameras eine Inszenierung aufführen und dabei das Signal ihrer CCTV-Kameras abfangen zu dürfen. Die Besitzer gaben dabei nicht nur ihre Zustimmung, sondern nahmen das Engagement der Jugendlichen positiv auf:

> „The shop owners were very surprised and happy for the young people to create a film this way. […] These kinds of projects allow people to see how a common technology that is normally used for the surveillance of the same young people can be repurposed by them for creative activities. The project created great interest from the local council and local businesses who positively engaged with the project."[260]

---

[254] Dodson. (25.04.2008).

[255] "Mongrel is an internationally recognised artists group specialising in digital media. We are well known for our pioneering arts projects, including the first online commission from the Tate Gallery London and work in the permanent collections of the Pompidou Centre Paris and the Centre for Media Arts in Karlsruhe (ZKM). Combined with this we usually work with marginalised peoples who are on low incomes, socially excluded and cultural minorities. We do this by helping people to do things for themselves, creating social software and digital arts based projects that we then promote to a state of high visibility through our international network of arts connections. The groups gain a visible voice, self reliance, self confidence and informal training allowing them to get a foot hold into mainstream training, education, culture and the economic life most of us take for granted." (http://www.mongrel.org.uk/) (10.04.2008).

[256] Mediashed: delboy: *the commercial*. in: (www.mediashed.org/?q=videosniffincom) (05.05.08).

[257] Das Video dazu ist zu finden auf: (http://mediashed.org/videosniffincom) (10.04.2008).

[258] "The MediaShed is a Community Interest Company. The MediaShed is the first "free-media" space to open in the east of England. It's a place where members can come, hang out, learn, propose some training, create and propose new projects using free-media or show things they have made on one of our screening nights. The MediaShed is designed to be as open and accessible as possible, welcoming all." (http://www.mediashed.org). (05.05.2008).

[259] (http://www.we-make-money-not-art.com/archives/2007/09/in-linz-several.php) (05.05.08).

[260] Mediashed. (http://www.mediashed.org) (05.05.2008).

Abb. 22-24: Stills aus *the commercial* (2006).

Mit geringem technischem Aufwand kann ein Empfänger gebastelt werden, der die Funksignale von wireless-Kameras abfängt und aufzeichnet. Im Mai 2007 wurde bei dem Festival *Futuresonic*[261] in Manchester ein eigener Workshop geschaffen, der sich mit Überwachung auseinandersetzte und Filmen widmete, die durch *video-sniffin'* von CCTV-Anlagen entstanden sind.[262]

[261] Urban Festival of Art, Music & Ideas. (www.futuresonic.com) (05.05.2008).
[262] Der Workshop fand am 12. Mai 2007 statt, und wurde von MediaShed geleitet. Der Titel lautete: Video-Sniffin' and Spy-Kiting: Hack wireless CCTV while talking a stroll through the streets of Manchester, and fly kites equipped with CCTV cameras. A Gearbox free-media project by MediaShed. (http://www.futuresonic.com/07/social_technologies_summit.html) (10.06.2008).

Im weitesten Sinne sind *found footage*, *legal readymades* und *video sniffin'* als eine Gruppe (in ihrer Verwendung von Filmmaterial) zu sehen, die sich hauptsächlich durch die rechtliche Grundlage des Filmmaterials unterscheiden.

Auch in Österreich wurde der Versuch gemacht, wireless-CCTV-Systeme anzuzapfen. Hans Zeger von der Arge-Daten formulierte die „Schwierigkeit", ein wireless-System zu „hacken" so: Ein Babyphone mit integriertem Bildschirm und einem zusätzlichen Gerät zur Aufzeichnung reichten eigentlich schon.[263]
Martin Slunksy, ein Mitarbeiter von Quintessenz,[264] hat sich mit seinem Laptop ohne große Mühe in die Funkverbindung der Überwachungskameras am Schwedenplatz (Wien) gehackt. Die Ergebnisse wurden 2005 auf dem *22. Chaos Communication Congress* (22C3) in Berlin präsentiert. In einem Artikel über den Kongress wurde die Präsentation von Martin Slunsky folgendermaßen zusammengefasst:

> „[...D]ie Beamten bei einem der am Wiener Schwedenplatz aufgezeichneten Filme [schwenkten] von einem Fenster der benachbarten Häuser zum nächsten und zoomten ganz dicht ran. Man hätte recht genau beobachten können, ‚was sich hinter den Gardinen abspielt', [...] ein Zusammenhang mit Strafverfolgung sei [...] nicht ersichtlich gewesen."[265]

Das Fazit für Slunsky war, dass die Beamten die Kameras offensichtlich nicht zur Überwachung und Gewährleistung der Sicherheit benutzten, sondern sich über die Schwenk- und Zoomfunktion der Kameras vielmehr auf umliegende Fenster konzentrierten und somit in Privatsphären von Bürgern eingedrungen sind. Ein derartiger Eingriff stellt eine massive Datenschutzverletzung dar, zeigt gleichzeitig aber auf, wie einfach und simpel sich Überwachung, die der Sicherheit dienen sollte, in ihr Gegenteil verkehrt. Sicherheitsmaßnahmen können, und werden (auch) gegen jene verwendet, die den Schutz eigentlich gesucht haben.

[263] Diskussion im Top-Kino. (04.05.2008).
[264] Quintessenz ist ein österreichischer Datenschutzverein der sich unter anderem für die *Big Brother Awards* verantwortlich zeichnet.
[265] Krempl, Stefan: „Hacker überwachen Videoüberwachung" (30.12.2005) *Heise online* – 22C3 (http://www.heise.de/newsticker/meldung/67842) (10.04.2008).

9. *Mockumentary* und Realität

Eine (damals) fiktive, kontroverse Angelegenheit, die 1999 in einer Mockumentary thematisiert wurde ist der Film *Citizen Cam*. Er zeigt eine Stadt die Videoüberwachungsbilder in einen TV-Kanal einspeist, und stellt sich am Ende als unwahr heraus. 7 Jahre später realisiert ein Londoner Wohlfahrtverband genau diese Idee und lässt die Bevölkerung, sehr zum Unmut von Datenschützern, Aufgaben der Polizei übernehmen und die eigene Gegend überwachen.

9.1. *Citizen Cam*

Isländischen Regisseur Jérôme Scemla thematisierte 1999 in *Citizen Cam*[266] einem Kurzfilm eine obsessive Form der Videoüberwachung. Diese Mockumentary[267] präsentierte sich wie ein Dokumentarfilm. Darin zeigt Scemla ein fiktives Bild Reykjavíks: 200 Kameras speisen Bilder in einen TV-Kanal, HumaniTV, ein. Es werden Interviews mit dem Polizeichef, mit Künstlergruppen, mit Einwohnern und Datenschützern geführt. Der Kurzfilm klagt den übermäßigen CCTV-Gebrauch als scheinbares Allheilmittel gegen Verbrechen an, schließt mit einem Verweis auf den (tatsächlich vorgefallenen) Echelon-Abhörskandal[268] und verleiht ihm damit noch mehr Dokumentationscharakter. Am Ende des Filmes erscheinen allerdings die Credits der Schauspieler, und der Film wird als Farce aufgelöst. Die letzten Bilder stellen mit der Einblendung der Echelon-Abhörkuppeln, noch eine Mahnung dar: Der Zuseher soll nicht vergessen, dass Überwachung ein Thema ist, um das man sich Gedanken machen sollte. Scemlas Idee ist letzten Endes nicht weit von der Realität entfernt.[269]

---

[266] *Citizen Cam*. R.: Scemla, Jérôme. Canal+. 1999. Frankreich, Island.

[267] Mockumentary bezeichnet einen fiktionalen Dokumentarfilm der eine Parodie darstellen soll (siehe: http://de.wikipedia.org/wiki/Mockumentary) (10.05.2008): setzt sich den englischen Wörtern: *mocking* (spotten, sich lustig machen) und *documentary* zusammen. Ähnlich wie *faction*: eine Mischung aus *Fact* und *Fiction*.

[268] Der ECHELON-Abhörskandal wurde von dem neuseeländischen Journalisten Nicky Hager in seinem Buch: *Secret Power: New Zealand's Role in the International Spy Network* (1996) aufgedeckt. Unter der Führung der USA wurde ein Netzwerk aufgebaut, die UKUSA, die sich nach dem Kalten Krieg zusammenfand, um Informationen abzufangen. „So each station collects all the telephone calls, faxes, telexes, Internet messages and other electronic communications that its computers have been pre-programmed to select for all the allies and automatically sends this intelligence to them." (Hager zitiert in: Withaker, Reg. *The End of Privacy*. The New Press. New York, 1999. S.92) Mitglieder des UKUSA Netzwerkes sind die USA und GB als „Gründerstaaten", Kanada, Australien und Neuseeland als „junior partners." (Siehe: Withaker. S. 93).

[269] Der ehemalige österreichische Innenminister Ernst Strasser hat die Qualität dieses Kurzfilms unter Beweis gestellt, indem er bei einer Pressekonferenz auf diese „Dokumentation" verwies, ohne bemerkt zu haben, dass es sich um einen Kurzfilm handelte.

Abb.25-26: *Citizen Cam*: TC: 24:22.

Der ehemalige österreichische Innenminister Ernst Strasser hat die Qualität dieses Kurzfilms unter Beweis gestellt, indem er bei einer Pressekonferenz auf diese „Dokumentation" verwies, ohne bemerkt zu haben, dass es sich um einen Kurzfilm handelte.[270]

9.2. Shoreditch Trust

Die Idee Scemlas ist durch einen Londoner Wohlfahrtsverband Wirklichkeit geworden. Um die Überwachung nicht nur in „fremde" Hände zu legen, wurde 2006 der Bevölkerung in

Siehe: Artikel: *Der Standard* vom 19.03.2004 gefunden auf: (http://www.peterpilz.at/html/txt/index.php?jahr=2004&monat=3) (20.05.2008).

[270] Artikel: *Der Standard* vom 19.03.2004 gefunden auf: (http://www.peterpilz.at/html/txt/index.php?jahr=2004&monat=3) (20.05.2008).

einem Stadtteil in London die Möglichkeit gegeben, an der Überwachung der Straßen und somit auch der „Überwachung der Überwacher" teilzunehmen: Am 11. Jänner 2006 wurde beschlossen, einen heruntergekommenen Stadtteil in London East End mit einer neuen Technik für einen Überwachungsmodus auszustatten und in einen „sicheren Bezirk" zu verwandeln. Der Shoreditch Trust, ein Londoner Wohlfahrtsverband, macht über eine Breitbandverbindung CCTV-Kamerabilder für die Bevölkerung zugänglich. Dabei werden Bilder von ca. 400 Kameras abwechselnd gezeigt und im Abstand von 30 Sekunden auf die Bildschirme übertragen. Die Bevölkerung kann bei Auffälligkeiten über den Fernseher per Textnachricht mit der Polizei Kontakt aufnehmen. Der Shoreditch Trust nennt es den „community safety channel".[271] Über diesen Kanal hat die Polizei auch die Möglichkeit Informationen über Verdächtige zu übertragen.[272] auszustrahlen. Diese Art von „Verbrechensbekämpfung" ist in England nicht unbedingt neu und nennt sich „naming and shaming."[273] Der Chief Executive von Digital Bridge, die dieses System für den Shoredtich Trust technisch erstellt hat, ist da allerdings anderer Meinung: „This is not naming and shaming or spying, it is getting the community engaged with their services."[274] Der Trust argumentiert ähnlich. Er behauptet, dass jeder auf jeden aufpassen kann, so wie es in den 40er und 50er Jahren in der Nachbarschaft stattgefunden hat. Der Pressesprecher Dan Hodges führt das verharmlosend weiter, dass es sich dabei ja nicht um einen anonymen Big Brother handelt: Die Gesellschaft passt auf sich selber auf.[275]

In der Anfangsphase wurden in 1000 Haushalte die Bilder von 11 Kameras gesendet. Sollte dieses Projekt erfolgreich sein, wird eine Aufstockung auf 400 Kameras und 20.000 Haushalte geplant. Laut James Morris (*Vorstandsvorsitzender von Shoreditch Trust*) ist ein hohes Maß an Beachtung gegeben, sowohl von Seiten der Presse, aber auch von Interessenten aus dem Ausland.[276]

Das Projekt selber ist umstritten. Vorwürfe wie „Voyeurismus", „Selbstjustiz" und „Verletzung der Privatsphäre" sind in diesem Zusammenhang laut geworden. Neugier spielt

[271] Weaver. (11.01.2006).
[272] Siehe: Ebenda.
[273] Becker, Matthias. „Heute Abend im Fernsehen: Alles.")15.04.2006) *Telepolis.* (http://www.heise.de/tp/r4/artikel/22/22461/1.html) (10.10.2007).
[274] James Morris (Chief Executive von Digital Bridge) zit. in: Iggulden, Amy. "CCTV channel beamed into you home". (10.05.2006) *Telegraph-Online* (http://www.telegraph.co.uk/news/uknews/1517836/CCTV-channel-beamed-to-your-home.html) (05.07.2008).
[275] Siehe: Weaver. (11.01.2006).
[276] Becker. 2006.

keine geringe Rolle zum Gelingen dieses Projekts, ist sich Dan Hodges sicher. Allerdings glaubt er nicht, dass dieser Kanal in einem voyeuristisch Weisen genutzt wird.[277]
Gegenstimmen gibt es von mehreren Seiten wie z.B. der *Crime and Society Foundation*:

> „Durch dieses Projekt wird das Strafrechts[!] in den Alltag ausgedehnt. Warum sollen Anwohner etwas tun, was Aufgabe der Polizei ist?“[278]

ASBO-Concern (*Anti-Social Behaviour Order*) befürchtet eine Veränderung des Verhaltens in Richtung Selbstjustiz, z.B. gegen Bettler.[279] Der Shoreditch Trust selbst argumentiert damit, dass die Bevölkerung nicht bloß in die Kriminalitätsbekämpfung miteinbezogen wird. Es soll den Menschen die Möglichkeit geben sich zu vergewissern, dass es draußen auch sicher ist. Das Sicherheitsgefühl soll gestärkt werden, vor allem von jenen die Angst haben das Haus zu verlassen.[280]

> „It addresses not just the reality of crime but the fear of crime, which can be just as debilitating as crime itself. Its[!] something that residents find reassuring.“[281]

Der Shoreditch Trust ermöglicht damit eine Bespitzelung z.B. durch Nachbarn, ähnlich wie in Orwells *1984*, bzw. erweckt es Ähnlichkeiten zum Stasi-Spitzelapparat.

---

[277] Ebenda. (Der Trust wird mit ca. 60 Millionen Pfund vom britischen Staat und der EU bis 2010 gefördert. Haushalte, die diesen Kanal empfangen wollen, müssen £3,50 pro Woche zahlen.)
[278] William McMahon von der Crime and Society Foundation. zit. In: Becker. 2006.
[279] Siehe: Andrew Mackay (ASBO). zit. in: Becker. 2006. (ASBOs sind Verweise an Jugendliche die sich „unsozial” verhalten („causing harrass, alarm or distress to others“). Sie können Platzverbote beinhalten, Radfahren verbieten u.ä. Werden diese Vorstrafen missachtet, können die Jugendlichen zu Gefangnisstrafen bis zu 5 Jahren verurteilt werden.) Siehe: Anti-Social Behaviour Orders (ASBO’s). (http://www.antisocialbehaviour.org.uk/asbo/index.php) (10.10.2008).
[280] “Services will include access to online CCTV cameras s.o that vulnerable people can see if it is safe to go out.” Sherwin, Adam. “Broadband will make life rich in Shoreditch.” (19.01.2005) *Times-Online*. (http://www.timesonline.co.uk/tol/news/uk/article410580.ece) (10.10.2007)
[281] Weaver. (11.01.2006).

10. Sicherheit und Religion

Einen gibt's der alles sieht,
auch wenn's in dunkler Nacht geschieht.

In dem Projektbericht zu einer ihrer Aktionen (*Orchestra of Anxiety 2007*) schreibt Manu Luksch, mit dem Verweis auf den wachsenden Sicherheitssektor, dass

> „[...] Sicherheit nicht gekauft werden kann (die innere Unruhe lässt sich nicht bestechen) sondern vergleichbar wie eine Religion funktioniert: man kann blos[!] dran glauben, Garantie gibt es keine."[282]

Es wenden sich zunehmend mehr Menschen von der Religion ab, und suchen ihr „Heil" in der Sicherheitsindustrie. Dadurch entsteht ein wachsendes Netzwerk an Videoüberwachung, das von der Bevölkerung zum Teil nicht nur gewünscht wird. Sie wird sogar selbst aktiv und installiert Kameras. Im Hinblick auf die Themen Religion und Videoüberwachung, bezeichnet Luksch die Videooperatoren als „Priester der (neuen) Sicherheitsreligion"[283] die über einen God's Eye POV verfügen: „[...] the character shows itself to someone who, while gazing and seeing, remains unseen."[284] Der Videooperator ist derjenige der nicht gesehen wird, der versteckt und unsichtbar bleibt und der die Kontrollfunktion ausübt. In Faceless wird der Zuseher mit dieser Rolle bedacht. Auch wenn er nicht direkt eingreifen kann, so ist doch der Blick der des Überwachers. Den Videooperatoren ist als „Priester" die Macht gegeben, die Daten der Überwachung zu lesen und sie auszuwerten, und daraufhin Entscheidungen zu treffen, die stark von ihren Vorurteilen geprägt sind.

Wenn man von der Videoüberwachung in einer Stadt wie London spricht, drängt sich der Vergleich mit dem „allwissenden, allsehenden Auge Gottes" beinahe auf. Man wird ständig beobachtet, Abweichungen werden registriert. In den Religionen wird erst nach dem Ableben die Schuld „abgerechnet",[285] dahingehend haben Kameras (theoretisch) einen stärkeren, weil unmittelbareren Charakter.

---

[282] Luksch, Manu: Einreichung Projekt 2007-1 Orchestra of Anxiety
[283] Diskussion im Top-Kino. 04.05.2008
[284] Casetti, Francesco. *Inside the Gaze*. The Fiction Film and its Spectator. Indiand University Press: Bloomington, 1998. S. 48.
[285]: „Denn ihre Sünden haben sich bis zum Himmel aufgetürmt, und Gott hat ihre Schandtaten nicht vergessen." Offenbarung 18:5. Die Bibel. S.1390.

Zu Beginn handelt es sich um die Angst vor Verbrechen, Schmerz und Verlust die den Wunsch nach Schutz auslösen. Diese Angst verwandelt sich allmählich aber in eine Bedrohung: „Einen gibt's der alles sieht..." (siehe auch: S. 90. McCahill) Der Psalm 139 (Altes Testament) dokumentiert die Zerrissenheit des Betenden und wie zwiespältig doch die Macht Gottes sein kann: Gott sieht in unsere Herzen, man kann keinen Gedanken vor ihm verstecken, kann nicht vor ihm fliehen. Dieser Psalm wirkt fast schon visionär, wenn man damit die gegenwärtige Situation beschreiben könnte. Es handelt sich dabei um einen Zustand wie die Polizei es in manchen Fällen für wünschenswert finden würde: Zu wissen was passiert, bevor es überhaupt passiert.

Psalm 139

„Der Mensch vor dem allwissenden Gott
[1] Herr, du hast mich erforscht und du kennst mich./ [2] Ob ich sitze oder stehe, du weißt von mir./ Von fern erkennst du meine Gedanken.
[3] Ob ich gehe oder ruhe, es ist dir bekannt;/ du bist vertraut mit all meinen Wegen.
[4] Noch liegt mir das Wort nicht auf der Zunge - / du, Herr, kennst es bereits.
[5] du umschließt mich von allen Seiten/ und legst deine Hand auf mich.
[6] Zu wunderbar ist für mich dieses Wissen, / zu hoch, ich kann es nicht begreifen.
[7] Wohin könnte ich fliehen vor deinem Geist,/ wohin mich vor deinem Angesicht flüchten?
[...]
[16] Deine Augen sahen, wie ich entstand,/ in deinem Buch war schon alles verzeichnet; Meine Tage waren schon gebildet,/ als noch keiner von ihnen war.
[17] Wie schwierig sind für mich, o Gott, deine Gedanken / wie gewaltig ist ihre Zahl!
[18] Wollte ich sie zählen, es wären mehr als der Sand. / Käme ich bis zum Ende, wäre ich noch immer bei dir.
[...]
[23] Erforsche mich Gott, und erkenne mein Herz, / prüfe mich, und erkenne mein Denken!
[24] Sieh her, ob ich auf dem Weg bin, der dich kränkt,/ und leite mich auf dem altbewährten Weg!"[286]

Ist der angesprochene Psalm also ein Loblied auf die Allgegenwärtigkeit Gottes, an jedem Ort und zu jeder Zeit? Oder formuliert er die Überdrüssigkeit an der „göttlichen Verfolgung", die den Psalmisten in seiner Freiheit, seiner Entscheidungsfreiheit beschneidet? Auf die Überwachung angewandt, kann man die Frage stellen, ob die Allgegenwärtigkeit der Kamera jenen „Segen" bringt, der versprochen wurde, oder ob sie als Instrument der Einschränkung, Ausgrenzung und Kontrolle eingesetzt wird.

[286] Österreichisches Katholische Bildungswerk (Hg.). Die Bibel. Einheitsübersetzung der Heiligen Schrift. Carinthia. Klagenfurt, 1986.

Die beiden letzten Verse scheinen der Realität schon nahe zu kommen. Man kann der Bevölkerung den Wunsch unterstellen, überwacht werden zu wollen. Dies beruht nicht zuletzt auf den Terroranschlägen von 9/11, den Bombenanschlägen von Madrid und London. Es könnte sich aber auch um ein „Sicherheits-Wollen" handeln, das sich weniger darin begründet, persönlichen Schutz vor Verbrechen zu gewährleisten, als darum, selbst nicht vom richtigen Weg abzukommen: „Die beiden letzten Verse (V. 23f.) erinnern uns daran, daß[!] auch wir ständiger Kurskorrektur bedürfen."[287] Ist der Blick der Kamera als moralische Ersatzinstanz für den abhanden gekommenen Glauben zu sehen?

Der Psychoanalytiker Tilman Moser (*Psychoanalytiker und Schriftsteller*) hat mit seinem Buch *Gottesvergiftung* (1980)[288] eine Art Abrechnung mit Gott in Form eines Briefes, bzw. mehr einer Anklageschrift, veröffentlicht. Er klagt darin über einen aufgezwungenen Gott, der ihn seit seiner Kindheit verfolgt und ihn nicht mehr loslässt: ein Gott der alles sieht, der immer da ist, ein Gott der Normen, der Abweichungen bestraft.

> „Aber weißt du, was das Schlimmste ist, das sie mir über dich erzählt haben? Es ist die tückisch ausgestreute Überzeugung, daß *du* [*Herv. Moser*] alles hörst und alles siehst und auch die geheimen Gedanken erkennen kannst. Hier hakte es sehr früh aus mit der Menschenwürde; doch dies ist ein Begriff der Erwachsenenwelt. In der Kinderwelt sieht das dann so aus, daß man sich elend fühlt, weil du einem lauernd und ohne Pausen des Erbarmens zusiehst und zuhörst und mit Gedankenlesen beschäftigt bist."[289]

Für Moser wird dieser Gott, den man „fürchten und lieben" sollte, ein Gott den er hasst, der für ihn eine Krankheit darstellt.

> „Herr erhebe dein Antlitz über uns...", so haben wir am Ende jedes Gottesdienstes gefleht, als gäbe es keine größere Sehnsucht, als immerzu dein ewig-kontrollierendes big-brother-Gesicht über uns an der Decke zu sehen. Du als Krankheit in mir bist eine Normenkrankheit, eine Krankheit der unerfüllbaren Normen, [...][290]

Diese „Normenkrankheit" wie Moser die dauernde Beobachtung nennt, wird auch in der Technik eingesetzt die in dieselbe Richtung arbeitet. Es sollen homogene Bilder einer Stadt produziert werden. Die Kamera beobachtet nur äußerliches und daraus wird geschlossen wer

[287] Groß. 1980. S. 401.
[288] Moser, Tilman. Gottesvergiftung. Suhrkamp. Frankfurt am Main, 1980.
[289] Moser. 1980. S. 13.
[290] Moser, 1980. S. 14.

„krank“ ist und wer nicht. Jene Elemente die nicht in ein „normales“ Stadtbild gehören, Bettler, Obdachlose und Randgruppen sollen dadurch kontrolliert und entfernt werden.

11. Wissen ist Macht

> „Gott sieht alles, hieß es einmal. Das muss ein anderes Zeitalter gewesen sein. Längst hat der Staat – und ausgerechnet der britische – sich Gottes Augen gebastelt.“[291]

Normierung ist einer jener wesentlichen Punkte, die Kritiker immer wieder ansprechen. Foucault beschreibt in *Mikrophysik der Macht* (1976), dass die Normierung das Gesetz ersetzt bzw. seine Regeln bestimmt. Moderne Kritiker wie z.B. Hans Zeger teilen diese Befürchtung einer großflächig angewandten Normierung, die eine Straffähigkeit des Anormalen mit sich bringt. Jeder Schritt außerhalb des gewohnten Rahmens (der Norm) wird als Auffälligkeit gewertet.

Michael Zinganel (*Architekturtheoretiker, Graz*) legt in seinen Untersuchungen zu *Real Crime* (2005) den Begriff des Verbrechens (der Abnorm) weitläufig aus. Er bezieht sich dabei auf „*jedes* [*Herv. Zinganel*] abweichende Verhalten, das von der Mehrheit – richtiger: von den dominanten Kräften einer Gesellschaft – kriminalisiert wird.“[292] Diese Definition beinhaltet „Einbrecher, Gewalttäter oder Mörder als auch politisch motivierte Terroristen, Revolutionäre oder Demonstranten, [...] Flüchtlinge, Arme und Obdachlose, die an bestimmten Orten unerwünscht sind.“[293] Er legt den Rahmen des Abnormen also nicht nur auf tatsächliche Verbrechen, sondern auch inkludiert auch Personengruppen die „Angst hervorrufen“. Zu diesen gehören auch Unbekannte oder Fremde: Sie weichen von der Norm ab, da sie „Spuren der Unordnung“[294] hinterlassen.

Walter Peissl (*Technikfolgenabschätzung, TU Wien*) spricht von der Wichtigkeit der „Abweichung“.[295] Langfristig wäre durch die Überwachung eine Anpassung des Verhaltens

[291] Luyken, Rainer. „Big Brother ist wirklich ein Brite“. (März 20007). (http://images.zeit.de/text/2007/03/Big-Brother) (11.10.2008).
[292] Zinganel, Michael. Real Crime. Architektur Stadt & Verbrechen. Edition Selene. Wien, 2003. S. 20.
[293] Ebenda. S. 20.
[294] Ebenda. S. 18.
[295] Peissl, Walter: Überwachung und Sicherheit: Eine fragwürdige Beziehung. (S. 73-90). In: Nentwich/ Peissl. 2005.

gegeben – ein Übergang zur Konformität der die soziale, kulturelle und wirtschaftliche Entwicklung zum Stillstand kommen lassen könnte.

> „[...] abweichendes Verhalten in unterschiedlichster Ausprägung [ist] nicht nur schlecht, sondern sogar notwendig. Es stellt ein wesentliches Momentum in Gesellschaften dar. Wird dieses unterdrückt, laufen die gesellschaftlichen Subsysteme und mit ihnen die Gesellschaft an sich Gefahr zu stagnieren. Wenn aber liberale Gesellschaften aufhören sich weiterzuentwickeln, sich zu verändern, sind sie vom Untergang bedroht. Das würde bedeuten, dass wir das Sicherheitsbestreben so hoch getrieben haben, dass wir uns ‚zu Tode gefürchtet haben' [...]"[296]

Karl Marx, zitiert nach Zinganel, spricht davon, dass der Satz „Crime doesn't pay" eigentlich falsch ist. Crime pays![297] Dabei spricht er nicht unbedingt vom Verbrecher selbst, sondern von der Gesellschaft, die vom Verbrechen profitiert: Sie sorgen für die Notwendigkeit von Polizei, Strafjustiz, Juristen, Jus-Professoren, Berichterstattung, und Medien. Das Verbrechen gibt der Polizei letztlich ihre „Existenzberechtigung".

Der Grund für den „Wissensdurst" der modernen Gesellschaft ist Macht die damit einhergeht. Wissen bringt Macht mit sich, und diese schafft Wissen.[298] „Und Wissen wiederum helfe, die Kontrolle auszuweiten."[299] In diesem Sinne

> „[...] bringt die Ausübung von Macht Wissensgegenstände hervor; sie sammelt und verwertet Informationen. Man versteht nichts vom ökonomischen Wissen, wenn man nicht weiß, wie sich die ökonomische Macht im täglichen Leben durchsetzt. Die Machtausübung bringt ständig Wissen hervor und umgekehrt bringt das Wissen Machtwirkungen mit sich. [...] es ist nicht möglich, daß sich Macht ohne Wissen vollzieht; es ist nicht möglich, daß das Wissen nicht Macht hervorbringt[.]"[300]

Je mehr man also über die Bevölkerung weiß, desto einfacher ist es, soziale Kontrollen und Normen einzuführen. Sind diese Normen einmal etabliert, ist es schwierig sie wieder rückgängig zu machen. In Fällen der Videoüberwachung sind die Überwacher, in

---

[296] Peissl. 2005. S. 87.
[297] Karl Marx. *Theorien über den Mehrwert. Erster Teil*, in: Karl Marx u. Friedrich Engels. *Werke*. Bd. 26.1, Berlin, 1985 zit. nach: Zinganel, Michael. 2003. S. 14ff. („Der Verbrecher produziert ferner die ganze Polizei und Kriminaljustiz, Schergen, Richter, Henker, Geschworene usw.; und alle diese verschiedenen Gewerbszweige, die ebenso viele Kategorien der Gesellschaftlichen Teilung der Arbeit bilden, entwickeln verschiedene Fähigkeiten des menschlichen Geistes, schaffen neue Bedürfnisse und neue Weisen ihrer Befriedigung." Marx, Karl. *Theorien über den Mehrwert* in: Zinganel. 2003. S. 14).
[298] Siehe: Foucault, Michel. *Mikrophysik der Macht. Über Strafjustiz, Psychiatrie und Medizin*. Merve: Berlin, 1976. S. 45.
[299] Zinganel. 2003. S. 44.
[300] Foucault. 1976. S. 45.

halbprivaten oder öffentlichen Räumen (im Sinne von Einkaufszentren, Einkaufsstraßen, Plätze, Parks;), diejenigen, die Macht ausüben und Normen festlegen. Unerwünschte Personen, d.h. Personen, die nicht dem Profil der „Norm", z.B. dem eines Konsumenten entsprechen, können somit als anormal qualifiziert und „aussortiert" bzw. ausgegrenzt werden.

11.1. „Beyond Foucault and Bentham"

On the Threshold to Urban Panopticon? Dies war die Ausgangsfrage des URBANEYE-Projekts war. Es geht auch darum, ob es wirklich noch *Bentham's Panopticon* ist, mit dem sich die Überwachungsgesellschaft auseinandersetzen muss. David Lyon,[301] (*Professor für Soziologie, CAN*) hält dazu allerdings fest: „Whatever one may learn from Jeremy Bentham's Panopticon or George Orwell's totalitarian telescreen technology, it is not clear if these are entirely helpful ways of understandig surveillance today."[302] Er glaubt nicht, dass der Vergleich mit Benthams Panoptikon des 19. Jahrhunderts heutzutage noch adäquat ist, vor allem wenn man die Mobilität und die technischen Möglichkeiten miteinbezieht. Mark McCahill (*Systemarchitekt im Büro für Informationstechnologie, Duke University*) führt diesen Gedanken weiter und meint, man müsse darüber hinaus, „beyond Foucault", gehen – denn das Panopticon sei viel mehr als die bloße Verwirklichung einer architektonischen Darstellung:

> „It implies at its ‚heart' already ‚the collection of individualized codified information'. As the deviant is segregated from society, the panopticon is 'exclusionary' as well as 'inclusionary'. It provides a 'rationale for social classification'."[303]

Das Panopticon blickt nicht mehr nur nach innen, sondern auch nach außen. Erwin Möchl erklärt die Videoüberwachung als eine Technik, die für Gefängnisse entwickelt wurde, und die nunmehr in den öffentlichen Raum hineinwirkt, ihn überwacht und die Bevölkerung zu potentiellen Verbrechern macht.[304]

---

[301] Professor David Lyon beschäftigt sich sein den 1980er Jahren mit Überwachung. Seine diversen Tätigkeiten sind ua. Principal Investigator of the "Globalization of Personal Data Project" (http://www.surveillanceproject.org/people/lead_researchers) (15.07.2008)
[302] Hempel/Töpfer. 2004. S. 19
[303] Ebenda. S. 19.
[304] Erich Möchel bei der Präsentation von *Faceless* im Top-Kino am 02.05.2008.

Der Blick löst sich vom panoptischen Blick innerhalb des Gefängnisses und begibt sich nach außen in die Öffentlichkeit. Die Videoüberwachung „erfasst [...] den Menschen als Ganzes, macht sein Verhalten umfassend transparent und sichtbar“[305], und zeigt wer „innerhalb“ und wer „außerhalb“ ist, wer der Norm entspricht und wer sich „abnorm“ verhält. Sie schließt nicht mehr nur aus (Verbrecher – im Gefängnis – aus der Gesellschaft), sondern auch ein („Einschluss“ – in Form der Kategorisierung – in eine Gruppe), und bildet somit eine Form der (sozialen) Klassifikation.

> „In fact the safety promise of a camera’s eye can turn out to be a risk itself as certain forms of social control and solidly action could be displaced by the use for the technology.”[306]

Die Kategorisierung in bestimmte Gruppen kann gesellschaftlich relevante Auswirkungen haben. „Es geht um die Beeinträchtigung von realen Lebenschancen aufgrund virtueller Merkmalszuschreibungen, um soziale Gerechtigkeit, um digitale Diskriminierung.“[307] Es könnten aus diesen Einteilungen, durch falsche Zuteilung, negative Auswirkungen für die jeweilige Person entstehen.

11. *VISION* und *VISIBILITY*

URBANEYE hat die Überwachungssysteme in zwei individuelle Systeme geteilt, in

- „vision (the capacity to make those under surveillance visible to an observer in real-time)“

und

- „visibility (the capacity to induce the feeling of being under the gaze of a camera)“.[308]

Es wird also zwischen der tatsächlichen Beobachtung und dem Gefühl des Beobachtet-Werdens unterschieden. Das Gefühl der Beobachtung alleine soll die Menschen schon

[305] König. In Jahnel. 2007. S. 109.
[306] Hempel/Töpfer. 2004. S. 50.
[307] Peissl, Walter. 2008. S. 136.
[308] Siehe: Hempel/Töpfer. 2004. S. 7.

„disziplinieren". „Sie ‚wirkt' aus dieser Sicht sogar, wenn sie gar nicht in Betrieb ist – denn auch die potentielle Überwachung kann schon Präventionseffekt haben."[309]

In einer Umfrage wurde festgestellt, dass sich vor allem junge Menschen als diejenige Gruppe ansehen, die „diszipliniert werden soll"[310] und die ihr Verhalten durch Videoüberwachung beeinflusst sehen. Auswirkungen lassen sich vor allem in „unerwünschten Verhaltensänderungen" feststellen, die sich durch das „Wissen um die Transparenz der eigenen persönlichen Daten und Profile"[311] erst manifestieren, als

> „[...] der subtile Zwang zum Konformismus, das Mainstreaming und die damit einhergehenden Folgen für die Gesellschaftliche und kulturelle Vielfalt und die ökonomische Entwicklung. Ein[!] zunehmend aktuelle Dimension betrifft das sog[!] ‚social sorting'"[312]

Bei den durchgeführten Umfragen von URBANEYE wurde ein Satz vorgebracht, der im Diskurs um den Datenschutz sehr häufig auftritt: „Who has nothing to hide, has nothing to fear from CCTV."[313] *Wer nichts verbrochen hat, muss sich nicht vor Überwachung fürchten!* Es erweist sich bisweilen als schwierig dagegen zu argumentieren, wenn jemand sagt, es mache ihm nichts aus auf der Straße gefilmt zu werden. Oder: Jeder dürfe seine Daten wissen, denn er habe nichts zu verstecken. Abgesehen davon, dass zwei Drittel der Befragten dieser Aussage zugestimmt haben, muss entgegengehalten werden, dass 53% der Befragten auch Angst davor haben, dass dieses Material missbräuchlich verwendet werden könnte.[314] Besonders wichtig war den Befragten, dass Videomaterial von Überwachungskameras nicht an Medien oder zu Werbezwecken weitergegeben werden dürfe.[315]

Das hierbei auftretende Problem ist **nicht** von einer Kamera beim Einkauf oder auf der Straße gefilmt zu werden, sondern die Art und Weise wie unser Recht auf Privatsphäre Stück für Stück beschnitten wird. Es gibt immer weniger Bereiche, in denen Privatsphäre noch privat bleibt, ob es sich dabei um Googles Street View handelt oder um WebCams in Lokalen, Daten die auf Kundenkarten oder der *e-card* gespeichert sind oder „Schnüfflereien" auf privaten Homepages. Die Bevölkerung wird einem „präventiven" Generalverdacht ausgesetzt und jeder wird als potentieller Verbrecher angesehen. Der oben genannte Satz sollte eigentlich

[309] Müller, Henning. „Zur Kriminologie der Videoüberwachung". *Monatsschrift für Kriminologie*. 2002/2. S. 34.
[310] Siehe: Hempel/Töpfer. 2004. S. 8.
[311] Nentwich/Peissl. Gesellschaftliche Risiken von öffentlichen Registern. In: Reiter/Wittmann-Tiwald. 2008. S. 43.
[312] Ebenda S. 43.
[313] Hempel/Töpfer. 2004.. S. 45
[314] Siehe: Ebenda. S. 45
[315] Siehe: Ebenda. S. 47

umformuliert werden: *Ich habe nichts verbrochen, warum sollte ich also überwacht werden?!*[316]

Abb. 27: Jerry Scott/ Jim Borghman. Zits-Cartoon. Man muss nicht unbedingt etwas zu verbergen haben, nur weil man nicht will, dass in seine Privatsphäre eingedrungen wird.

Mehr als die Hälfte der Befragten glaubte, dass Verbrechen durch Videoüberwachung nur verlagert wird und nicht vor „serious offences“ [317] schützen kann. Eine in der Vergangenheit oft praktizierte Möglichkeit, die Wirksamkeit von CCTV-Systemen zu werten, war die Analyse von Kriminalitätsstatistiken. Diese Methode wird mittlerweile von Experten (URBANEYE) aber als unzureichend angesehen, vor allem wenn es darum geht, ein korrektes Bild der Situation zu zeigen. („It is doubtful how professional the crime statistics evaluations are.“[318])

> „[...] several criminologist contest the analysis of crime statistics as an instrument for CCTV evaluation as they point out that registered crime do not necessarily reflect actual crime and victimisation.“[319]

Dadurch dass Verbrechen durch CCTV-Einsatz zumeist nur in Außenbezirke oder andere Städte verdrängt wird kann die Statistik nicht wiedergeben welche Auswirkungen auf welche Maßnahmen zurückzuführen sind. Ein Rückgang der Verbrechensrate muss auch nicht zwingend bedeuten, dass sich die Situation in den Bezirken verbessert, sondern vielleicht auch nur die Art der Verbrechen verlagert hat.

[316] Hans Zeger. Diskussion im Top-Kino. 04.05.2008.
[317] Siehe: Hempel/Töpfer. 2004. S. 9
[318] Ebenda. S. 14.
[319] Ebenda. S. 11.

11.3. Vernetzung von Systemen

Die Gefahr die durch CCTV-Systeme bzw. Videoüberwachung generell besteht, ist die des Missbrauchs bzw. der Verwendung außerhalb des ursprünglich beabsichtigen Zweckes („function creep"): „However, the potential of expandable mutability characterises the use of CCTV because – once in place – other forms of use might occur."[320] Diese *other forms of use* sind in Verbindung mit wireless-Systemen und einem Versuch der Gruppe *Quintessenz* (siehe S. 77) schon erwähnt worden.

In Zeiten des einfachen Datenaustausche sollten kleine Systeme aber nicht unterschätzt oder marginalisiert werden. Die Vernetzung von Systemen kann zu einem Problem werden, wenn sich dadurch ein komplexes soziales und technologisches Netzwerk ergibt, dessen Grenzen nicht mehr erkennbar sind und über das wiederum nur schwer Kontrolle auszuüben ist.[321]

> „½ of all systems employ a linkage to other systems. 50% of all systems with more than 10 cameras are linked to others by either switching images (33%) or some kind of communication link (46%)."[322]

Dass es derartige Verbindungen schon gibt, unterstrich Prof. Mayer-Schönberger bei der Tagung der Juristen in Linz 2007. Der in Amerika lebende Professor hatte nach einer Geschwindigkeitsübertretung einen Strafzettel bekommen. Kurze Zeit später erhielt er einen Brief von seiner Versicherung die seine Prämie erhöht hatte, mit der Begründung er sei ein „risikoreicher" Autofahrer.[323] Um Beispiele für Vernetzungen zu finden muss man allerdings nicht auf die USA zurückgreifen, denn es gibt sie auch in Österreich:

Ein gravierendes Problem entsteht wenn in vernetzte Daten zentral eingesehen werden kann, seien es Schulakten, Krankenakten, Polizeiakten, Melderegister o.ä. Im österreichischen Bildungsdokumentationsgesetz wird seit 2003 festgehalten, dass die Noten von Schülern über 60 Jahre lang gespeichert und an die Sozialversicherungsnummer geknüpft werden.[324] Die *e-card*, die eine Vereinfachung ärztlicher Behandlungen ermöglichen sollte, stellte sich als riesiges Datenschutzproblem heraus: Es wurden Daten über das Anstellungsvermittlungsverhältnis vom AMS unberechtigt an die Sozialversicherung

[320] Hempel/Töpfer. 2004. S. 6.
[321] Siehe: Hempel/Töpfer. 2004. S. 6-7.
[322] Hempel/Töpfer. 2004. S. 32.
[323] Viktor Mayer-Schönberger. Vortrag im Rahmen des *Goodbye Privacy Symposiums* zum Thema: „Grundrechte in einer digitalen Welt". (05.09.2007).
[324] Dafür bekam die Bundesministerin Elisabeth Gehrer den *Big Brother Award 2003*. Der *Big Brother Award* wird jenen Institutionen, Firmen oder Personen verliehen, die sich durch bereits gesetzte oder angekündigte Maßnahmen besonderer Datenschutzverletzungen bzw. –einschränkungen „rühmen" dürfen.

weitergegeben. In einigen Fällen hatte dies zur Folge, dass die Karte gesperrt wurde, obwohl noch ein Anspruch auf Sozialversicherung gegeben war.[325] Darüber hinaus konnten Beamte sowie private Versicherungen in gespeicherte Privatdaten einsehen.[326] Das Gesundheitstelematik-Gesetz verpflichtet zudem Ärzte, den Sozialversicherungen über das Alkoholkonsumverhalten der Patienten Auskunft zu geben.[327]

11.4. Soziale Kontrolle

Es stellte sich bei den Recherchen heraus, dass mit der Videoüberwachung nicht nur Kriminalität bekämpft werden sollte, sondern auch die Angst vor Kriminalität. Die Menschen sollten sich sicherer fühlen durch die Anwesenheit der Kamera. Angsträume sollte so entschärft werden. Zusätzlich wird es aber immer stärker als Instrument sozialer Kontrolle eingesetzt. Unerwünschte Personengruppen sollen damit ferngehalten werden, oder rechtzeitig entdeckt werden um sie zu „entfernen".

11.4.1. Angsträume

Anfang 1970 wurden in England Protestmärsche unter dem Motto „Take Back the Night" veranstaltet. Diese Protestkundgebungen wurden von Frauen veranstaltet die darauf hinweisen wollten, dass es Orte gibt, die immer noch als Angsträume empfunden werden.[328] Der Angstraum ist nicht als Angst vor dem Raum an sich zu verstehen, sondern jene Angst „unbeobachtet durch soziale Kontrolle Opfer eines Menschen zu werden."[329] Effekte, die diese Situation entschärfen, sind laut Dörte Kuhlmann (*Professorin für Architekturtheorie, TU Wien*), verstärkte Parkkontrollen, bessere Beschilderung, Beleuchtung u.ä.[330]

---

[325] Siehe: Arge-Daten. „Schörghofer räumt Datenschutzprobleme bei der e-card-Administration ein". (06.06.2005) (http://www2.argedaten.at/session/anonym811192tsssio549116.E42_INP.html) (20.09.2008).
[326] *Big Brother Award 2005* für Gesundheitsministerin Maria Rauch-Kallat für die *Schaffung des gläsernen Patienten samt Alkoholikerdatenbank* im Gesundheitstelematik-Gesetz.
[327] Siehe: *Big Brother Awards 2005*. (http://www.bigbrotherawards.at/2005/Pressetexte.html) (20.09.2008).
[328] Siehe: Kuhlmann, Dörte. Raum, Macht & Differenz. Genderstudien in der Architektur. Edition Selene. Wien, 2005. S. 190.
[329] Kuhlmann. 2005. S. 191.
[330] Siehe: Kuhlmann. 2005. S. 208f.

Das Projekt URBANEYE untersuchte nicht nur den Faktor Kriminalität, sondern eben auch die Angst vor Kriminalität. Für die Bevölkerung und die Wohnqualität einer Stadt ist das von großer Bedeutung. Durch Videoüberwachung wird versucht, diese Angsträume zu entschärfen. Sie sollen dem Stadtgebiet als „nutzbarer Raum" wieder „zurückgegeben"[331] werden und den Menschen ein Sicherheitsgefühl vermitteln. Videoüberwachung trägt zur Entschärfung von Angsträumen allerdings nur wenig bei.

> „Though CCTV schemes are among others often justified by the claim to make people safer, the surveys so far indicate that its effects on the fear of crime are marginal."[332]

Im Bericht von Frank Helten und Bernd Fischer (*URBANEYE*) wiederum,[333] wird vom Gegenteil gesprochen.

> „Thus it appears that the overall and most interesting social effect of CCTV is that most of the people feel safer."[334]

Allerdings gilt dies nur mit der Einschränkung, dass z.B. der Technologie mehr Vertrauen entgegengebracht wird als dem bedienenden Personal. Dabei handelt es sich vorwiegend um die Angst der Bevölkerung davor, nicht zu wissen mit welcher Absicht und welchen Methoden gearbeitet wird. Helten und Fischer erklären, dass diese Ängste als eine Demütigung des Körpers, der Individualität und Einschränkung der Identität gesehen werden.[335]

> „If this is so, then we evenly have to state that the benefit of feeling safer is accompanied by a process of alienation which probably causes further uncertainty.
> […]
> Others […] are oriented to take CCTV as sign for additional protection or for additional control." [336]

Die Ambivalenz der Videoüberwachung besteht also darin, dass nicht nur das Sicherheitsgefühl aufgewertet, sondern gleichzeitig auch eine Einengung der persönlichen Freiheit vermittelt wird, nämlich in Form von zusätzlicher Kontrolle.

---

[331] Hempel/Töpfer. 2004. S. 20.
[332] Ebenda. S. 18.
[333] Siehe: Helten/ Fischer. „What people think about CCTV in Berlin". (Februar 2003) (http://www.urbaneye.net/results/results.htm) (13.05.2008).
[334] Ebenda. S. 50.
[335] Siehe: Ebenda. S. 50.
[336] Ebenda. S. 50 ff.

Die Gründe, die URBANEYE für den Einsatz von Videoüberwachung ermittelte, liegen mit 86% bei „Vorbeugung und Verhinderung von Diebstählen", gefolgt von „Verbesserung von Diensten" (16%) und „Feuersicherheit" (5%)."[337] Abgesehen vom Risikomanagement (Tunnelsicherheit, Verkehrsinformation, Unfälle, und oben genannte Beispiele) wurde auffällig, dass die Erfassung von „abweichendem Verhalten wie unerlaubten Zutritten, so genanntem ‚anti-sozialen Verhalten' und Kriminalität"[338] als Grund immer häufiger genannt wurde.

> „Der Abgleich unserer Umfragedaten [...] zeigt, dass die Mehrheit der Überwachungssysteme darauf ausgerichtet ist, abweichendem Verhalten vorzubeugen, durch symbolische, aber mehr oder weniger unvollständige Abschreckung, weil die Kameras stark sichtbar sind, aber die überwachten Personen für den Überwacher kaum, was an der unregelmäßigen Beobachtung, Informationsüberfluss und auch dem Einsatz von Kamera-Attrappen liegt[!]. Trotzdem speichern mehr als drei Viertel (78%) der Überwachungssysteme das Filmmaterial dauerhaft."[339]

Die Distanz zwischen den Beobachtern und den Beobachteten kann allerdings dzu führen ganze Bevölkerungsgruppen unter Verdacht fallen zu lassen.

> „Thus, operators might tend to target whole categories of the public seen as likely criminals or nuisances.[…] In particular the growth of CCTV in semi-private spaces such as shopping malls bring with it an increasing emphasis on exclusion as dominant strategy of social control […] as it is reported from Oslo and London."[340]

Die Vorgaben der Betreiber spielen dabei eine genauso wichtige Rolle wie die Vorurteile der Videooperatoren selbst. Zinganel gibt hierfür ein hartes, aber gleichzeitig amüsantes Beispiel an: Um Zeit außerhalb des Seniorenheimes zu verbringen und „unter die Leute zu kommen" verbrachten Senioren ihre Zeit in einem Einkaufszentrum. Das sie nichts konsumierten wurden sie von der Geschäftsleitung hinausgeworfen. Um einem zukünftigen Rauswurf aus dem Einkaufszentrum zu entgehen „tarnten" sie sich mit Einkaufstüten.[341]

---

[337] Siehe: Hempel/Töpfer. 2004. S. 5.
[338] Hempel/Töpfer. „Videoüberwachung in Europa. Abschlussbericht." (August 2004) (http://www.ztg.tu-berlin.de/pdf/URBANEYE_Abschlussbericht_Zusammenfassung_dr.pdf) (12.06.2008) S. 5.
[339] Ebenda. S. 6
[340] Hempel/Töpfer. 2004. S. 7.
[341] Siehe: Zinganel. 2003. S. 245.

12. Maßnahmen ohne Videoüberwachung

CCTV wird als ein restrukturierendes Element bzw. Werkzeug verstanden, das vor allem für den wirtschaftlich nutzbaren Raum entdeckt worden ist. Es handelt sich dabei um einen Raum der vor allem für Touristen und Konsumenten „zurückgewonnen“[342] werden soll. Hier entsteht die Gefahr, Räume ausschließlich für ökonomische Zwecke zu „verbrauchen“. Damit wird allerdings, wie Alan Reeve (*Joint Centre for Urban Design; Oxford Brookes University*) es versteht, das Potential eines öffentlichen Platzes um seinen Charakter beraubt. Der öffentliche Platz wird zur homogenisierten Zone,[343] in der die Öffentlichkeit und Personen, die sich darin aufhalten, klassifiziert werden, mit dem Ziel der Ausschließung unerwünschter sozialer Gruppen.

> „Within the entrepreneurial city, it is said, that the managing of urban space means to classify people according to their economic purchasing power. According to this visual surveillance could become a tool of social exclusion. […] A certain behaviour and appearance is asked for in order to participate on the playground of leisure and consumption. Within this context of surveillance potential of CCTV turns out to be one of ‘social sorting’.”[344]

12.1. Beleuchtung

Beleuchtung wird als der Möglichkeiten angesehen die eine Abwendung von Videoüberwachung von Plätzen und Parks herbeiführen könnte. Durch verstärkte Beleuchtungsmaßnahmen können Angsträume entschärft werden. Dies ist eine Aufgabe, die der Architektur zufällt.

Ende des 17. Jahrhunderts gab es in Paris „Beleuchtungsinspektoren“, die mit dem Ziel eingesetzt wurden, den Parisern die Angst zu nehmen abends noch auszugehen.[345] Ein anderes interessantes Beispiel gibt es aus dem Jahr 1925: Es handelt sich dabei um ein Werbeplakat, in dem ein Polizist, dargestellt als personifizierte Glühbirne, einen Verbrecher jagt. Die Verbindung von Beleuchtung und Sicherheit wird dabei in einen kausalen Zusammenhang gesetzt.

[342] Hempel/Töpfer. 2004. S. 20.
[343] Ebenda. S. 20.
[344] Ebenda. S. 20f.
[345] Virilio, Paul. Die Sehmaschine. Merve. Berlin, 1989. S. 30.

In der historischen Werbung von Osram (1925) wird auch die Perfektionierung der städtischen Beleuchtung als Folge der Produktivkraft des Verbrechens dargestellt. Die städtische Beleuchtung eröffnete den Bewohnern einen neuen urbanen Erfahrungsraum, machte aber gleichzeitig auch all das sichtbar, vor dem sich das neue Establishment abzugrenzen versuchte – das also fortan verdrängt, diszipliniert, einer Besserung und Normierung unterzogen werden mußte.

Abb. 28: Sicherheit und Beleuchtung.

Die Überwachungskamera hat also eine ähnliche Funktion angenommen wie die Beleuchtung. Beiden wird ein „erhellender" Faktor zugeschrieben: „Die Videoüberwachung repräsentiert [...] nichts weiter als die Perfektion der städtischen Beleuchtung als Medium der Überwachung."[346]

Licht und Sichtbarkeit stellen das Medium der Sicherheit und Überwachung dar. Die Architektur, so Zinganel, reagiert darauf mit „passiven Überwachungsmechanismen", durch

- Einsehbarkeit von Räumen und Gebäuden
- Verzicht auf versteckte Winkel
- Beleuchtung im gesamten Stadtgebiet (auch in Kellern, Parkgaragen u.ä.)

> „Dieses Modell der ‚sicheren' Stadt besteht aus Glas und Licht, der Wachdienst wird von der gesamten Bevölkerung übernommen."[347]

Samjatin hat eben genau diese Art der Kontrolle in seinem Roman *Wir* eingebaut: eine Stadt in der Häuser nur Glasfassaden haben, in der nichts versteckt werden kann, in der jeder jeden kontrolliert,

[346] Virilio. in: Zinganel. 2003. S. 17.
[347] Zinganel. 2003. S. 36. (Siehe auch: S. 71. Samjatins Gebäude in *Wir* bestehen aus einsehbaren Glasfassaden.)

12.2. Ausschlussmechanismen

Um ungewünschte Personen zu vertreiben, gibt es mehrere Möglichkeiten, wie z.B. den Einsatz von Wachdiensten oder der Polizei. Mitunter führt die architektonische GEstaltung dazu, dass bestimmten Personengruppen der Zugang erschwert wird, oder die Bedingungen diesen Gruppen den Aufenthalt den Räumen verleidet. Kuhlmann bezeichnet diese Form der Architektur als Separationsarchitektur:

> „Extreme Ausschluss- und Separationsarchitekturen sind Gefängnisse, die, nach Geschlecht oder Art des Verbrechens getrennt, Individuen beinhalten, deren Verhalten seitens des Gesetzgebers als nicht gesellschaftskonform gewertet wird, oder Krankenhäuser, die nicht nur eine medizinische Versorgung der Kranken bieten, sondern gleichzeitig die kranken Körper von den gesunden Körpern fernhalten. Das Ziel besteht darin, Individuen auszugrenzen, weil sie entweder größere oder geringere Privilegien genießen als der Rest der Gemeinschaft, wobei die Separationsarchitekturen physisch und symbolisch diese Trennung untermauern.“[348]

Als ein Negativbeispiel in Wien führt Kuhlmann ein Wohnprojekt von Carl Pruscha an (Wien, Traviatagasse;). Die Konzeption des Gebäudes schottet die Bewohner der unteren Geschosse visuell ab. Sie können „somit nicht am öffentlichen Leben teilhaben.“[349] Die *fehlende* soziale Kontrolle (in Form von fehlender Beteiligung am sozialen Leben) kann zu Angsträumen führen, die eine Einschränkung für bestimmte Personengruppen zur Folge haben können.[350]

Einkaufszentren werden z.T. mit Kriminalität und Angst verbunden die auf herumlungernde Jugendliche, Betrunkene und Bettler projiziert wird. Dies kann sich darin auswirken, dass bereits „herumlungern“ verboten ist und zum Rauswurf führen kann.[351] Nicht-kaufkräftigen Kunden kann ein ähnliches Schicksal widerfahren.
Um Leute zu vertreiben werden nicht nur Sicherheitsdienste eingesetzt, sondern auch sehr subtile Methoden angewandt:

---

[348] Kuhlmann. 2005. S. 186.
[349] Ebenda. S. 191.
[350] Kuhlmann führt hier Hausfrauen, Kinder und ältere Frauen, die sich z.B. in der Nacht nicht mehr aus dem Haus wagen. Dies kann massive Einschränkungen in Bezug auf das soziale Leben der betroffenen Personen haben. (Kuhlmann. 2005. S. 191f.)
[351] Siehe: Sibley, David in: Kuhlmann. 2005. S. 194.

- In einigen deutschen Einkaufszentren kann die Klimaanlage so eingesetzt werden, dass bestimmte Teile des Raumes besonders zugig sind, um unerwünschten Personen den Aufenthalt in den Räumlichkeiten zu verleiden.
- Dasselbe kann mit gezielter Einspielung von „unerträglicher" Musik funktionieren:[352]

> „Hierfür soll sich, so deutsche Experten, österreichische Volksmusik sehr bewährt haben, zum Beispiel Hansi Hinterseer, *Du ich mag Dich*, BMG Ariola (1999), produziert von Karl Moik, dem Erfinder des *Musikantenstadl*. [*Herv. Zinganel*]"[353]

- In den neuen Wiener U-Bahnstationen wurden Sitzbänke durch Armlehen getrennt. Damit bieten sie den Obdachlosen keine Möglichkeit mehr darauf zu schlafen, da.[354]
- Im Praterbahnhof gibt es im Erdgeschoss zwar über 40 Kameras, aber keine Sitzmöglichkeit
- In deutschen Bahnhöfen werden Putztrupps als „Rausschmeißer" eingesetzt, die über Videoüberwachungszentrale Anweisungen bekommen und unerwünschten Personen solange „hinterher putzen" bis diese „freiwillig" das Gebäude verlassen.[355]

[352] Siehe: Zinganel. 2003. S. 274ff.
[353] Zinganel. 2003. S. 276. „Der vermeintliche Widerspruch zwischen der ernormen Popularität dieser Lieder und ihrer Unerträglichkeit liegt in der physischen und psychischen Befindlichkeit der Ziel-personen, die deren relativ hohe Frequenzen und die radikale Melancholie nicht ertragen können." Ebenda. S. 277.
[354] Siehe: Kuhlmann. 2005. S. 198.
[355] Siehe: Zinganel. 2003. S. 274ff.

Schlussbemerkung

Scotland Yard hat im Mai 2008 bestätigt, dass der Einsatz von Videoüberwachung in der Praxis nicht zu jenen Ergebnissen geführt hat die man sich gewünscht hatte. CCTV-Fails – „Billions spent on CCTV have failed to cut crime and led to an ‚utter fiasco', says Scotland Yard surveillance chief". [356] In Zonen, die von hunderten Kameras eingesehen werden können, ließ sich sogar ein Anstieg von Diebstählen und Gewaltverbrechen nachweisen. Die Polizei begründet diesen Zuwachs damit, dass Verbrecher sich nicht vor den Kameras fürchten. Des Weiteren ist die Verbrechensaufklärung durch Überprüfen der Videoüberwachungsbänder mit einem derartig hohen Arbeitsaufwand verbunden, den die Polizei z.T. gar nicht mehr durchführen kann.[357] Die Aufklärungsrate der Londoner Polizei kommt bei Straßendiebstählen dabei nur auf 3%. Der Information Commissioner Richard Thomas hatte schon 2004 den geringen Widerstand der Bevölkerung kommentierend, vor der Bedrohung der Überwachungsgesellschaft gewarnt: „[...] the UK is in danger of ‚sleepwalking into a surveillance society'."[358] Der Schlafwandel in die Überwachungsgesellschaft hat sich durch fehlenden Widerstand fortgesetzt: Die Überwachung wird nicht mehr als Einschränkung gegenüber der eigenen Privatsphäre gewertet, sondern wird hingenommen und akzeptiert.[359]

Verbrechensbekämpfung – jenes Wort, das mit Videoüberwachung als beinahe brüderliches Paar einherging – hat seine Glaubwürdigkeit als Argument für die Überwachung mittlerweile eingebüßt, obwohl es in den Köpfen vieler Briten immer noch unverändert als Maßnahme gilt. Als das Home Office die Fakten über den CCTV-Einsatz vorlegte, wurde es in der britischen Presse als „fiasco" bezeichnet. Die geringe Effizienz von CCTV-Systemen konnten die Milliarden-Investitionen die ihnen gegenüberstehen, nicht rechtfertigen konnten.

---

[356] Bates, Daniel. „Billions spent on CCTV have failed to cut crime and led to an ‚utter fiasco', says Scotland Yard surveillance chief". *Dailymail* (06.05.2008) (http://www.dailymail.co.uk/news/article-564240/Billions-spent-CCTV-failed-cut-crime-led-utter-fiasco-says-Scotland-Yard-surveillance-chief.html) (12.05.2008).

[357] „[Chief Detective Inspector] Neville […] claimed officers can't be bothered to seek out CCTV images because it's 'hard work'." Ebenda.

[358] Ford, Richard. "Beware rise of Big Brother state, warns data watchdog". (16.08.2004) *Times-Online.* (http://www.timesonline.co.uk/tol/news/uk/article470264.ece). (05.10.2008).
Das Information Commissioner's Office (ICO) hat dieselben Aufgaben und Pflichten wie die DSK bzw. der Vorstand. (Siehe auch: Freedom of Information. „What is an Information Commissioner". (http://www.foi.gov.ky/pls/portal/docs/PAGE/FOIHOME/INFORMATION%20COMMISSIONER%20BROCHURE.PDF) (15.10.2008).

[359] Siehe: Peissl. 2008. S. 135.

> „[...] there was a lack of realism about what could be expected from CCTV. In short, it was oversold – by successive governments – as the answer (indeed the 'magic bullet' […]) to crime problems.[360]

Der Einsatz von CCTV hatte in England zur Folge, dass Polizeistreifen eingespart wurden. Die Statistiken über die Auswirkungen konnten allerdings nicht den versprochenen Erfolg vorweisen. Anstelle von mehr Sicherheit (und verstärkter Polizeipräsenz) bekam die Bevölkerung mehr Kameras. Die Begründung für diese Handlungsweise dürfte sich darin finden lassen, dass es kostengünstiger war eine CCTV-Anlage zu finanzieren als Gehälter für Polizisten zu bezahlen. Der Schluss der daraus gezogen werden kann ist wohl: „Es ist billiger – jedoch nicht effizienter."[361] Trotz der Eingriffe in ihre Privatsphäre, scheint die positive Einstellung zur Videoüberwachung bei den Briten ungebrochen zu sein.[362]

> „[…] they [the public; *Anm. Fürst*] were still predominately in favour of its use [CCTV; Anm. Fürst]. Even though they concluded that it did not reduce crime, there was no pressure to have it removed, and there were no major concerns, once people had experienced CCTV, about infringement of civil liberties."[363]

> „Wie ist das alles möglich – wie konnte die Heimatinsel liberaler Bürgerfreiheit innerhalb weniger Jahre zum rabiatesten Überwachungsterrain der westlichen Welt mutieren, zum größten Freilandversuch staatlichen Generalverdachts gegen die Bürger?"[364]

Manu Luksch hat mit ihrer Arbeit nicht den Versuch gemacht, CCTV auf seine Verbrechenswirksamkeit zu testen, sondern zu aufzuzeigen, dass wir ständig überwacht werden. Sie meint, um dieses System zusammenbrechen zu lassen bzw. auf jenes Maß zu reduzieren das vernünftig erscheint, müsse der Bürger von seinem Recht gebrauch machen, einzufordern was ihm zusteht, nämlich Einsicht in die Daten zu nehmen. Je mehr von diesem Recht gebrauch gemacht wird, desto weniger können sich die Firmen leisten, Kameras weiterlaufen zu lassen die nicht unbedingt nötig sind.

---

[360] Gill, Martin/Spriggs, Angela. *Home Office Research Study 292. Assessing the impact of CCTV*. 2005. (www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf) (10.08.2008). S.116.
[361] Peissl. 2008. S. 135.
[362] Clark, Ross. "Big Brother? Hardly. The CCTV cameras don't work – and actually make crime even worse". (07.05.2008) *Dailymail* (http://www.dailymail.co.uk/news/article-1018394/Big-Brother-Hardly-The-CCTV-cameras-dont-work--actually-make-crime-worse.html) (12.05.2008).
[363] Gill, Martin, Spriggs, Angela. Home Office Research Study 292. Assessing the impact of CCTV. 2005. (www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf) (10.08.2008). S. 117.
[364] Ebenda.

Man wird überall beobachtet, gesehen, registriert, verzeichnet, vernetzt, verlinkt. Illegale Datenzugriffe, Datenweitergaben und Datendiebstähle geben mehr und mehr von unserem Privatleben preis, ohne dass wir es wissen oder kontrollieren können.
Es sind nicht nur Videoüberwachung und Internet, es sind RFID Chips in unseren Pässen, es Gesichts-Erkennungprogramme (Facial-Recognition), DNA-Datenbanken, Finger- und Iris-Scans, die im Namen der Terrorabwehr zum Einsatz kommen. Die permanent heraufbeschworene Bedrohung durch Terroranschlägen erwachsen könnte, ist aber jenes Werkzeug mit dem unsere Rechte beschnitten werden. „Those with the darkest nightmares, became the most powerful!“[365] Es ist genau *diese* Entwicklung die die Bevölkerung fürchten sollte.

In den Unterhaltungsmedien bekommen die Mehoden der Überwachung einen positiven Spin versetzt, werden geradezu pervertiert. In Reality-Shows wie *Big Brother* oder *Taxi Orange* werden Kameras naturalisiert und als Alltagsgegenstände verharmlost. Zinganel sieht in diesen Reality-Shows eine neue Form der Überwachungsgesellschaft.[366]
Im speziellen Fall einer Kriminalserie werden die Datenschutzrechte mit Füßen getreten: *C.S.I. Crime Scene Investigation* (Anthony E. Zuiker), die Kriminalserie in der sich die Protagonisten computergestützt durch riesige Datenbanken arbeiten, und dabei DNA- und Fingerabdruck-Datenbanken, Kreditkartenabrechnungen, Telefonlisten, Online-Einkaufslisten verwenden, ohne auch nur einen Moment lang auf die Rechte der Verdächtigen Rücksicht zu nehmen. Jedes nur erdenkliche Recht auf Privatsphäre wird ohne richterliche Genehmigung gebrochen um den Fall zu lösen. Damit wird ein Zustand verharmlost der die Grundrechte aufs heftigste verletzt.[367] So erfolgreich diese Möglichkeiten der Verbrechensbekämpfung auch dargestellt werden, genauso erschreckend sind sie. Es stellen sich in diesem Zusammenhang und im Verbindung mit dem Datenschutz, immer wieder dieselben Fragen: Wer hat Zugang zu Daten? Was macht er damit? Welchem Zweck dienen sie?

Natürlich gibt es Organisationen die gegen diese fortschreitenden Einschränkungen des Datenschutzes eintreten. Die österreichischen Organisationen Arge-Daten und Quintessenz

[365] “The Power of Nightmares – BBC TV Documentary – 2004” (Video). (www.Everystepyoutake.org) (05.05.2008).
[366] Siehe: Zinganel. 2005. S. 266.
[367] Programmheft Big Brother Awards 2007. Der C.S.I. Autor Anthony E. Zuiker wurde 2007 für den Big Brother Award in der Sparte Kommunikation und Marketing vorgeschlagen, da diese Serien „Rasterfahndung, DNA-Analysen und die Aushebelung von Bürgerrechten unkritisch, verharmlosend und gefährlich einseitig [präsentieren].“ Ebenda.

(Organisation der *Big Brother Awards*) wurden schon genannt. Der Kampf gegen die „Überwachungswütigen" wird aber auch spielerisch aufgenommen: In New York City wurde 1996 die Gruppe *Surveillance Camera Players* gegründet um gegen Überwachung(-skameras) zu protestieren. Diese Gruppe hat es sich zu Aufgabe gemacht, vor U-Bahnkameras Stücke aufzuführen, um, wie sie sagen, „den Videokontrolloren etwas Unterhaltung zu bieten".

> „If you, too, are worried about the destruction of your constitutional rights in the name of 'fighting crime', we encourage you to form your own anti-surveillance camera group. [...] Just let the message go out: Down with Big Brother!"[368]

Überwachung führt zu angepasstem Verhalten. In den letzten Kapiteln wurde dieses „Syndrom" bereits erörtert. Man verhält sich anders wenn man weiß, dass man unter Beobachtung steht. Man ist nicht mehr frei.[369] Die Gesellschaft wird unter Generalverdacht gestellt und damit wird die Rechtsstaatlichkeit der Demokratie gefährdet, die Aushöhlung der Unschuldsvermutung ohne Widerstand hingenommen.[370] Wiederin schreibt: Es gibt keinen „überwachungsresistenten inneren Kreis der Privatsphäre".

> „Wir müssen uns deshalb mit der traurigen Wahrheit abfinden, dass der Bürger eine dem Staate schlechthin unzugängliche Privatsphäre gar nicht hat [...]."[371]

Ist es also hoffnungslos für unsere Privatsphäre zu erkämpfen, noch zu hoffen, dass wir „Herr unserer Daten" sind, oder ist dieser Kampf schon verloren? Das Datenschutzgesetz und die Datenschutzkommission in Österreich hinken der Technik hinterher. In den Medien häufen sich Meldungen über Datendiebstähle, illegalen Datenhandel, illegale Überwachung von Mitarbeitern, Schülern und Angestellten. Viel zu wenige Wenige machen von ihrem Recht auf Datenschutz gebrauch, wer nicht nicht davon Gebrauch macht, verliert es.

Das Potential der Information, das in Profilen steckt, seien es Nutzerprofile oder Konsumentenprofile, haben viele noch nicht verstanden. Information wird beiläufig mit der Anschaffung einer Kundenkarte weitergeben. Was passiert wenn Privatdaten in öffentlichen Registern ökonomsichen Interessen geopfert werden? Wenn Daten die der Staat zum

[368] Surveillance Camera Players. (http://www.notbored.org/the-sep.html) (25.07.2008).
[369] Peissl. 2008. S. 85.
[370] Peissl. 2008. S. 88.
[371] Wiederin. 2007. S. 123.

Bilanzieren braucht, an eine Firma verschachert, die genügend dafür bezahlt? Um in dieser Entwicklung mitbestimmen zu können, muss eine öffentliche Diskussion geführt werden.

Hans Zeger (*Arge-Daten*) spricht bei Diskussionen explizit nicht von *einem* Big Brother sondern von vielen Little Brothers.[372] Technische Neuerungen, einfache Handhabung und der kostengünstige Erwerb von Überwachungskameras, erleichtern es Privaten, ihre eigenen Überwachungsanlagen zu installieren, d.h. es ist „nicht nur der Staat, der überwacht. Jeder überwacht jeden."[373]. Das Problem, das dabei allerdings wieder aufdrängt, wurde schon angesprochen: Es gibt keine Möglichkeit der Kontrolle, weder darüber, wer überwacht, noch was mit diesen Aufzeichnungen geschieht.

Diese Affinität wurde vom Präsidenten des österreichischen Verfassungs-Gerichtshofes Karl Korinek bestätigt. Im Ö1-Journal (15.09.2007) wurde er allgemein zum Thema Datenschutz befragt. Seine Befürchtungen betrafen vor allem die Gesetzesänderungen in Bezug auf die Terrorismusbekämpfung, die ein „Abrutschen in einen totalen Überwachungsstaat"[374] zur Folge haben könnten. „Ich habe manchmal den Eindruck, wir werden ähnlich stark überwacht wie seinerzeit die DDR-Bürger von der Stasi."[375] Die Sicherheit der Bevölkerung geht auf Kosten des Datenschutzes. Korinek empfindet es als fehlende „Sensibilität für die Gefahren",[376] die durch Eingriffe in den Datenschutz erfolgen. Es muss sich also der Einzelne wieder darauf besinnen, auf seine Privatsphäre zu achten und aufmerksamer zu werden. Sollten wir uns soweit einschüchtern lassen, dass wir diese Privilegien aufgeben, haben wir mehr verloren als uns bewusst ist.

[372] Diskussion im Top Kino (04.05.2008). Teilnehmer an der Diskussion: Manu Luksch (Regisseurin) , Hans Zeger (Arge-Daten), Doris Kaiserreiner (Quintessenz). Moderation: Ingrid Brodnig (Falter).
[373] Dax. 2008.
[374] „VfGH-Präsident Korinek: „Kontrolle wie in der DDR"." (22.09.2007) *Die Presse* (http://diepresse.com/home/politik/innenpolitik/331831/index.do?from=suche.intern.portal) (10.05.2008).
[375] Korinek zit. in: Ebenda.
[376] Ebenda.

ANHANG:

Abstract

Diese Arbeit handelt von Videoüberwachung und seine gesetzliche Regelung im Datenschutzgesetz. Manu Luksch, die für dieses Thema ausschlaggebend war, hat in London einen Film gemacht der ohne eigene Kamera zustande kam: Sie machte von ihrem Recht gebrauch, Kopien von CCTV-Material (Videoüberwachung) anzufordern. Aus diesen Kopien entstand der Film *Faceless*. Ihre Arbeit basiert auf der intensiven Auseinandersetzung mit dem britischen Datenschutzrecht, dem *Data Protection Act 98*, und einer 4 Jahre andauernden Zeitspanne in der es erst möglich wurde, den Film fertig zu stellen.

Davon ausgehend behandelt der erste Teil der hier vorliegenden Arbeit das österreichische Datenschutzgesetz (DSG). Es hat sich herausgestellt, dass im DSG kein expliziter Hinweis auf Videoüberwachung vorhanden, bzw. die abgeleiteten Regelungen nicht eindeutig sind. Die Datenschutzkommission ist die verantwortliche Behörde die in diesen Situationen die Rahmenbedingungen vorgibt. Trotz allem herrscht sowohl bei Juristen wie auch Betreibern von Videoüberwachungsanlagen Unklarheit darüber, wie sich die rechtliche Lage verhält.

Manu Luksch, der Film *Faceless* und sein Zustande kommen bilden den zweiten Teil. Ihre Motivation war, eindringlich zu zeigen, dass wir immer und überall von Videokameras überwacht werden, dass wir immer gesehen werden: In einer Stadt wie London, die so viele Kameras besitzt, braucht eine Regisseurin eigentlich keine eigene Kamera. Dabei wird gezeigt wie Luksch das Gesetz „testet“ und versucht, ihr Recht anzuwenden.

Videoüberwachung hat sich zur Verbrechensbekämpfung als nicht funktionstüchtig erwiesen. Das Ende der Arbeit zeigt die Auswirkungen und Gefahren die sich vor allem in Normierung, Klassifizierung, Ausschluss und „social sorting“ niederschlagen.

Manifesto for CCTV-Filmmakers[377]

THE FILMMAKER AS SYMBIONT:
opportunistic infections of the surveillance apparatus

(published in the NODE-LONDON READER 2006)

Filmmakers render aspects of nature, human activity and imagination visible. The documentary film continues to be a potent form in all its variety, from the personal video diary to "objective" fly-on-the-wall shoots, to the hybrid fact/fiction ("faction") film. But the most prolific documentarists are no longer to be found in film schools and TV stations. In some European and American cities, every street corner is under constant surveillance using recording closed-circuit TV (CCTV) cameras. Such cameras are typically operated by local government, police, private security firms, large corporations and small businesses, and private individuals, and may be automatic or controlled (zoomed and panned) from a remote control room. Filmmakers, and in particular documentarists of all flavours, should reflect on this constant gaze. Why bring in additional cameras, when much private and public urban space is already covered from numerous angles?

MANIFESTO FOR CCTV FILMMAKERS declares a set of rules, establishes effective procedures, and identifies further issues for filmmakers using pre-existing CCTV (surveillance) systems as a medium in the UK. The manifesto is constructed with reference to the Data Protection Act 1998 and related privacy legislation that gives the subjects of data records (including CCTV footage) access to copies of the data. The filmmaker's standard equipment is thus redundant; indeed, its use is prohibited. The manifesto can easily be adapted for different jurisdictions.

MANIFESTO FOR CCTV FILMMAKERS (UK VERSION, 2004)

GENERAL

The filmmaker is not permitted to introduce any cameras or lighting into the location.

SCRIPT

A protagonist ("data subject") is required to feature in all sequences.
*Data Protection Act 1998; 1998 Chapter 29; Part II Section 7(1). ***
[A]n individual is entitled –
(a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller,
(b) if that is the case, to be given by the data controller a description of –
(i) the personal data of which that individual is the data subject,
(ii) the purposes for which they are being or are to be processed, and
(iii) the recipients or classes of recipients to whom they are or may be disclosed,
(c) to have communicated to him in an intelligible form –
(i) the information constituting any personal data of which that individual is the data subject, and

[377] AmbientTv.net. (http://www.ambienttv.net/content/?q=dpamanifesto) (03.10.07).

(ii) any information available to the data controller as to the source of those data, and
(d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.

The documented activity of the protagonist must qualify as personal or sensitive data. The filmmaker is to establish this by locating a surveillance camera and circumscribing the field of action for the actors relative to it, so that incidents of biographical relevance (i.e. that reveal personal data) occur in the frame.
ICO CCTV systems and the Data Protection Act JB v.5 01/02/04 (***)
2. The court decided that for information to relate to an individual (and be covered by the DPA) it had to affect their privacy. To help judge this, the Court decided that two matters were important: that a person had to be the focus of information, the information tells you something significant about them.

The provisions of the 1998 Act are based on the requirements of a European Directive, which at, Article 2, defines, personal data as follows:
"Personal data" shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
The definition of personal data is not therefore limited to circumstances where a data controller can attribute a name to a particular image. If images of distinguishable individuals' features are processed and an individual can be identified from these images, they will amount to personal data.

All people other than the protagonist ("third parties") will be rendered unidentifiable on the data obtained from the CCTV operators. Typically, operators blur or mask out faces of third parties. The filmmaker is to consider the visual impact of this manipulation, and to establish a rule for the handling of footage delivered with ineffectual masking or blurring – for example, reporting the offence.
Right to Privacy in Article 8 of the Human Rights Act 1998 (****):
RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE
1. Everyone has the right to respect for private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights or freedoms of others.

DPA1998
4. On the other hand, the disclosure of third party information in compliance with a subject access request may also expose the data controller to complaint or action by the third party, for example [...] for breach of confidence.
6. The data controller should consider to what extent it is possible to communicate the information sought without disclosing any third party information [...] This might be achieved by editing the information to remove names or other identifying details.

LOCATION

The filmmaker is to choose sites that are covered by multiple surveillance cameras, preferably operated by a large business, private security firm or public authority – or, if operated by a small retailer, cameras of the kind that can be panned and zoomed remotely. Sites may be mobile – for example, a public bus.
ICO CCTV systems and the Data Protection Act JB v.5 01/02/04
If you have just a basic CCTV system your use may no longer be covered by the DPA. [...]
Small retailers would not be covered who
– only have a couple of cameras,
– can't move them remotely,
– just record on video tape whatever the camera picks up,
– only give the recorded images to the police to investigate an incident in their shop.

For every camera used, the operator's name and contact details are to be noted.
Code of practice issued by the Data Protection Commissioner, under Section 51(3)(b) of the Data Protection Act 1998, 07/2000 (*****)
7. Signs should be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment.
The signs should contain the following information:
Identity of the person or organisation responsible for the scheme.
The purposes of the scheme.
Details of whom to contact regarding the scheme.
(First Data Protection Principle).

FOOTAGE REQUESTS

After completing each shoot, the filmmaker is to address a written request ("subject access request letter") to the CCTV operator ("data controller") immediately to ensure that the data recovery process can be initiated while the recordings are still archived. (Mandatory retention periods vary.)
Code of practice issued by the Data Protection Commissioner, under Section 51(3)(b) of the Data Protection Act 1998, 07/2000
1. Once the retention period has expired, the images should be removed or erased (Fifth Data Protection Principle).

The subject access request letter is to state the place and time of the recording and include a picture of the protagonist, wearing the same clothes if possible, and a cheque for £10 (the maximum fee chargeable). Letters should be sent by a secure system which provides evidence of delivery. (Some data controllers may require the notarisation of the letter to legally establish identity.)
Data Protection Act 1998; 1998 Chapter 29, Part II Section 7(2)
A data controller is not obliged to supply any information under subsection (1) unless he has received –
(a) a request in writing, and
(b) except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.

The filmmaker is to allow a maximum 40 days after sending the data request for an initial response.

Code of practice issued by the Data Protection Commissioner, under Section 51(3)(b) of the Data Protection Act 1998, 07/2000
A data controller must comply with a subject access request promptly, and in any event within forty days of receipt of the request or, if later, within forty days of receipt of:
the information required (i.e. to satisfy himself as to the identity of the person making the request and to locate the information which that person seeks); and the fee.

The filmmaker is to establish a set of rules for handling the various formats in which the data may be sent (video tape, DVD-video, digital files encoded with proprietary codecs, hard copies of frames).

SOUND

CCTV systems are not permitted record sound. The filmmaker is to establish a set of rules for the soundtrack (if any) of the movie – for example, prohibiting field recordings.

DISTRIBUTION

Footage received is subject to complex copyright issues. The filmmaker is to take legal advice and establish a strategy.

FOOTNOTES

(*) In addition to the boom in surveillance, the proliferation of miniature mobile cameras (many built into phones and other handheld devices) has led to the phenomenon of "sous-veillance" activities carried out by the population at large. News services now actively solicit amateur recordings from camcorders and even mobile phones, often combining them with CCTV footage where they have access to it, when reporting from scenes of crimes, accidents or natural disasters. The manifesto can be extended to provide a framework for films that work with acts of sous-veillance.

(**) Data Protection Act 1998 Chapter 29
http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm

(***) CCTV systems and the Data Protection Act JB v.5
http://www.informationcommissioner.gov.uk

(****) Article 8 of the Human Rights Act 1998 (CCTV and the Human Rights Act)
http://www.crimereduction.gov.uk/cctv13.htm

(*****) CCTV Guidance and the Data Protection Act - Good Practice Note
http://www.informationcommissioner.gov.uk/eventual.aspx?id=5740

Transkription FACELESS

[*Insert*]
A new time
The new machine
Amidst which
A single dream survives

This is the story of a woman, haunted by an echo of a memory, a dislocated dream in which the past telescopes into the future. She has no understanding of these images that revisit her, that take her out of RealTime, out of her role in the New Machine. Only later will she recognise them as nostalgia and resentiment.
At work, the woman inspects data traces. She is one of many thousands who scrutinize the data, mind by the new machine.
(*Dream sequence*)
Another echo. She emerges from its spell. The pulse of RealTime impells her again.
Later the woman will go shopping. She has an elegant home in a handsome towerblock. The pulse of RealTime orients the life of every citizen. Eating resting, going to work, getting married… every act is tied to RealTime. And every act leaves a trace of data. A footprint in the snow of noise. The new machine monitors these data traces, making sure that all is well.
In a distant era, people had become discontented. Anxiety about the future, and guilt over the past, caused great unhappiness. The present was continuously in short supply. Then a reform of the calender was proposed to dispense with the troublesome past and future and fill everyone's lifes with the perfect presence. An advanced technology called the new machine was developed to supersede the past and the future. And soon afterwards the system of RealTime was unanimoulsy accepted.
The new machine broadcasts pulses of RealTime, that guide each life in an optimal path. The new machine surveys the city, monitoring the datatraces left by every citizen. The new machine dispatches overseers, to correct any errors and deviations instantly.
In the luminous world of the new machine, each moment of time saturates each consciousness. There is no memory, no anticipation. There is no past, so there can be no guilt or regret, and no future, therefore no anxiety or fear. RealTime, the perfect and perpetual present is the heartbeat of the healthy universe,

Another morning, another dream. Unfamiliar to emotion, the woman feels an uneasiness. Then she picks up a journal and reads of present times: The news is familiar, and reassures her, that all is well.

She sees a child in a flash of colour. The untimeliness of it nauseates her.
Then: All is well

An abberation, a face. (17' *Beginning of blurring*.) She panicks, attempts to scrub it away. But the face stares stubbornly back.
At the woman's desk a letter awaits. She reads of a meeting. The words used are unusual. On one page are depicted a number of circles on another echelons of figures, on a third, a labyrinth. She understands little, but feels drawn to the sender. At the end she reads: Follow your dreams!
The colourful child, her turbulent dreams, they weigh on her. And her face and the letter remain persistently present. Sensations inside, feelings difficult to name, despair, loneliness,

helplessness, fear… but, these are words from a different age! She does not know how to admit them.
Her new face burns. She makes a mask to hide behind. And retreats to an abandoned place

Circles whirl within circles, dreams within dreams. Maps, codes, rituals – the dance sings of many things strange to her. The movements articulate the circles of the letter, revealing secret passageways through the city. She eases herself back into consciousness. A pathway unfolds in front of the woman and she runs along it. Overseers pursue her.

In an elaborate garden, scintilating with colour, childred flicker in division, then disappear. For the first time, she senses something is about to happen. She turns. The overseer, surprised, hesitates. Then fires. She jumps. She is falling. (25')
Then, ground beneath her feet, and the sound of bells. Spectral children illuminate the space around her. One child on a bycicle welcomes her, tells her that they are fugitives, escaped from the synchro-centres of the new machine, where all children are discoloured and disciplined into RealTime. The natural colours of the fugitives confound the new machine. They roam the city without leaving a trace. She follows him deeper into the childrens layer.
Movements begin to flow, like memories. A radiant dance, radiant children. Real children. Real laughter, real rhythm, real friendship, real risk.
More children gather. They warn her. Her face, the letter, her flight from work: all have alerted the new machine. Overseers are being marshalled – grave danger awaits. Her only hope lies with the sender of the letter.
At a public terminal the woman deciphers the lines of figures in the letter. A meeting place is revealed. Another pathway opens up before her.
A perilous shortcut through RealTime that she must race across to avoid capture.
He awaits her. He will tell her about their common past. About a child. He tells the woman that he is a friend, that he is the sender of the letter. He tells her: once they had a life together. (35')
He talks of a child. Removed to a synchro-centre. He explains why they parted, how he become an overseer, how she moved into the towerblock, oblivious that she had been part of a family a moment before. He speaks of her face, unveiled by her dreams. And of his dreams, which reveal the presence of her, of a love that persists through RealTime. He then speaks of an era before RealTime, when all humans had a face, each one different, each one capable of expressing tenderness, anguish, hate, each one capable of anticipation and remebrance. A brilliant but violent world. He tells her about the coming of the new machine, of how fear of the future and distrust of the past were cultivated. And how the perpetual present came into being. But the spectral children reveal the imposture of RealTime – only the spectral children truly inhabit the present. Only the spectral children… and her.
For the woman there passes a moment of epiphany. She now has a name for her feelings. That name is the name of a child. Her child. Their child. Face to face with an infinity of time before this moment, she grasps the infinity that lies ahead.
He tells her: To free their child she must infiltrate the new machine. Its sanctum lies on the far shores of the blue water. A treacherous journey by seapod. The seapods are well guarded for they sail across the blind spot of the new machine where no datatraces register. He offers help. Allies who can smuggle her on board. He points to the labyrinth of the letter – a map of the sanctum. His allies will accompany her up to its threshold. Beyond, she must go alone. Outside, 4 accomplices wait to escort the woman across the blue water.
(39') Aboard the seapod, the accomplices warn her: Inside the sanctum, she will be exposed. Her dreams will guide her. But she must not linger in them. The new machine will seek to imprison her there by closing her path back to consciousness, forever.

They arrive at the far shores of the blue water.
Cautious gates… hesitate. Then, allow her in.

IN THE SANCTUM SHE ENCOMPASSES PAST, PRESENT AND FUTURE IN A SINGLE GLANCE. VISIONS IMPELL HER, FACES RETURNED, THE CITY LIBERATED! REFLECTED IN HER GAZE THE VEIL OF REALTIME BEGINS TO FALL.
(45') There is a violent disturbance. Later, an adjustment is made. The woman finds herself reunited with her child and her lover. Her child? Her lover? Doubts mulitiply. Is this her dream? Her past? Or nostalgia for a time that never was? A prison of another perfect present? Then, all is well(?)

[*Inserts*]
46. London has the highest density of xsurveillance cameras in the world. The Uk Data protection act and EU directive give you the right to access personal data held in computer databeses.
This includes cctv recordings.

All cctv images in this work were obtained under the terms of the data protection act. Legislation requires that the privacy of other persons be protected when data is released.
For cctv recordings, this is typically done by obscuring their faces.

This work treats cctv images as 'legal readymades' (objets trouvés)
The scenario of feaceless dereives from the legal properties ot the images.

The plot evolved alongside the process of obtaining the recordings.

Abbildungsverzeichnis

Ich habe mich bemüht, sämtliche Inhaber der Bildrechte ausfindig zu machen und ihre Zustimmung zur Verwendung der Bilder in dieser Arbeit eingeholt. Sollte dennoch eine Urheberrechtsverletzung bekannt werden, ersuche ich um Meldung bei mir.
(Sämtliche Stills die in dieser Arbeit dem Film *Faceless* präsentieren, unterliegen dem Copyright von Amour Fou, die mir freundlicherweise die Genehmigung zur Verwendung des Bildmaterials erteilt haben.)

Bibliographie

- Billman, Larry. *Film Choreographers and Dance Directors*. McFarland&Company: London, 1997.

- Casetti, Francesco. Inside the Gaze. The Fiction Film and its Spectator. Indiana University Press: Bloomington, 1998.

- Daniels, Dieter. Vom Readymade zum Cyberspace. Kunst/Medien: Interferenzen. Hatje Cantz Verlag: Ostfildern-Ruit, 2002.

- Dittrich, Robert. *Taschenbuchkommentar ABGB*. Manz: Wien, 2005.

- Foucault, Michel. *Mikrophysik der Macht. Über Strafjustiz, Psychiatrie und Medizin*. Merve: Berlin, 1976.

- Groß, Heinrich. Reinelt, Heinz. *Geistliche Schriftlesung. Erläuterungen zum Alten Testament für die Geistliche Lesung. Das Buch der Psalmen Teil III (Ps 73-150)*. Patmos Verlag: Düsseldorf, 1980. (S.396-401).

- Jahnel, Siegwart, Percher (Hg.). *Aktuelle Fragen Datenschutzrechts.* Facultas: Wien, 2007.

- König, Gregor. *Videoüberwachung. Fakten, Rechtslage und Ethik ; mit dem Schwerpunkt auf generalpräventiver Videoüberwachung im öffentlichen Raum*. (Juristische Schriftenreihe Bd. 179.). Verlag Österreich: Wien, 2001.

- Kuhlmann, Dörte. *Raum, Macht & Differenz. Genderstudien in der Architektur*. Edition Selene. Wien, 2005. (S. 186-210.)

- Lem, Stanisław. Sterntagebücher. Suhrkamp: Frankfurt am Main, 1988.

- Lupton, Catherin. Christ Marker. Memories of the Future. Reaktion Books: London, 2005.

- Mayer-Schönberger, Viktor / Brandl, Ernst O. *Das Datenschutzgesetz 2000*. Linde: Wien, 1999.

- Moser, Tilman. *Gottesvergiftung*. Suhrkamp. Frankfurt am Main, 1980.

- Nentwich, Michael / Peissl, Walter (Hg.). *Technikfolgenabschätzung in der österreichischen Praxis.* (Festschrift für Gunther Tichy.) Verlag der Österreichischen Akademie der Wissenschaften. Wien. 2005.

- Orwell, George. *Nineteeneightyfour*. Signet Classics: USA, 1977.

- Österreichisches Katholische Bildungswerk (Hg.). *Die Bibel. Einheitsübersetzung der Heiligen Schrift*. Carinthia: Klagenfurt, 1986.

- Österreichische Juristenkommission (ÖJK) (Hg.). *Sicherheit im öffentlichen Raum*. 20. Oktober 2005. Neuer Wissenschaftlicher Verlag: Wien, 2006.

- Österreichische Juristenkommission (ÖJK) (Hg.). *Grundrechte in der Informationsgesellschaft*. Mai 2001. Neuer Wissenschaftlicher Verlag: Wien, 2001.

- Reiter, Michael / Witmann-Tiwald, Maria. (Hg.). *Goodbye Privcy – Grundrechte in einer digitalen Welt*. *Internationales Symposium veranstaltet von der Fachgruppe Grundrechte in der Vereinigung österreichischer Richterinnen und Richter in Kooperation mit der Ars Electronica Linz*. (Dokumenation der Tagungsergebnisse vom 5.9.2007). Linde: Wien, 2008.

- Rummel, Peter. *Kommentar zum Allgemeinen Bürgerlichen Gesetzbuch*. Manzsche Verlags- und Universitätsbuchhandlung: Wien, 2000.

- Samjatin, Jewgenij. *Wir*. Verlag Kiepenheuer & Witsch: Köln, 1984.

- Terrien, Samuel. *The Psalms. Strophic Structure and Theological Commentary*. William B. Eerdmans Publishing Company: Cambridge/UK, 2003. (S.876-879).

- Virilio, Paul. *Die Sehmaschine*. Merve: Berlin, 1989.

- Wiederin, Ewald. *Privatsphäre und Überwachungsstaat*. Manz: Wien, 2003.

- Withaker, Reg. *The End of Privacy*. The New Press: New York, 1999.

- Zinganel, Michael. *Real Crime. Architektur Stadt & Verbrechen*. Edition Selene: Wien, 2003.

Artikel:

Kunnert, Gerhard. „Big Brother in U-Bahn, Bus und Bim“. *juridikum* 2006/01. S. 42-50.

- Knyrim, Rainer. „25 Jahre Datenschutzrecht in Österreich.“ *Medien und Recht* Dezember 2005. S. 415-420.

- Lachmayer, Konrad. „Überwachung im Informationszeitalter.“ *juridikum* 2006/01. S. 29-33.

- Müller, Henning Ernst. „Zur Kriminologie der Videoüberwachung“. *Monatsschrift für Kriminologie und Strafrechtsreform* 2002/1. S. 33-46.

- Steiner, Gerald/Andreewitch, Markus. „Videoüberwachung aus datenschutzrechtlicher Sicht. *Medien und Recht*.“ 2006/02. S. 80-83

Zeitungen:

- Der Standard:
„Das neue ‚Mist-TV’ im Gemeindebau“. *Der Standard* (19.02.2008)

Frey, Eric: „Rechtslabyrinth als Videospiel“. *Der Standard* („Wohnen“-Beilage März 2008)

Simoner, Michael. „Grobe Mängel beim Lauschangriff“. *Der Standard* (16.09.2008)

Springer, Gudrun: „ ‚Kamera läuft’ in acht Wiener Gemeindebauten“. *Der Standard* (27.03.2008)

Stemmer, Martina: „Alles unter Kontrolle“. *Der Standard* (16.10.2007)

Zeitschriften:

- Zeitschrift der Österreichischen Liga für Menschenrechte. Überwachung. 02/2007. Druckerei Berger, Wien. 2007.

- P.M.-Magazin
Vašek, Thomas. „Was wird uns da ‚vorgegoogelt’“. *P.M*. März 2006. S. 16-23.

Internetquellen:

- AmbientTV.net
Webseite von Manu Luksch und Mukul Patel
(http://www.ambienttv.net) (1.10.2008)

Broadbandit Highway
(http://www.ambienttv.net/2001/broadbandit/disturb/cam26.html). (15.05.2008).

“*Faceless*: Chasing the Data Shadow.”
http://www.ambienttv.net/2007/faceless/chasingthedatashadow2007.pdf (25.05.2008).

Manifesto for CCTV Filmmakers
http://www.ambienttv.net/content/?q=dpamanifesto (10.10.2007)

Orchestra of Anxiety
(http://netznetz.net/wiki/Einreichung_Projekt_2007-1_ Orchestra_of_Anxiety).
(28.04.2008).

Spy School
(http://www.ambienttv.net/3/spyschool/1/index.html) (05.10.2008).

- Anti-Social Behaviour Orders (ASBO’s).
(http://www.antisocialbehaviour.org.uk/asbo/index.php) (10.10.2008).

- Arge-Daten:
„Überwachungskameras in Wiener U-Bahn Zügen“ (12.04.2005)
(http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=18195sst) (05.04.2008)

„Schörghofer räumt Datenschutzprobleme bei der e-card-Administration ein.“ (06.06.2005) (http://www2.argedaten.at/session/anonym811192tsssio549116.E42_INP.html) (20.09.2008).

- Big Brother Awards
(www.bigbrother.at) (1.10.2008).

- Buckland, Warren
(www.warrenbuckland.com) (18.10.2008).

- Dogma 95. „The Vow of Chastity“.
(http://www.dogme95.dk/menu/menuset.htm) (21.05.2008).

- Home Office Research
Gill, Martin, Spriggs, Angela. “Home Office Research Study 292. Assessing the impact of CCTV”. 2005. (www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf) (10.08.2008).

- Internet und Recht: internet4jurists
SPG
(http://www.internet4jurists.at/ges/spg2008.htm) (08.04.2008).

Artikel 8 EMRK
(www.internet4jurists.at/gesetze/emrk.htm) (08.04.2008).

§ 16 ABGB
(http://www.internet4jurists.at/ges/abgb.htm) (08.04.2008).

§ 78 UrhG
(http://www.internet4jurists.at/gesetze/bg_urhg2a.htm#§_78.) (05.04.2008).

- Information Commissioner’s Office: *Code of Practice* (Version 2008):
(http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf) (24.04.2008).

- Der Detektiv. Fachzeitschrift für das Sicherheitsgewerbe:
Haupt, Cornelia: „Schadenersatz für indiskrete Webcams“ (03.08.2007)
(http://weblog.derdetektiv.at/categories/35-Videoueberwachung) (08.02.2008)

- Homepage der Österreichischen Datenschutzkommission
Datenschutzbericht, Formulare, DSG 2000
(www.dsk.gv.at) (01.04.2008)

DSK-Artikel: „Videoüberwachung in Wohnhäusern der Stadt Wien“.
(www.dsk.gv.at/Bekanntmachung:wienerwohen.htm) (12.05.2008)

- Freedom of Information (FOI)

„What is an Information Commissioner“.
(http://www.foi.gov.ky/pls/portal/docs/PAGE/FOIHOME/INFORMATION%20COMMISSIONER%20BROCHURE.PDF) (15.10.2008).

- Futuresonic.com: Urban Festival of Art, Music & Ideas.
(www.futuresonic.com) (05.05.2008).

- Glotel
(http://www.glotel.com/content_dynamic/display_news.asp?id=357&session_id=%7B475418E6-B310-410F-9A92-EF1B0424B173%7D) (1.10.2008).

- IMDB The Internet Movie Database
Faceless
(http://www.imdb.com/title/tt1068949/) (05.04.2008).

La jetée
(http://www.imdb.com/title/tt0056119/) (10.07.2008).

- Kunst der Vermittlung.de
Pantenburg, Volker. „Gefängnisbilder“. (09.10.2008) (http://www.kunst-der-vermittlung.de/artikel/filmbeschreibung-gefaengnisbilder/) (18.10.2008).

- Middlesbrough Council
„You’ve heard nothing yet … CCTV wired for sound“. (02.08.2006)
(http://www.councillor.info/middlesbrough/3336/Default.aspx) (11.10.2008).

- „Manifest: Dogma 95“ *Mediaculture-online*. (http://www.mediaculture-online.de/Manifest-Dogma-95.442.0.html) (21.05.2008).

- Mediashed
delboy: *the commercial*.
(www.mediashed.org/?q=videosniffincom) (05.05.08).

Video-Sniffin’.
(http://mediashed.org/videosniffin) (10.04.2008).

- Medienkunstnetz
Wolf, Reinhard. „Der Riese“. (http://www.medienkunstnetz.de/werke/der-riese/)
(10.10.2008).

- Microdrones GmbH.
(http://microdrones.com/home/home_p1_big.jpg) (02.09.2008).

- Mongrel
(http://www.mongrel.org.uk/) (10.04.2008).

- Musil, Steven. „Google finds no privacy on private roads“. News – Digital Media.
(24.08.2008). (http://news.cnet.com/8301-1023_3-10024294.html?tag=mncol). (20.09.2008).

- Netzwelt. Online für IT & Consumer Electronics.

Woods, Patrick. Google Street View: Stadtrundfahrt am Bildschirm. (20.06.2007) (http://www.netzwelt.de/news/75729-google-street-view-stadtrundfahrt-am.html) (20.09.2008)

- ÖBB-Homepage
„Ausbau der Videoüberwachung bei ÖBB“ APA
http://www.oebb.at/euro2008/de/Aktuell/2008/05/06/3207162881/index.jsp (14.05.2008)

- ORF.AT

„Was bringen Videoüberwachungen?“ http://oesterreich.orf.at/wien/stories/270105 (14.05.2008)

Moechl, Erich. „Videodrohnen bald für jedermann“. *Futurezone ORF.at* (13.08.07) (http://futurezone.orf.at/produkte/stories/214259/) (05.09.2008)

Dax, Patrick: „Filme machen mit Überwachungskameras. Interview mit Manu Luksch.“ *Futurezone ORF.at*. (http://futurezone.orf.at/it/stories/275169/) (03.05.2008)

Moechl, Erich. „Videodrohnen bald für jedermann“. *ORF.at* (13.08.07) (http://futurezone.orf.at/produkte/stories/214259/) (05.09.2008)

- Tonmitschnitt des Films „faceless“ im Ö1-Interview mit Manu Luksch. (www.oe1.orf.at/audio) (12.10.2007).

- Peter Pilz - Homepage: *Der Standard* Artikel vom 19.03.2004 gefunden auf: (http://www.peterpilz.at/html/txt/index.php?jahr=2004&monat=3) (20.05.2008).

- Rechtsinformationssystem des Bundeskanzleramtes
DSK-Bescheid der Wiener Linien:
(http://www.ris2.bka.gv.at/Dokument.wxe?QueryID=Dsk&Dokumentnummer=DSKTE_20050621_K507515-021_0004-DSK_2005_00&TabbedMenuSelection=JudikaturTab&WxeFunctionToken=dc47ac20-0735-455b-babf-71bc857dda03) (05.04.2008).

- Robertson, Struan. „Google’s Street View could be unlawful in Europe“. *The Register-Online*. (05.06.2007).
(http://www.theregister.co.uk/2007/06/05/google_street_view_legality_in_europe/).
(15.09.2008).

- StreetViewFun
(www.streetviewfun.com) (11.09.2008).

- Telepolis/Heise.de

Bager, Jo. „Der Datenkrake.“ *c’t.* 10/2006. (168ff). (www.heise.de/ct/06/10/168/) (10.09.2008).

Rötzer, Florian. „Bildbereinigung durch Google Earth“. *Telepolis*. (21.07.2007) (http://www.heise.de/tp/r4/artikel/24/24483/1.html) (14.09.2008).

Becker, Matthias. „Heute Abend im Fernsehen: Alles.“ (15.04.2006) *Telepolis.* (http://www.heise.de/tp/r4/artikel/22/22461/1.html) (10.10.2007).

Krempl, Stefan: „Hacker überwachen Videoüberwachung“ (30.12.2005) *Heise-Online* (http://www.heise.de/newsticker/meldung/67842) (10.04.2008).

- The Kitchen.org: Center for video, music, dance, performance, film + literature (http://www.thekitchen.org/MovieCatalog/Titles/DerRiese.html). (26.05.2008).

- URBANEYE – On the Threshold to the Urban Panopticon? (www.urbaneye.net) (10.09.2008).

Hempel, Leon/Töpfer, Eric. No. 15: Final Report: CCTV in Europe. (http://www.urbaneye.net/results/ue_wp15.pdf) (10.09.2008).

Helten, Frank/Fischer, Bernd. No. 13: What people think about CCTV in Berlin. (http://www.urbaneye.net/results/ue_wp13.pdf) (10.09.2008).

Ney, Steven. Pichler, Kurt. No. 7: Videosurveillance in Austria. (http://www.urbaneye.net/results/ue_wp7.pdf) (10.09.2008).

Hempel, Leon/Töpfer, Eric. „Videoüberwachung in Europa. Abschlussbericht.“ (August 2004) (http://www.ztg.tu-berlin.de/pdf/URBANEYE_Abschlussbericht_Zusammenfassung_dr.pdf) (12.06.2008).

- We make money not art (http://www.we-make-money-not-art.com/archives/2007/09/in-linz-several.php) (05.05.08).

- Wiener Linien: Bericht 2005. http://www.wienerlinien.at/wl/ep/programView.do?channelId=-8358&displayPage=%2fep%2fprogram%2fcontentOverview.jsp&programId=10739&pageTypeId=9322 (05.04.2008).

- Wikipedia Online Lexikon „Mockumentary” (http://de.wikipedia.org/wiki/Mockumentary) (10.05.2008).

- 3Sat „Dokumentarfilmzeit: *Gefängnisbilder*“. (05.04.2007). (http://www.3sat.de/3sat.php?http://www.3sat.de/specials/11034/index.html) (28.05.2008).

Online-Zeitungen:

- Dailymail – Online

Bates, Daniel. „Billions spent on CCTV have failed to cut crime and led to an ‚utter fiasco’, says Scotland Yard surveillance chief“.(06.05.2008) *Dailymail.*

(http://www.dailymail.co.uk/news/article-564240/Billions-spent-CCTV-failed-cut-crime-led-utter-fiasco-says-Scotland-Yard-surveillance-chief.html) (12.05.2008).

Clark, Ross. "Big Brother? Hardly. The CCTV cameras don't work – and actually make crime even worse". (07.05.2008) *Dailymail.* (http://www.dailymail.co.uk/news/article-1018394/Big-Brother-Hardly-The-CCTV-cameras-dont-work--actually-make-crime-worse.html) (12.05.2008).

- Daily Telegraph – Online

Iggulden, Amy. "CCTV channel beamed into you home". (10.05.2006) *Daily Telegraph - Online* (http://www.telegraph.co.uk/news/uknews/1517836/CCTV-channel-beamed-to-your-home.html) (05.07.2008).

- The Guardian – Online

Dodson, Sean. "The secret art of video sniffing. Real-life stars of CCTV". (25.04.2008) T*he Guardian.*. (http://arts.guardian.co.uk/filmandmusic/story/0,,2275895,00.html) (05.05.2008).

Weaver, Matt. "Residents given access to live CCTV footage" (11.1.2006) *The Guardian*. (http://www.guardian.co.uk/uk_news/story/0,,1684043,00.html) (11.10.2007).

- Le Figaro – Online

Threard, Yves. „Society under surveillance". (15.10.2007) *Le Figaro.* (http://www.lefigaro.fr/debats/2006/11/08/01005-20061108ARTWWW90245-society_under_surveillance.php) (12.02.2008).

- Die Presse – Online

Brandstetter, Sabine. „Wie Myspace & Co. die Karriere gefährden". (02.20.2008) *Die Presse*. (http://diepresse.com/home/bildung/unilive/416782/index.do?_vl_backlink=/home/bildung/unilive/index.do) (02.20.2008).

Marits, Mirjam.: „ ‚Big Brother': Gemeindebau-Videoüberwachung fix" (18.02.2008) *Die Presse*. (http://diepresse.com/home/panorama/oesterreich/363821/print.do) (07.04.2008).

Marits, Mirjam: „Gemeindebau: Überwachung kommt, Probleme bleiben" (25.03.2008) *Die Presse*. (http://diepresse.com/home/panorama/oesterreich/372177/print.do) (07.04.2008).

Nowak, Rainer, Fritzl, Martin, Stöger, Klaus: „Prokops Pläne: Massive Ausweitung der Videoüberwachung" (2.2.2005) *Die Presse.* (http://diepresse.com/home/politik/innenpolitik/134969/index.do?from=suche.intern.portal) (05.04.2008).

Röhsner, Georg. „Schon eine Attrappe kann zu viel sein" (31.03.2008) *Die Presse.* (http://diepresse.com/home/recht/rechtallgemein/373606/index.do?from=suche.intern.portal) (05.04.2008).

Wetz, Andreas: „Boom bei Spionagekameras“. (19.10.2007) *Die Presse*. (http://diepresse.com/home/politik/innenpolitik/338173/index.do?from=suche.intern.portal)(05.04.2008).

„ÖBB starten Videoüberwachung“ (01.05.2007) *Die Presse.* (http://diepresse.com/home/panorama/oesterreich/301059/print.do) (14.05.2008)

„Kontrolle wie in der DDR“.“ (22.09.2007) *Die Presse*. (http://diepresse.com/home/politik/innenpolitik/331831/index.do?from=suche.intern.portal) (10.05.2008).

- Der Spiegel – Online

„Telekom-Skandal. Diebe klauten 17 Millionen T-Mobile Kundendatensätze.“ (04.10.2008) *Spiegel-Online*. (http://www.spiegel.de/wirtschaft/0,1518,581938,00.html) . (05.10.2008).

Schmitt, Stefan. „Paradies der Gaffer und Spanner“. (10.06.2007) *Spiegel-Online*. (http://www.spiegel.de/netzwelt/web/0,1518,487708,00.html). (15.09.2008).

- Der Standard – Online:

„Videoüberwachung – Wiener Linien: ‚Vandalismus kommt nicht mehr vor’“ (25.07.2008) *Der Standard.* (http://derstandard.at/?id3234049) (13.05.2008).

- The Times – Online

Ford, Richard. “Beware rise of Big Brother state, warns data watchdog”. (16.08.2004) *Times-Online.* (http://www.timesonline.co.uk/tol/news/uk/article470264.ece). (05.10.2008).

Sherwin, Adam. “Broadband will make life rich in Shoreditch.” (19.01.2005) *Times-Online*. (http://www.timesonline.co.uk/tol/news/uk/article410580.ece) (10.10.2007).

- Die Zeit – Online

Luyken, Reiner. „Big Brother ist wirklich Brite“. (März 20007). *Die Zeit – Online*. (http://images.zeit.de/text/2007/03/Big-Brother) (11.10.2008).

Filmographie:

- *Citizen Cam*. R.: Scemla, Jérôme. Canal+. 1999. Frankreich, Island.

- *Die sichere Stadt* (Video) (http://www.zeit.de/video/player?videoID=200707185ecff9) (10.12.2007).

- *Equilibrium*. R. Kurt Wimmer. DVD. Highlight Video. 2000.

- *Every Step You Take: A documentary about video surveillance in the United Kingdom.* R.: Leitner, Nino. DVD. 2007. Österreich/Spanien.

- *Faceless.* D/R: Manu Luksch. DVD. Amour fou Filmproduktion. 2007. 50 min.

- *La Jetée*. (Am Rande des Rollfeldes) D/R: Chris Marker. Argos-Film. Französisch. Ut: Deutsch. UK. 1963. 28 min.
und: (http://www.youtube.com/watch?v=3RvmJan17q8) (10.06.2008).

- *Operation Spring*. R: Angelika Schuster / Tristan Sindelgruber. Schnittpunkt Filmproduktion. DVD: Der Standard-Edition. 2005. Österreich. 94.min.

- *the commercial*.
(www.mediashed.org/?q=videosniffincom) (05.05.08).

Weitere Quellen:

- Programmheft der „Big Brother Awards 2007“.

- „Talking the Fish”: Workshop mit Manu Luksch und Mag. jur. Alex Barasits. Graz: 28.-30. November 2007.

- Wien-Premiere: *Faceless*, 2. Mai 2008; daran anschließend ein Gespräch mit Manu Luksch. Moderation: Erich Möchl (futurezone.orf.at).

- Podiumsdiskussion: Wien 4. Mai 2008 mit: Manu Luksch, Hans Zeger (Arge-Daten), Doris Kaiserreiner (Quintessenz). Moderation: Ingrid Brodnig (Falter).

- Diskussion mit Dr. Hans Zeger zum Thema „Überwachungsunion Europa“. Wien: 8. Mai 2008.

Lebenslauf

- geb. 30.05.1981.
- 1987-1995: VS/HS Mauthausen
- 1995-2000: Höhere Land- und Forstwirtschaftliche Bundeslehranstalt (HLBLA) St. Florian (22 Wochen Praxis); Matura: Juni 2000.
- November 2000 - Mai 2001: Ableistung des Präsenzdienstes als Kraftwagenfahrer (LKW)
- seit 2001: Studium an der Universität Wien:

  Theater-, Film- und Medienwissenschaft

  Anglistik/Amerikanistik

2002/03: Ausbildung zum „Medizinischen Masseur“

Mitarbeit an Filmprojekten:

„Die Diebe“ R: Tom Eichtinger. 2005
Assisant to Art Director
„Mein Werk“ R: Erik 2006
Produktionsassistent
Imagefilm für die Diplomatische Akademie. R: Anna Baltl. 2006
Produktionsassistent
„Derniére“ R: Katrina Batliner. 2006
Produktionsassistent
„Bleiben will ich wo ich nie gewesen bin“ R: Libertad Hackl. 2006
Produktionsassistent
Musikvideo: Guadalajara – „No Matter“ R: Irfan Rehman. 2007
Assistant to Art Director
„H&M – Motivationsfilm“ R: Irfan Rehman. 2007
Art Director

Gebhardt Filmproductions:

„Die 4 Da“ R: Rupert Henning. 2008
Produktionsassistent
GIS – Werbung. R: Oliver Baier. 2008
Produktionsassistent
„Wir sind Kaiser“ R: Barbara Eder. Christopher Schier. 2008
Produktionsassistent