

1/2002

März 2002

H 7625

**LÄCHELN ... GLEICH KOMMT
DAS VÖGELCHEN**



**GEDANKEN ZUR
VIDEOÜBERWACHUNG**

ISSN 0938-3476

Inhalt

Editorial

■ <i>Alle(s) im Bilde ... – Gedanken zur Videoüberwachung</i>	3
---	---

Aktuell

■ <i>Kein Placet für Placebo – Helmut Pollähne</i>	7
■ <i>»Im aufrechten Gang« – Frieder Nake</i> <i>Laudatio zu Ehren von Prof. David L. Parnas</i>	9
■ <i>Sicher ist sicher ... – Peter Bittner</i>	54

Schwerpunkt

»Videoüberwachung«

■ <i>Im Haus der 1000 Augen – Eric Töpfer</i>	14
■ <i>Das Beispiel Videoüberwachung – eine neue Kultur der Kontrolle? –</i> <i>Hubert Beste</i>	18
■ <i>Chronologie der Dummheiten ... – padeluun und Wolfgang Föste</i>	21
■ <i>Videoüberwachung in Großwohnanlagen – Harald Stelljes</i>	25
■ <i>Technik und Leistungsfähigkeit automatischer Gesichtserkennung –</i> <i>Rolf P. Würtz</i>	27
■ <i>Videoüberwachungsregelung auf dem Prüfstand – Thilo Weichert</i>	30
■ <i>Kameraverhalten – Rena Tangens und padeluun</i>	34
■ <i>Das elektronische Auge im Blick – Leon Hempel</i>	38
■ <i>Freiheit und ihre Verstümmelung im »Synopticon«? – Hardy Frehe</i>	42
■ <i>Intelligent Bathroom Fixtures and Systems – Steve Mann</i>	46

FIfF e.V.

■ <i>18. FIfF-Jahrestagung in Freiburg im Breisgau</i>	6
■ <i>FIfF e.V., Vorstand und Regionales</i>	59
■ <i>FIfF Bibliothek</i>	60
■ <i>FIfF Adressen</i>	62

Rubriken

■ <i>Lesen – Neues für den Bücherwurm</i>	12
■ <i>Impressum</i>	63

Zum Titelbild:

Die getarnten Videokameras wurden gesehen in Aleskanderinkatu 8, Helsinki, erstmalig im Jahr 1996, aufgenommen im August 2001. Quelle: Julia Stoll.

Editorial

Alle(s) im Bilde ...

Gedanken zur Videoüberwachung

»Ich existiere nur insofern, als ich dauernd beobachtet werde«
(Zizek, 2000)¹

»Froschsein im Wasserglas« – Das Realexperiment Videoüberwachung

Seit nunmehr über 40 Jahren begegnet uns Kameraüberwachung im öffentlichen Raum. Was Ende der 50er Jahre mit Kameras zur Verkehrsüberwachung begann, setzte sich in Banken, Einzelhandel und Nahverkehr fort. Heute findet sich Videoüberwachung auch in Wohngebieten, Krankenhäusern, (Hoch-)Schulen, auf Flughäfen und Fernbahnhöfen, bei Groß-Events, in Shopping Malls oder gar in Umkleidekabinen und Toiletten. Angesichts der ständigen Verbreitung der Kameras und der »schlappen« Gegenwehr fühlt mensch sich wie der Frosch im Wasserglas:

»Die Reaktionsfähigkeit komplexer fortgeschrittener Gesellschaften lässt sich in bestimmter Hinsicht mit denen von Fröschen vergleichen. Wirft man eine solche Amphibie experimentealber in heißes Wasser, so wird der Frosch dieser unangenehmen Umgebung sofort zu entfliehen versuchen und mit einem Satz heraushüpfen. Setzt man das sensible Tier hingegen behutsam in ein mit Wasser gefülltes Gefäß und erhöht die Temperatur nur ganz allmählich in kleinen Schritten, so wird es die geringfügigen Veränderungen ertragen, sich jeweils an die Erwärmung gewöhnen und schließlich so lange verharren, bis es am Ende zu spät ist.«²

Es stellt sich also die Frage³: »Wie kann der Frosch über die langsame

Erwärmung aufgeklärt werden?« oder »Wie kann die Erwärmung des Wassers gestoppt werden?«

Bestandsaufnahmen

Zuallererst wollen wir uns innerhalb dieses Schwerpunktes der Bestandsaufnahme und der Beschreibung konkreter Diskurse und Projekte widmen:

Eric Töpfer beschreibt ein Europäisches Haus der 1000 Augen. Dabei wird besonders deutlich, dass die Kameraüberwachung des öffentlichen Raumes zu einem (nicht nur) »europäischen Trend« geworden ist – und das weitgehend unabhängig von den jeweiligen politischen Rahmenbedingungen. Schwerpunkte seiner Betrachtung sind die vier bestehenden europäischen Rechtsnormen, die Videoüberwachung betreffen, und die aktuelle Diskussion unter den Politikern im Europäischen Parlament und im Europarat.

Die Umrisse einer »neuen Kultur der Kontrolle« werden von Hubert Beste nachgezeichnet. Er thematisiert die nicht ausdrücklichen Funktionen der Videoüberwachung und formuliert die Erwartung ihrer zunehmenden Bedeutung. In der öffentlichen Diskussion herrschten pauschale Pressemeldungen und polizeiliche Lagebeurteilungen vor, die in den weitaus meisten Fällen bei der kriminalpräventiven Wirksamkeit ansetzten. Leider sind sozialwissenschaftlich informierte Befunde – bezogen auf die bundesdeutsche Situation – absolute Mangelware. Jedenfalls lassen sich die tiefgreifenden Veränderungen, die die Kriminalitätskontrolle in den letzten drei Jahrzehnten durchlaufen hat, nur dann verstehen, wenn wir die sozialen, kulturellen und politischen Kräfte integrativ betrachten, die diesen Wandel getragen und forciert haben.

Einer der »Modellversuche« zur Videoüberwachung betrifft den

Ravensberger Park in Bielefeld. In einer »Chronologie der Dummheiten« entlarven padeluun und Wolfgang Föste aus bürgerrechtlicher Sicht den (ordnungs-)politischen Wahnsinn, einen innenstadtnahen Park als »Kriminalitätsschwerpunkt« zu deklarieren, um dort entsprechend der polizeigesetzlichen Erfordernisse Videoüberwachung durchzusetzen. Das Ende vom Lied ... die Kameras werden abgeschaltet, da auf sie nach »erfolgreicher Minderung der Kriminalität« (so die offizielle Lesart) nun verzichtet werden könne. Der hierzu kurz nach Redaktionsschluss eingegangene aktuelle »Nachruf« auf das Pilotprojekt im Ravensberger Park von Helmut Polilähne liefert wichtige Hintergründe für diese Posse!

Im Jahre 1999 beabsichtigte ein Bremer Wohnungsunternehmen, ihre Großwohnanlagen mit Videokameras zu überwachen. Man zielte mit dieser Maßnahme auf die Verhinderung/Minderung von Sachbeschädigungen. Harald Stelljes berichtet uns aus Sicht des zuständigen Landesbeauftragten für den Datenschutz von den damaligen Ergebnissen des Prüfungsverfahrens auf der Grundlage der gesetzlichen Regelungen vor Inkrafttreten des neuen § 6b (Videoüberwachung) des Bundesdatenschutzgesetzes.

Eine Studie des Büros für Technikfolgenabschätzung (STOA) des Europäischen Parlamentes von 1998 macht sehr deutlich, dass »the revolution in urban surveillance will reach the next generation of control once reliable face recognition comes in«. Berichte von Einsätzen von Gesichtserkennungssoftware und vor allem die im Rahmen des sog. Terrorismusbekämpfungsgesetzes vorgenommenen Änderungen der Ausweis- und Passgesetze mit der Einführung biometrischer Merkmale »von Fingern oder Händen oder Gesicht«, fordern uns auf, uns näher mit der Technik und Leistungs-

1. Zizek, S. (2000): Die Kamera liebt dich. Unser Leben als Seifenoper. In: Balke, F. et. al. (Hrsg.): Big Brother. Beobachtungen, Bielefeld: transcript Verlag, 2000, S. 151–155, hier: S. 152.
2. Nogala, Detlef: Der Frosch im heißen Wasser? in: Schulzki-Haddouti, Christiane (Hrsg.): Vom Ende der Anonymität. Die Globalisierung der Überwachung. Hannover: Heise Verlag, 2000, S. 139
3. wie sie Rena Tangens und padeluun in ihrem Beitrag stellen!

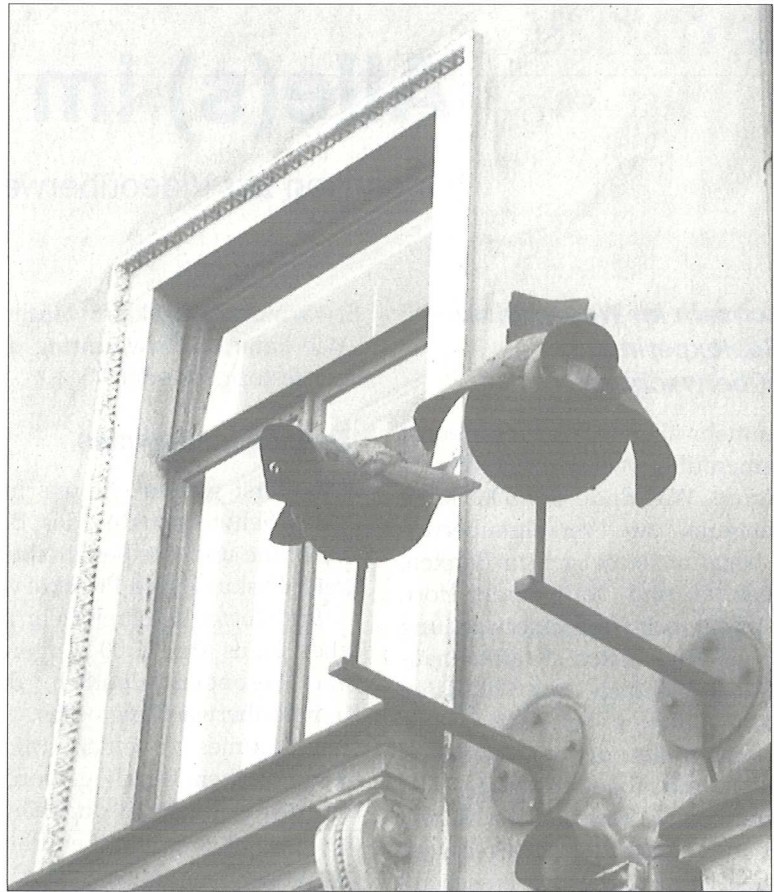
fähigkeit automatischer Gesichtserkennung auseinander zu setzen. Rolf P. Würtz gibt uns einen Überblick über Aufgaben und Probleme im Forschungsbereich des automatischen Bildverstehens, der sich in den vergangenen Jahren zunehmend auf die Verarbeitung von Bildern und Bildfolgen von Personen konzentriert. Er erläutert die Funktionsweise von Gesichtserkennungssystemen und die Probleme der unabhängigen Beurteilung solcher Systeme. Er macht klar, dass derzeit nur wenig »Vertrauen« in solche Systeme gesetzt werden sollte. Nichtsdestotrotz sollte aber die gesellschaftliche Diskussion um Videoüberwachung nicht ob der »mangelnden Funktionsfähigkeit« vertagt werden.

Späte rechtliche »Einhegung« eines Phänomens

Obschon wir es seit über 40 Jahren mit Kameraüberwachung in der Praxis zu tun haben, ist sie erst spät als besonderes verfassungs- und datenschutzrechtliches Problem erkannt worden. Regelungen bestanden bisher im Rahmen der Strafprozeßordnung (§§ 81b und 100c StPO), seit Juni 1989 gibt es Befugnisnormen für das Versammlungsrecht. Daneben bestehen Überwachungsbefugnisse des Bundesgrenzschutzes bzw. länderspezifische Regelungen im Polizei- und Ordnungsrecht. Letztere Regelungen wurden nach dem 11. September vielerorts verschärft – insbesondere auch in Hinblick auf die »vereinfachte« Ermöglichung von Videoüberwachung.

Die Leser/innen möchten wir in diesem Kontext auf eine sehr wichtige und nützliche Netzquelle hinweisen. Unter <http://www.datenschutz.hessen.de/o-hilfen/VideoverfassFragen.pdf> findet sich eine quellenintensive Zusammenschau und Beurteilung verfassungs- und verwaltungsrechtlicher Regelungen im Kontext von Videoüberwachung, die wir dem Hessischen Datenschutzbeauftragten Prof. Dr. Friedrich von Zezschwitz zu verdanken haben.

Im Mai 2001 wurde im Rahmen der letzten BDSG-Novelle mit dem § 6b eine Vorschrift erlassen, die die Beobachtung und Aufzeichnung im öffentlichen Raum sehr knapp, aber aus unserer Sicht wenig aussagekräftig



regelt. Thilo Weichert setzt sich sehr kritisch mit dem Entstehen und den konkreten rechtlichen Regelungen des § 6b BDSG auseinander. Neben dem Vollzugsdefizit bei der Hinweispflicht (leider sind Verstöße gegen die Hinweispflicht nicht bußgeldbewährt) ergeben sich aus der getroffenen Regelung zwei erhebliche Probleme: zum einen eine uferlose Weite an Erlaubnistatbeständen, zum anderen der Verzicht auf die Meldepflicht. Letzteres ist auch schwerlich mit den Art. 20 (Vorabkontrolle) und 21 (Anzeige- und Veröffentlichungspflichten) der EU-Datenschutzrichtlinie vereinbar: denn erst durch eine Anzeigepflicht wird der Betreiber einer Videoanlage dazu angehalten, eine rationale Begründung der Erforderlichkeit der Anlage zu liefern.

Rena Tangens und padeluun bearbeiten das Problem der notwendigen »Einhegung« der Kameraüberwachung ausgehend vom Recht auf informationelle Selbstbestimmung. Sie machen deutlich, inwiefern informationelle Selbstbestimmung für eine »lebendige« Demokratie wichtig ist und wie sehr die Beschädigung eben

jenes Grundrechtes anhand der Kameraüberwachung sich negativ auf die Demokratie auswirkt.

Wir können eigentlich nur der Einsicht Weicherts folgen, dass der wesentliche rechtliche Aspekt bei der »normativen Einhegung von Videoüberwachung« darin gesehen werden muss, »dass Videoüberwachung das Pilotprojekt für die anlasslose technische Überwachung potenziell der gesamten Bevölkerung ist«.

Analysen und »Deutungen«

Ein wesentliches Problem bei der adäquaten Bewertung von Videoüberwachung liegt hierzulande darin, dass Evaluationen bislang nur als Begleitmaßnahmen von Pilotprojekten vorliegen, die über die Zielerreichung eines Einsatzes berichten. Diese werden meist von den Betreibern der Überwachungsanlagen durchgeführt, wobei der Fokus auf der statistischen Auswertung von Kriminalität liegt. In Großbritannien haben wissenschaftliche Evaluationen hingegen zu einer Fülle inkonsistenter Ergebnisse über den Nutzen geführt. Dies hat nicht zuletzt dazu beigetragen, Evaluie-

rungsansätze neu zu überdenken. Leon Hempel zeigt in seinem Beitrag auf, wie »realistische Evaluationen« aussehen sollten, die Videoüberwachung nicht mehr allein auf ihre intendierten Ziele und Wirkungen prüfen, sondern auch hinsichtlich ihrer politischen und sozialen Nebeneffekte untersuchen.

Der Beitrag »Freiheit und ihre Verstümmelung im 'Synopticon'?« von Hardy Frehe schließlich widmet sich der sozialphilosophischen Dimension der Überwachungstechnik. Thematisch wird dabei der latente Anpassungsdruck durch die Überwachung, das Aufkündigen des Vertrauens in den neuinstrumentierten Räumen sowie die Gefahr der Verselbständigung der technischen Überwachungsinfrastruktur. Er untersucht akribisch die Auswirkungen, die sich für unser Selbst- und Weltverhältnis ergeben, und bettet dies in die aktuellen sozialphilosophischen Diskurse ein.

Kunst der Gegenwehr – Gegenwehr der Kunst

Shooting back – titelte der NetGuide im Juni 1995 in einem Beitrag (von Larry Husten) über den damaligen Studenten am MIT Media Lab – Steve Mann, der nach Mitteln des fairen Ausgleichs auf dem »Surveillance Superhighway« suchte. Berühmt wurde er als »wandelnde Kamera«; über seine WearCam stellt er die aufgenommenen Bilder (manchmal live) im Internet zur Verfügung. In seinem Beitrag »Intelligent Bathroom Fixtures and Systems« liefert Steve Mann tiefe Einblicke in die Forschungsabteilung »Aquionics Research« der EXISTech Corporation, die sich auf den Weg gemacht hat, uns in die »schöne neue Badewelt« zu entführen. »By using video based sensors, the intelligent bathroom provides a safe, hygienic, and user friendly environment that responds automatically to the needs of the user. Concomitant functions, such as security, drowning prevention, and other safety features are possible with the intelligent bathroom«. Ein Schelm, wer Böses dabei denkt!

Mit viel Phantasie haben das »Institute for Applied Autonomy« (<http://www.appliedautonomy.com>)

und das »New York Surveillance Camera Project« (<http://www.mediaeater.com/cameras/>) einen Stadtplanservice der besonderen Art geschaffen: Nach Eingabe eines Startpunktes und eines Zielpunktes (in Manhattan) erhält man eine Empfehlung für den Weg der geringsten Kameradichte (siehe unser Schlußpiff). Wer also nichts zu verbergen hat, der ist bei iSee richtig.

Kunstfertig hat der Australier Denis Beaubois die klassische Beobachtersituation bei der Videoüberwachung verkehrt. Er erschien jeweils drei Tage lang hintereinander in unmittelbarer Sichtweite einer Kamera und erwiderte deren indifferenten Blick. Dank seiner Ausbildung in der Bhuto-Performance-Technik mit einer ungewöhnlichen Fähigkeit zu willentlicher Unbewegtheit ausgestattet, forderten seine demonstrative Regungslosigkeit und die starre Gerichtetheit seiner Augen früher oder später irgendeine Reaktion heraus. Manchmal erfolgte sie so rasch, dass Beaubois nur wenige Minuten nach seiner Ankunft aus dem »öffentlichen« Raum »hinauskomplimentiert« wurde, mit der »Erklärung«, er sei ein Ruhestörer oder er habe keine Genehmigung oder irgendeiner ähnlichen, ebenso unplausiblen wie symptomatischen bürokratischen Banalität. Seine Performances »In the event of Amnesia the city will recall...« waren den Juroren des Internationalen Medienkunstpreises bei der Verleihung in Karlsruhe einen Sonderpreis wert.

Ähnlich zeigen die New Yorker Surveillance Camera Players (<http://www.notbored.org/the-scp.html>) seit 1996 ihren gewaltlosen Protest durch die stumme Aufführung von Kurzfassungen von (z.T. eigenen) Theaterstücken vor Videokameras. In einem Manifest schreibt die Gruppe um den Gründer Bill Brown⁴: »Wir sind nur ein paar Otto-Normalverbraucher, die sich vorstellen können, wie langweilig es für die Wachmänner, die ununter-

brochen unser Verhalten in der ganzen Stadt beobachten, sein muss, den ganzen Tag die Videobilder auf ihren Monitoren anzusehen«.

Wer sich für einen umfassenderen Überblick über die Techniken der Überwachung und ihre Spiegelung in den Künsten interessiert, der sollte einen Blick in die Dokumentation⁵ der Ausstellung »CTRL (Space) Rhetorik der Überwachung von Bentham bis Big Brother« am Zentrum für Kunst- und Medientechnologie (Karlsruhe) werfen.

Wir machen weiter!

In dieser Ausgabe haben wir uns um ein breites Themenspektrum – viele Blickpunkte – bemüht, sicher blieben einige Aspekte des Komplexes »Videoüberwachung« nicht berücksichtigt oder konnten aus Platzgründen nicht in der notwendigen Tiefe behandelt werden. Deshalb hat sich die Schwerpunktredaktion dazu entschlossen, zum Thema »Videoüberwachung« ein Buch⁶ herauszugeben, das Langfassungen einiger vorgestellter Beiträge und weitere im Heft nicht berücksichtigte und neue⁷ Beiträge enthalten wird. Dieses kann ab Anfang April zum Vorzugspreis vorbestellt werden unter: <http://waste.informatik.hu-berlin.de/peter/kritinf/subskription.html>

Um die begonnene interdisziplinäre Arbeit auszuweiten und das »kritische« Potential besser vernetzen zu können, wird demnächst ein überregionaler Arbeitskreis »Videoüberwachung und Bürgerrechte« vom FIFF ins Leben gerufen werden. Bei Interesse wenden Sie sich bitte an Peter Bittner (bittner@informatik.hu-berlin.de).

So – nun bleibt uns nur noch, Ihnen eine spannende Lektüre zu wünschen. Wir sind sehr gespannt auf Ihre Reaktionen.

Das Redaktionsteam:
Peter Bittner, Hardy Frehe,
Julia Stoll & Jens Woinowski

4. Ein Interview mit Bill Brown, dass Tilman Baumgärtel führte, ist in dessen Buch »Net.art 2.0« (Nürnberg: Verlag für moderne Kunst, 2001) unter dem Titel »Paranoide Leute sind rational« abgedruckt. Der zitierte Passus stammt aus dem dort veröffentlichten Beitrag zum bezeichneten Interview.

5. Die Ausstellung hat leider schon Ende Februar ihre Pforten geschlossen.
6. Dieser Sammelband soll in der Reihe »Kritische Informatik« beim LIT-Verlag in Münster erscheinen. Wir planen die Herausgabe des Bandes für das Jahresende.
7. Weitere Beiträge sind herzlich willkommen. Senden sie bitte Vorschläge und Kurzfassungen bis Ende April an die Schwerpunktredaktion (bittner@fiff.de).

Achtung! Geänderter Termin! – Achtung! Geänderter Termin! – Achtung! Geänderter Termin!

18. FIFF-Jahrestagung

Technik, Geschlecht, Gesellschaft

18. bis 20. Oktober 2002 in Freiburg i. Br.

Die FIFF-Jahrestagung 2002 wird sich auf breiter Basis mit Veränderungen durch Informations- und Kommunikationstechnik beschäftigen, die auch das Geschlechterverhältnis betreffen. Von Freitagabend bis Sonntag werden in mehreren Hauptvorträgen und Arbeitsgruppen vielfältige Themen aus diesem Bereich vorgestellt und diskutiert.

Hauptvorträge:

Christiane Floyd:

(Universität Hamburg)

zu Software Engineering
(angefragt)

Gabriele Winker

(FH Furtwangen)

zu Telearbeit

Cecile Crutzen

(Open Universiteit Heerlen)

zu Objektorientierung

Wie immer wollen wir während der Tagung verschiedene Themen in Arbeitsgruppen intensiver bearbeiten. Vorgesehen sind halb- und ganztägige AGs zu unterschiedlichen Themen. Ein besonderer Fokus soll auf dem Thema Überwachungsstaat liegen, das in einer ganztägigen Arbeitsgruppe diskutiert werden soll.

Wer aktiv mit einer AG oder einem Tutorial teilnehmen möchte, sollte sich umgehend mit der Organisationsgruppe der Tagung in Verbindung setzen.



Daneben bietet Freiburg natürlich noch einige Attraktionen, die das Programm abrunden werden: das könnte z.B. eine Stadtführung, ein spanisches Abendessen oder eine Weinprobe mit Weinen aus dem Ländle sein.

Bitte helft uns, die Tagung bekannt zu machen: Fordert Plakate, Flyer etc. bei der Organisationsgruppe an und sagt allen euren FreundInnen, KollegInnen und GeschäftspartnerInnen Bescheid: Treffpunkt im Oktober im sonnigen Süden.

Weitere Informationen gibt es demnächst unter:

<http://mod.iig.uni-freiburg.de/fiff-JT2002>

Kontakt über die Organisationsgruppe:

FIFF-Jahrestagung
Institut für Informatik und Gesellschaft
Abteilung 1: Modellbildung und soziale Folgen
Friedrichstr. 50
79098 Freiburg i. Br.
Tel.: 0761/203-4952
Fax: 0761/203-4960
fiff@modell.iig.uni-freiburg.de

Wir hoffen, dass durch die Terminänderung niemand an der Teilnahme verhindert sein wird. Es war die endgültig letzte Terminänderung.

Helmut Pollähne

Kein Placet für Placebo

Ravensberger Videoüberwachung – Nachruf auf ein Pilotprojekt

Der Beitrag von padeluum & Wolfgang Föste (S.21-24) über die »Chronologie der Dummheiten« aus dem 'Oberzentrum der Mittelmäßigkeit' endet mit der Meldung, dass die Videoüberwachung (VÜ) im Ravensberger Park der Stadt Bielefeld am 31.3.2002 abgeschaltet wird ... werden soll: Ich glaube es erst, wenn tatsächlich – wie geplant – Säcke (!) über den installierten Kameras hängen; abmontiert werden sie wohlweislich nicht.

Wege des juristischen Widerstands

Zum besseren Verständnis der 'Karriere' dieses nordrhein-westfälischen VÜ-Pilotprojekts – von der unbeirrbar Installation bis zum jähen Ableben – seien hier einige rechtliche Imponderabilien¹ ausgebreitet, die der VÜ im Allgemeinen und in Bielefeld im Besonderen nicht nur das virtuelle sondern vor allem auch das justizielle und damit nicht zuletzt das ganz reelle Leben schwer machen.

Um nicht lange drum herum zu reden: Ich habe als Bielefelder Bürger den Weg des juristischen Widerstands beschritten, habe gegen die Inbetriebnahme der VÜ-Kameras Widerspruch eingelegt und nach dessen zu erwartender Ablehnung durch den örtlichen Polizeipräsidenten Klage vor dem Verwaltungsgericht in Minden erhoben.²

Dort liegt die Klage noch immer unbearbeitet in einem Stapel auf dem Tisch eines Verwaltungsrichters, wie ich vermute ... sie hat aber offenbar ihre Wirkung nicht verfehlt, auch wenn sich die Polizei bemüht zu beweisen, die VÜ sei ein voller Erfolg gewesen und deshalb (!) könne sie, nein: müsse sie nun abgeschaltet werden. Es erscheint nicht ganz abwegig anzunehmen, so möchte ich ohne

Bescheidenheit hinzufügen, dass der Bielefelder Polizeipräsident eine gerichtliche Niederlage vermeiden wollte ... aber der Reihe nach und in kleinen Schritten, die auch juristischen Laien verständlich machen, woran die VÜ in Bielefeld verstorben ist.

VÜ als gesetzlich zu regelnder Eingriff in Grundrechte

Anderenorts musste man sich in der Vergangenheit darüber streiten, ob VÜ überhaupt einen Eingriff in individuelle Grundrechte darstellt, der gerichtlich angefochten werden kann, da die VÜ zum Teil ohne (spezial)gesetzliche Grundlage installiert worden war. Bei dem darüber entbrannten juristischen Streit ging es u.a. um die Frage, ob die Kameras auch dann einen Eingriff darstellen, wenn sie 'nur' sog. 'Übersichtsaufnahmen' liefern, auf denen einzelne Personen angeblich nicht identifizierbar seien.

So hat etwa das Verwaltungsgericht Halle einen Eilantrag gegen die VÜ des Marktplatzes der Stadt mit der Begründung als unzulässig abgelehnt, mangels Eingriffsqualität bedürfe es keiner gesetzlichen Grundlage³. Mag sein, dass jener Antrag etwas naiv war ... die Begründung des VG Halle war mindestens so ignorant, denn jenseits der Gerichte und Polizeibehörden haben bisher alle Juristen, die sich fachwissenschaftlich dazu geäußert haben, die Eingriffsqualität bejaht und spezialgesetzliche Grundlagen gefordert.⁴

Was letzteres betrifft ist der Streit inzwischen einigermaßen gegenstandslos, denn immer mehr Bundesländer haben binnen kurzer Zeit entsprechende Rechtsgrundlagen verabschiedet – der juristische Streit um die Eingriffsqualität wird die Gerichte

aber voraussichtlich noch einige Zeit beschäftigen.

Rot-grüne Kompromisse: § 15a Polizeigesetz und das Bielefelder Pilotprojekt

In Bielefeld gab es diese Probleme nicht, denn hier existierte bereits seit April 2000 eine ausdrückliche gesetzliche Grundlage in § 15a des nordrhein-westfälischen Polizeigesetzes. Was aber noch wichtiger ist: Gegenüber den meisten anderen polizeirechtlichen Vorschriften zur VÜ, die in den letzten zwei Jahren entstanden sind, erweist sich die hiesige Regelung als relativ restriktiv, denn die tatbestandlichen Voraussetzungen, die vorliegen müssen, um den VÜ-Betrieb zu legalisieren, sind vergleichsweise eng gefasst: »Zur Verhütung von Straftaten kann die Polizei einzelne öffentlich zugängliche Orte, an denen wiederholt Straftaten [von erheblicher Bedeutung] begangen wurden, mittels Bildübertragung beobachten, solange Tatsachen die Annahme rechtfertigen dass dort weitere Straftaten [von erheblicher Bedeutung] begangen werden ...«

Teil des mühsam errungenen rot-grünen Kompromisses zu § 15a PolG-NW war, zunächst ein Pilotprojekt zu starten und erst nach Abschluss der Begleitforschung (Prof. K. Boers, Universität Münster) über die Zukunft der Regelung und weiterer VÜ in Nordrhein-Westfalen zu entscheiden. Warum ausgerechnet Bielefeld den Zuschlag für das Pilotprojekt erhielt, bleibt unerfindlich und nährt allenfalls Spekulationen, die hier nicht ausgebreitet werden müssen: Immerhin zeichnet sich das 'Oberzentrum der Mittelmäßigkeit' u.a. dadurch aus, dass es die Großstadt mit der niedrigsten Kriminalitätsrate im Lande ist (und – in diesem Sinne – eine der 'sichersten' der Republik).

1. Unwägbarkeiten, unvorhersehbare Umstände oder Einflüsse

2. Widerspruch und Klage (Az 2 K 1548/01) sind einzusehen unter www.foebud.org/texte/aktion/vibi/Video-spruch.pdf

3. abgedruckt in der Zeitschrift *Landes- und Kommunalverwaltung*, Heft 4/2000 S.164

4. eine jeweils aktuelle Literaturliste kann beim Autor angefordert werden

Zudem gab es bereits im Vorfeld warnende Stimmen, die das Scheitern des Pilotprojekts prophezeiten ... alles in den Wind geschlagen: Am 28.02.2001 wurden die nur mit Mühe installierten fünf Kameras in der Bielefelder Innenstadt in Betrieb genommen (vgl. dazu die 'Chronologie der Dummheiten').

Zur Rechtswidrigkeit der Ravensburger VÜ

Meine Klage konnte sich – den engen gesetzlichen Vorgaben entsprechend – darauf beschränken, die Rechtswidrigkeit der Inbetriebnahme zu reklamieren, weil spätestens zu diesem Zeitpunkt die gesetzlichen Voraussetzungen nicht (mehr) vorlagen. Pech für die Polizei, dass dies mit den offiziellen Zahlen zu belegen war: Die Anzahl der sog. 'Straftaten von erheblicher Bedeutung', die das Gesetz in § 15a verlangt, ging in diesem Park von 21 im Jahre 1999 auf 7 im Jahre 2000, also dem Jahr vor (!) der VÜ-Inbetriebnahme, zurück. Für das VÜ-Jahr 2001 wurden hingegen 9 solcher Delikte verzeichnet.

Zunächst einmal: Wenn die Zahl von 7 oder 9 Straftaten von erheblicher Bedeutung (konkret: Drogenhandel, gefährliche Körperverletzung, Raub) im Laufe eines Jahres in einem Innenstadtbereich von gut fünf Hektar Parkfläche bereits einen Kriminalitätsschwerpunkt ausmacht, so wären damit wohl nahezu alle Innenstädte Kriminalitätsschwerpunkte und reif für die VÜ ... das mag ganz im Sinne so mancher VÜ-Protagonisten sein, lässt sich jedoch weder mit dem hiesigen Landespolizeirecht noch mit dem Grundgesetz vereinbaren, aber das nur am Rande.

Placebo-VÜ – oder: Das Spiel mit der Kriminalstatistik ...

Die Peinlichkeit, dass die einschlägigen Straftaten vor Ort von einem niedrigen Niveau auf ein noch niedrigeres absanken, bevor (!) die VÜ installiert wurde, versuchte die Polizei auf zwei Wegen zu parieren: Mit einem plumpen Rechenrick, der die Zahlen für die Jahre 1998/99 einerseits und 2000/01 andererseits so gruppierete, dass auf den ersten Blick der Eindruck eines

Kriminalitätsrückgangs entstand, und mit einer – wohl ebenso ernst gemeinten – kriminologisch anmutenden Erklärung: Der Placebo-Effekt 'angedrohter' Kameras. Die Ravensberger VÜ wird mit anderen Worten nachträglich als ein Erfolg gefeiert, der bereits eintrat, bevor sie überhaupt auf Sendung ging. Potentielle Straftäter 'von erheblicher Bedeutung' lassen sich offenbar – jedenfalls im 'Oberzentrum der Mittelmäßigkeit' – schon von der bloßen Ankündigung einer VÜ abschrecken ... was aus ihnen geworden ist, blieb zunächst offen, und dass gewisse Probleme in einem anderen Park der Stadt zunahmen, blieb unkommentiert ...

Ohne hier rechtsdogmatische Details ausbreiten zu können und zu wollen, nur so viel zur Rechtslage der Ravensberger VÜ: Die Polizei muss belegen und vor Gericht gegebenenfalls unter Beweis stellen, dass die gesetzlichen Voraussetzungen vorliegen; die bloße Behauptung eines Kriminalitätsschwerpunkts, dem man anders als durch VÜ nicht mehr Herr werde, reicht vielleicht vor einer uninformierten Öffentlichkeit, nicht aber vor dem Gesetz aus. Es muss sowohl die Kriminalitätsentwicklung (im Hinblick auf die genannten 'Straftaten von erheblicher Bedeutung') dargelegt werden, und zwar insbesondere im Vergleich zur sonstigen Kriminalitätslage der Stadt, und es muss die prognostische Einschätzung belegt werden, nur mit Hilfe der VÜ (und nicht durch andere Maßnahmen, die weniger in die Rechte von BürgerInnen eingreifen) könne diese Kriminalität zurückgedrängt werden, ohne sie jedoch lediglich zu verdrängen, denn das wollte der Gesetzgeber explizit nicht. Die Beweise wurden bisher nicht erbracht, die dargelegten Zahlen belegen vielmehr das Gegenteil. Die Vermutung liegt nahe, dass die Kameras im Februar 2001 in Kenntnis dieser Zahlen installiert und in Betrieb genommen wurden, um das Pilotprojekt nicht zu gefährden und das Gesicht nicht zu verlieren – wie kurzfristig ... und (eben) rechtswidrig!

Von der rechtlich umstrittenen zur vorsätzlich rechtswidrigen VÜ

Nun rudert die Polizei zurück, spät, zu spät, aber immerhin: Dass sie bemüht ist, das Pilotprojekt als Erfolg zu verkaufen ist verständlich, entpuppt sich aber als untauglicher Versuch – das wird spätestens der Abschlussbericht der Begleitforschung belegen, die sich (wie zu hören war) die fachwissenschaftlichen Haare raufte.

Das rechtswidrige i-Tüpfelchen ist freilich, dass die Kameras noch bis Ende März weiter betrieben werden sollen, obwohl bereits öffentlich bekundet wurde, dass die gesetzlichen Voraussetzungen nicht mehr vorliegen: Seit dem Tag, an dem den Verantwortlichen dies bewusst wurde, werden die Kameras vorsätzlich rechtswidrig betrieben ...

Mag es dafür auch 'gute' Gründe geben (in einem Museum innerhalb dieses Parks läuft bis Ende März die sog. 'Wehrmachtsausstellung', vielleicht ist auch die Laufzeit der Begleitforschung noch nicht um), mit § 15a PolG-NW ist dies nicht vereinbar und das ist den Verantwortlichen klar. Möglicherweise bedarf es doch noch eines Antrags auf Erlass einer einstweiligen Anordnung ...

Zwiespalt am Ende

Leider hat der 'kleine Triumph' am Ende doch einen bitteren Beigeschmack: Die Debatte um eine Verschärfung des § 15a PolG-NW hat bereits begonnen, nicht nur hier in Bielefeld. Das Scheitern des Pilotprojekts müsste eigentlich dazu führen, wenn schon nicht VÜ prinzipiell in Frage zu stellen, so doch wenigstens beim nächsten Mal etwas genauer hinzusehen, ob es sich wirklich im Sinne des Gesetzes um einen sog. 'Kriminalitätsschwerpunkt' handelt, damit wenigstens die Begleitforschung Sinn macht.

Statt dessen wird in Leserbriefen und aus bestimmten politischen Ecken heraus der rot-grünen Landesregierung absurder Weise vorgeworfen, die Städte des Landes schutzlos der Kriminalität auszuliefern. Dazu fällt einem in der Tat nicht viel mehr ein als padelun: »Dumppbackenpolitik für Dumppbacken«.

Im aufrechten Gang

Zu Ehren von Prof. David L. Parnas
aus Anlass der zweiten Vergabe des FlfF Preis
auf der Jahrestagung am 30.9.2001 in Bremen

Frieder Nake, Universität Bremen

Das FlfF ehrt mit der Vergabe seines Preises an Prof. David L. Parnas einen Ingenieur der Software, wie man ihn sich als Vorbild für den aufrechten Gang nicht würdiger vorstellen kann. Dies ist die zweite Verleihung des Preises, nach Joseph Weizenbaum.

Mir ist die Aufgabe zugedacht worden, einige Worte über David Parnas zu sagen. Ich tue das gern und muss zugleich um Verständnis dafür bitten, dass ich keine umfassende Darstellung von Leben und Werk Parnas' geben kann. Ich kann nur den Aspekt herausgreifen, dessentwegen ihm der Preis verliehen wird.

Zur aktuellen Situation und zum Rahmen des FlfF

Wir leben in einer Zeit, die von großer Unruhe unter dem Himmel gekennzeichnet zu sein scheint. „All that is solid melts into air“, heisst es in der englischen Übersetzung des Kommunistischen Manifest – ein Satz, dessen Wahrheit die Geschichte immer wieder beweist. Seit knapp drei Wochen, seit dem 11.9.2001, scheint es uns, als sei eine gravierende Zäsur im politischen Weltgeschehen eingetreten. Auch diese Tagung legt Zeugnis davon ab.

Im Radio hörte ich, wie jemand fragte, wo denn angesichts der Ereignisse und Beunruhigungen Amerikas Intellektuelle seien? Man höre kaum etwas von ihnen, hieß es. Und Susan Sontag sei die rühmliche Ausnahme. Es stimmte dies nicht so wörtlich zwar. David Parnas gehörte zu jenen, von denen man bald schon nach dem Ereignis hören konnte. „We must be willing to live by the rules that we expect others to follow, if we want to live in peace“, sagte er am Schluss einer nachdenklichen Presse-Betrachtung in

Kant'scher Manier. „Nobody will be safe until all are safe.“

Die US-Vereinigung von WissenschaftlerInnen und PraktikerInnen, *Computer Professionals for Social Responsibility* (CPSR), die die Norbert Wiener Award verleiht, entstand 1981 aus der Sorge um das Reagan'sche SDI-Programm, das populär als „Star Wars Program“ bezeichnet wird. Die deutsche Schwester-Organisation FlfF trat aus gleichem Anlass etwas später in Erscheinung. Einige Menschen sind hier anwesend, die zu den Vorbereitern und Gründern des FlfF gehören. In der damals noch westdeutschen BRD war es eine deutlich oppositionelle Gründung, gegen das Establishment in Staat und Informatik gerichtet, in der sich liberale, moralische und linke Gesinnungen zusammentaten. Für manche unter uns, so auch mich, war es deswegen leicht befremdend, als David Parnas seine Stimme gegen die Planungen zum Krieg der Sterne erhob. Was, um Himmels Willen, wollen die Technokraten in unserem politischen Einklang, so vielleicht die Frage. Von ihm konnte man aber lernen, schälte sich heraus, dass eine politische Schlussfolgerung auch aus professioneller Einsicht gezogen und in grösster Ernsthaftigkeit entwickelt werden konnte. Denn er war ja nicht einfach nur überhaupt gegen das, was da getan werden sollte; er fand vielmehr, die Ziele seien durchaus in Ordnung, der Weg aber sei der falsche, ja, dieser Weg sei sogar gefährlich, man müsse ihn ablehnen und dies auch kundtun. Seine Argumente dafür waren detailliert und mussten technisch nachvollzogen werden. So steht Parnas seit 16 Jahren als ein Ingenieur in der Welt, der als Professioneller seine Stimme zum Zeitgeschehen erhebt. Er erhebt sie auch im grimmigen Gegenwind.

Lebensdaten

David Parnas ist am 10.2.1941 in Plattsburgh im Staat New York geboren. Sein Vater war aus Berlin, die Mutter aus Wien. Er ist heute Kanadier, mit einer Chinesin verheiratet. Vor kurzem also ist er 60 Jahre alt geworden. Im Mai 2001 gab es im Rahmen der International Conference on Software Engineering in Toronto zu Ehren von Parnas ein David L. Parnas Symposium, das unter dem Motto „Thinking hard about software“ stand. Programmatisch.

Die Liste einiger seiner Stationen ist beeindruckend:

- er hat nach Bachelor- und Master-Abschlüssen in Elektrotechnik an der Carnegie Mellon University (damals noch Carnegie Institute of Technology) dort promoviert,
- er hat an der Carnegie Mellon University, der University of Maryland, der TH Darmstadt, der University of North Carolina at Chapel Hill, der University of Victoria, B.C., der Queen's University in Kingston, Ont., gelehrt und geforscht,
- er ist seit einigen Jahren im Computing and Software Department an der McMaster University in Hamilton, Ont., tätig,
- er war außerhalb des akademischen Bereiches u.a. bei Philips in Appeldoorn, beim United States Naval Research Laboratory in Washington, D.C., bei IBM, beim Atomic Energy Control Board of Canada als Berater tätig,
- er hat Ehrendoktorgrade von der ETH Zürich und der Université Catholique de Louvain (Belgien) erhalten,
- er war 1987 der erste Preisträger der Norbert Wiener Award, die

von CPSR vergeben wird. Die Tagung von CPSR fand passenderweise am MIT statt, Terry Winograd hielt die Laudatio,

- er weist eine beeindruckende Liste von Publikationen auf, die ein weites Themenspektrum überstreichen,
- er ist Mitglied der Royal Society of Canada und ein ACM Fellow,
- seinen eigenen Zielsetzungen gemäß ist er ein anerkannter Professional Engineer in Ontario.

Wissenschaftler und Ingenieur

Manchem unter uns gehen wissenschaftliches Handeln und Ingenieur-dasein nicht ungebrochen durch die Gehirnwindungen. Ein Gesichtspunkt, in dem beide sich jedoch treffen müssen, ist die Begeisterung für das rigorose Vorwärtsdrängen und Weiterfragen wie gleichzeitig die Sorge um das unerläßliche Aufdecken der Grenzen und Unmöglichkeiten der eigenen Disziplin. Parnas steht bewusst für beides.

Im normalen Lauf der Wissenschaft (ich denke an Thomas Kuhn) wird behauptet, es ginge nicht, die grundsätzlichen Schranken einer Methode gleichzeitig mit den aktuellen Ausdehnungen einer Forschungsanstrengung zu denken und zu behandeln. Diese ängstliche Auffassung führt zum Zuckerguss von „Informatik und Gesellschaft“ als Kompensat im Studium. Nein, in der Wahrnehmung professioneller Expertise selbst müssen Bedenken aufkommen und aktiv verfolgt werden. *Dass* und *wie* das geht, lebt David Parnas uns seit Jahren vor. Laufend schreibt er uns dabei Seite um Seite in unsere Poesiealben hinein.

Parnas gehört zu denjenigen in der Welt, denen am klarsten vor Augen steht, dass wissenschaftliche Radikalität und ingenieurgemäße Sorgfalt zusammenkommen müssen, um komplexe Softwaresysteme höchster Qualität zu entwickeln. Auf einem Dagstuhl-Seminar zur Geschichte des Software Engineering 1996 beklagte er, dass wenige Ingenieure etwas von der Wissenschaft des Programmierens verstünden, dass andererseits aber

auch wenige Wissenschaftler ein Gespür für das hätten, was einen Ingenieur ausmache. Parnas ist angetreten, diesen beklagenswerten Zustand zu beheben.

Gewiss ist nicht unumstritten, wie weit Grundlagenforschung nicht auch um ihrer selbst willen betrieben und ausdrücklich gefördert werden müsse. Zu zahlreich sind die Beispiele sog. brotloser Elfenbein-Türmereien, die später, oft viel später, zu großen Fortschritten der auf ihre Praxis so stolzen Ingenieurkunst geführt haben. *Wofür* David Parnas steht, darüber kann und soll man gelegentlich streiten; *dass* er da aber steht, das ist zu loben.

Einem ist sie die hohe, die himmlische Göttin, dem andern eine tüchtige Kuh, die ihn mit Butter versorgt,

sagt Schiller von der Wissenschaft. Keine Frage, unser idealistischer Dichter steht auf der Seite der Göttin. Als Wissenschaftler der Ingenieurkunst muss David Parnas den Blick stärker aufs Diesseits richten. Aus strengster Anwendung harter und, wenn wir so wollen, unerbittlicher Ingenieur-Methodik heraus spricht und handelt er.

Software Engineer

David Parnas befasst sich innerhalb der Informatik mit Software-Engineering. Er gehört zu den Personen, die in der Welt am meisten zur Entwicklung und zum Niveau dieses Teilbereiches der Informatik beitragen. Er ist einer seiner Wegbereiter.

Was ist ein gutes System? Wie kann man komplexe Systeme von Software durch systematischen Entwurf sicher machen? Welche Rolle können (und müssen) dabei insbesondere mathematische Methoden spielen? So lauten Fragen, die ihn beschäftigen.

Aus den zahlreichen Beiträgen konkreter Projekte und verallgemeinernder Reflexion, die Parnas zur Beantwortung solcher Fragen geleistet hat, sind hervorzuheben das Geheimnisprinzip, das Prinzip der Modularisierung und die strenge Spezifikation von Modulen. Dabei hat er z.T. zur rechten Zeit das formuliert, was in der Luft lag.

Solche Ansätze zur Software-Konstruktion zielen stets in die Richtung

einer kontrollierten Arbeitsteilung (sprich Rationalisierung) und lokalen Verantwortlichkeit des Konstrukteurs. Ein grosses System soll so in kleinere Einheiten zerlegt werden, dass mehrere beteiligte Ingenieure sich über die Schnittstellen explizit und präzise verständigen müssen, dass sie jedoch die internen Einzelheiten in lokaler Begrenzung (und Verantwortung) konstruieren können. Das Verhalten des Gesamtsystems soll so besser und sicherer vorhersagbar werden.

Die hohen Anforderungen, die Echtzeitsysteme an die Entwicklung von Software stellen, sind ihm wichtig. Da es dabei oft um Leben und Tod geht, interessieren ihn strenge formale Methoden, nach denen hochkomplexe technische Systeme entwickelt werden sollen. Seine Erwartung ist dabei, dass nur und gerade in der Formalisierung jener Grad an Durchsichtigkeit und Verbindlichkeit erreicht werden kann, der für eine zuverlässige und vollständige Überprüfung kritischer Aspekte notwendig ist. Ein Punkt von zentraler Bedeutung ist dabei für ihn die Dokumentation. Ein typischer Fall, in dem Parnas in solchem Sinne tätig geworden war, ist der Einsatz sicherheits-kritischer Software beim Atomkraftwerk Darlington in Ontario.

Bemerkenswert und lehrreich ist das Beispiel, das Parnas uns für die gleichzeitige und gleichrangige Beachtung abstrakt-formaler und konkret-situativer Aspekte komplexer Systeme gibt.

Software Engineering als eine Profession

David Parnas blickt von seinem wissenschaftlichen Standort aus nach innen und verlangt Hohes von der Ausbildung derjenigen, die in der Entwicklung von Software generell, besonders aber der kritischer Systeme, tätig sein wollen. Aus der Bedeutung, die die Entwicklung von sicherheits-kritischer Software für die Gesellschaft besitzt, zieht er seit langem den Schluss, dass eine professionelle Zunft der Software-Ingenieure etabliert und anerkannt werden müsse. Diese müsse sich in vieler Hinsicht von den wis-

senschaftlich auszubildenden InformatikerInnen unterscheiden.

Wer also als Software-Ingenieur tätig werden wolle, müsse dafür akkreditiert werden, wie wir das von Rechtsanwälten, Architekten oder Ärzten kennen (in den USA deutlich anders als in der BRD). Er muss dafür bestimmte Kenntnisse und Fähigkeiten nachweisen, bestimmte Methoden und Vorschriften einhalten und für Fehler in seiner Tätigkeit zur Verantwortung gezogen werden können. Gerade indem er die fachlich-professionelle Kompetenz zum Ausgangspunkt einer moralischen Verpflichtung macht, gelangt Parnas zu seinen einschneidenden Vorstellungen. Sie scheinen in die aktuelle Debatte um die IT Profession langsam Einzug zu nehmen.

Software Engineering als eine gesellschaftliche Verantwortung

David Parnas blickt von seinem wissenschaftlichen Standort auch nach außen und klagt Verantwortung vor der Gesellschaft ein.

Sein Austritt 1985 aus dem kleinen, hochrangigen Beraterkreis des Präsidenten zur SDI-Entwicklung und seine damit verbundene professionelle Stellungnahme setzten ein Fanal. Diese Tat und ihre um den Globus herum reichende Wahrnehmung und Wirkung gehören zu den bemerkenswertesten Auftritten des wissenschaftlichen Gewissens in moderner Zeit. Vermutlich wäre er früher dafür auf den Scheiterhaufen gekommen. Verglichen damit hatte er es leichter als historische Vorbilder. Jedoch – wie selten hören wir Warnungen vor Falschem und Unsinnigem, wie seltener noch zieht jemand persönliche Konsequenzen!

Die kleine Geschichte jener SDI-Beraterstätigkeit ist bemerkenswert. Durch seine Teilnahme an nur zwei Tagen im Kreis der Berater bemerkte Parnas, dass das Projekt vor keine klare Aufgabe gestellt war und zu keinem praktikablen Ergebnis führen würde. Er brachte seine Bedenken im Kollegenkreis der Berater vor, die die Einwände durchaus einsahen, sie jedoch angesichts der winkenden Gel-

der in den Wind schlugen. Besser *wir* nehmen das Geld und machen mit, und die Informatik wird insgesamt sogar einflussreicher, als dass jemand anderes es täte. Klingt uns das nicht vertraut?

Erst nachdem Parnas seine Bedenken höheren Ortes bei Regierungsstellen vorgetragen hatte und nicht erhört worden war, hatte er nichts dagegen einzuwenden, dass die New York Times die Sache publik machte. Aus irgendeiner Quelle waren sie mit dem Material versorgt worden. Die Tatsache, dass die acht kurzen Essays aus seiner Feder stammten, leugnete er nicht.

Zuerst erschienen seine Warnungen im *American Scientist* im Sept./Oct. 1985. Die *Communications of the ACM* druckten die Papiere im Dezember 1985 nach und machten sie ungekürzt der wissenschaftlichen Öffentlichkeit der Informatik bekannt. 1986 erschienen dänische, japanische, hebräische, schwedische, deutsche Übersetzungen (die deutsche im *Kursbuch* 83). Vermutlich gibt es noch mehr. Im Februar 1987 hatte Parnas Gelegenheit, in einem Themenheft des *Informatik Spektrum* erneut zum Thema zu schreiben.

Die Reaktionen, Fortsetzungen, Publikationen, Vorträge und Diskussionen im weiteren Verlauf waren grandios. Parnas' Einwände trafen so recht auf das, was die damalige Friedensbewegung unmittelbar aus der Höhle des Biestes heraus brauchen konnte.

Die Bemühungen Parnas' trugen sogar zu einem leisen Abrücken Reagans von der grandiosen Ankündigung bei, dass durch das SDI Programm Atomwaffen außer Kraft gesetzt werden würden, ein Ankündigungsschachzug, der auch Parnas zunächst dafür gewonnen hatte, sich zu beteiligen. Später wurde das ganze Star Wars Konzept allmählich eingemottet – um neuerdings allerdings aus der Mottenkiste geholt und begeistert aufgegriffen zu werden, dieses Mal ohne Rekurs auf die atomare Bedrohung.

Interessant mag sein, dass Parnas im selben Jahr 1985 in den *Communications* eine Debatte um die Frage des

Umfangs der Programmiersprache Ada angezettelt hatte.

Mit David Parnas, hatte ich eingangs gesagt, ehrt das FIFF einen *Wissenschaftler des aufrechten Ganges*. Der aufrechte Gang wird aber schon verbraucht als Gattungs-Merkmal des Menschen. Es kann wohl kaum wahr sein, dass einer schon deswegen geehrt wird, dass er als Wissenschaftler auch noch Mensch sei.? Und doch!

Der aufrechte Gang

- das ungebeugte Rückgrat,
- der nicht aus Stolz, sondern Aufrichtigkeit erhobene Kopf,
- der unerschütterliche Gedanke, der sich aus der Sorge speist,
- der klare Blick in die zukünftige Ferne
- der feste Stand am aktuellen Ort
- und der Mut zum ersten Schritt und zum Durchhalten

das sind Eigenschaften, die man sich zur Erhaltung einer humanen Demokratie von mehr Menschen im Lande erhofft. Wer klarer als die Wissenschaftler und Wissenschaftlerinnen sollte diesen aufrechten Gang zur alltäglichen Übung, d.h. zur Disziplin, erhoben haben? *Sollte*, müssen wir wohl melancholisch feststellen. Denn vor Königs und anderen Thronen beugt sich dann doch so manches Knie und mancher Rücken in ungeahnter Geschmeidigkeit. In David Parnas aber haben wir einen, der den aufrechten Gang *lebt*.

Immer untersucht Parnas den vorliegenden Einzelfall auf seine kritischen Stellen hin. Er verabscheut es als Ingenieur aus Überzeugung, pauschale Urteile, also Vorurteile, zu fällen und zu propagieren, die so oft so bequem sind. Parnas entwickelt seine Konsequenzen stets aus der Betrachtung des Einzelfalles in seinen Besonderheiten.

Die Professoren werden dafür bezahlt, dass sie *Bekanntnis ablegen*. Die Gesellschaft braucht sie, damit ständig und allenthalben gedacht, erforscht, entworfen, konstruiert wird, was die Gesellschaft benötigt, was heisst, dass die Akteure der Gesellschaft es vom

Staat verlangen, ohne es selbst schaffen zu können oder zu wollen. Die Professoren sind aber ursprünglich und über diese quasi normale Anforderung hinaus diejenigen, die bekennen, was sie erkennen, die also erkennen sollen und bekennen müssen. Wenn sie es doch häufiger täten – manches sähe anders aus im Lande!

Professor David Parnas tut es. Er geht aufrechten Ganges mit hörbar erkennender Stimme durchs Land. Es täte uns gut, er ginge so noch lange, und viele folgten seinem Beispiel in alle Richtungen des Himmels.



**Verleihung des FIF-Preises 2001:
Reinhard Keil-Slawik, David Parnas, Frieder Nake
(von links nach rechts)**

Lesen *Neues für den Bücherwurm – kurz belichtet*

Joseph Weizenbaum

Computermacht und Gesellschaft. Freie Reden.

Suhrkamp Verlag, Reihe Taschenbuch Wissenschaft. Frankfurt am Main, 2001.
139 S., ISBN 3518291556, EUR 10,17

Das vorliegende Buch ist eine Sammlung von zehn Aufsätzen, die auf Vorträge aus den Jahren 1990 bis 2000 zurückgehen und von Gunna Wendt und Franz Klug herausgegeben worden sind.

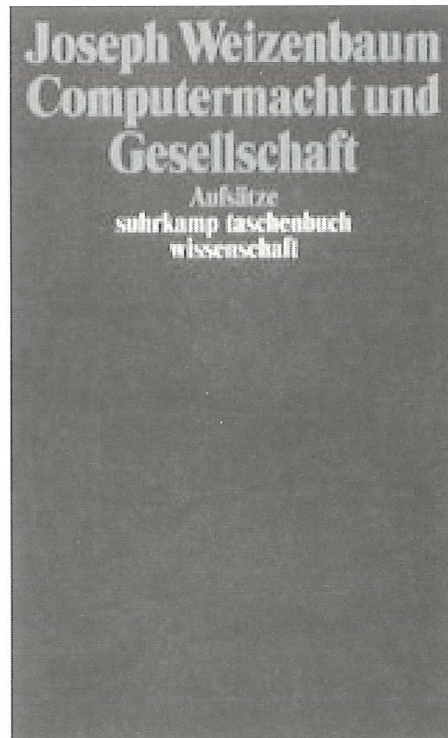
Der heutige Einsatz des Computers wird als Massenmedium aufgefasst und dieses Medium ins Verhältnis zur Ge-

sellschaft gesetzt: »Wichtig ist immer, in welches gesellschaftliche Umfeld ein Massenmedium, egal welches, eingebaut ist. [...] Jedes Instrument erbt oder erhält seinen Wert von der Gesellschaft, in die es eingebettet ist.« (S. 32). Die Inhalte dieses Buches gehören zu den beinahe klassischen Themen von Joseph

Weizenbaum. Es werden behandelt: die Bedeutung von Information, Metaphern des WWW, Mythen des Computers und der heutigen Naturwissenschaften und der dazugehörige Entwurf eines Menschenbildes – insbesondere geprägt durch Weizenbaums Erfahrungen am MIT im Umgang mit dem Gebiet der Künstlichen Intelli-

genz –, Sprache als Mittel des Lernens und Lehrens, Computer und Schule mit Bezug auf Methoden des Lehrens, die Welt unter dem Einfluss des militärischen Wahnsinns initiiert durch die Computerforschung und die Verantwortung des Wissenschaftlers und die Grenzen der Forschung.

Die Auswahl, der hier in aller Kürze referierten Aufsätze, ist geprägt von der bereits genannten zentralen Idee, dass nichts ohne die Wirkung im Umfeld – auch nicht der Einsatz des Computers – bestehen kann. Im ersten Vortrag (Berlin 2000) wird die Bedeutung von Information dargestellt. Ein elektronisches Signal ist noch keine Information. Wir verstehen ein Signal, indem wir es interpretieren. Dieses setzt voraus, dass wir in derselben Kultur sozialisiert wurden. Die Interpretation kann von Kulturkreis zu Kulturkreis unterschiedlich sein, so können wir z.B. keinem Japaner raten, da wir nicht wie er sozialisiert sind. In den Vorträgen 2, 3, 4 und 5 aus den Jahren 1990 und 1991 wird vom wissenschaftlichen Umgang mit Metaphern berichtet, die gleichzeitig ein Welt- und Menschenbild transportieren. Als initiales Beispiel ist das Teilgebiet der Informatik, die Künstliche Intelligenz. Weizenbaum reibt sich an der These von H. Moravec, dass der Mensch nur eine Menge von Informationen ist, die dauerhaft auf einem Computer gespeichert werden können. Wenn ein System veraltet, müssen die Daten nur in einen neuen Rechner übertragen werden. Der Computer als das unsterbliche Wesen. Tatsächlich streiten sich nur wenige heute, ob »der Mensch im Grunde genommen eine informationsverarbeitende Maschine ist oder« ob »Teile des lebenden Menschen künstlich oder durch Spenderorgane ersetzt werden können.« (S. 40). Die Kritik am heutigen Menschenbild wird zugespitzt auf die These: »Die Naturwissenschaft ist die heutige nachhaltige Weltreligion!« (S. 35). Im Gegensatz dazu steht die Feststellung, dass der Menschen unersetzbar ist, denn verstehen und erleben kann nur ein Mensch. Er besitzt eine »aktuelle Verbindung« zur Welt und kann Zusammenhänge semantisch deuten.



Insgesamt erleben wir Weizenbaum als streitbaren Wissenschaftler, der den Leser an seinem reichen Schatz von Lebenserfahrungen teilhaben lässt. Er kritisiert und kombiniert Beobachtungen in für manchen Leser sicherlich überraschender Weise. Auch wenn man das Buch in einem fort liest, ist es – trotz thematischer Wiederholungen in den verschiedensten Aufsätzen – unterhaltend, da wissenschaftliche Ideen, um viele Beispiele aus vergangenen Jahrzehnten angereichert sind; z.B. zeigt Weizenbaum Parallelen zwischen heutigen Entwicklungen und den Entwicklungen der 1960er und 1970er Jahren auf. Man betrachte dazu das folgende Beispiel der Einführung des Fernsehens, das »als etwas begrüßt« wurde, »das die Welt vereinigen und einen demokratischen Einfluss ausüben wird. [...] Ich bin der Auffassung, dass alles das, was das Satellitenfernsehen und die Datenübertragung möglich gemacht hat, der menschliche Erfindergeist, die Technik, die Wissenschaft und speziell die Naturwissenschaften als ein Meisterwerk der Menschheit verstanden werden können. [...] Man sollte dabei bedenken, es sind noch nicht einmal 40 Jahre vergangen, seit es den Sowjets zum ersten Mal gelang, einen Satelliten in den Weltraum zu bringen.« (S. 27 ff.). Die in beiden Fällen eingesetzte

Technik ist in vielem identisch. Solche Beispiele sind interessant, weil die Gruppe der jüngeren Leser an diesen Entwicklungen nicht teilhaben konnte.

Weizenbaums kritisches Hinterfragen von Entwicklungen in der (Computer-)Welt wirkt polarisierend, ohne den technischen Fortschritt zu verneinen. Weizenbaum fordert auf, dass wir mit unseren wissenschaftlichen Erkenntnissen sorgsam umgehen. Eine wiederkehrende Frage lautet: »Was passiert damit?« (S. 123), wenn wir ein Ergebnis erzielt haben. »Jeder einzelne muss an seine Macht glauben, und das bedeutet, man darf nicht an der Phantasie der Machtlosigkeit scheitern.« (S. 70), dieses auch wenn eine Universität, wie das MIT eng mit dem Pentagon verknüpft ist.

Das Buch eignet sich sowohl für Einsteiger auf dem Gebiet »Informatik und Gesellschaft« als auch für »alte Hasen«. Einige von uns haben viele der aufgezeigten Beobachtungen im alltäglichen Umgang mit dem Computer schon gemacht, aber vermutlich nicht in der hier dargestellten Weise kombiniert darüber reflektiert. Weizenbaum produziert Denkerlebnisse!

Rezension von Julia Stoll

Schwerpunkt

Eric Töpfer

Im Haus der 1000 Augen

Videoüberwachung in Europa

Europas Alltag wird mehr und mehr von Überwachungskameras durchdrungen. 1997 wurde das Volumen des europäischen Marktes für Videoüberwachung auf etwa 1,1 Milliarden Euro geschätzt – mit Wachstumsraten zwischen 10 und 15 Prozent (Wege 1999). Neben der Anwendung der Technik in Forschung und Produktion dominiert ihr Einsatz beim Risikomanagement: Sie soll helfen, den Verkehr zu lenken, Großunfälle zu verhindern und die Kriminalität zu bekämpfen. Was Ende der 1950er Jahren mit Kameras zur Verkehrsüberwachung begann, setzte sich in Banken, Einzelhandel und Nahverkehr fort. Heute findet sich Videoüberwachung auch in Wohngebieten, Krankenhäusern, Schulen, Universitäten, auf Fernbahnhöfen, in Flughäfen, bei Groß-Events und Shopping Malls sowie in wachsendem Maße auf öffentlichen Straßen und Plätzen. Das »Europäische Haus« ist zu einem Haus der 1000 Augen geworden.

Obwohl Videoüberwachung seit ihren Anfängen im öffentlichen Raum präsent ist, explodierte die Zahl der Kameras in vielen Ländern Europas in den 1990er Jahren, nachdem die Politik diese Technik für die Kriminalitätsbekämpfung entdeckt hatte. Die Befürworter kamen ursprünglich aus konservativen Parteien. Inzwischen setzen aber Politiker jedweder Couleur auf Videoüberwachung als »Law-and-Order«-Strategie. In Großbritannien führt »New Labour« den Kurs der Major-Regierung fort. In Frankreich setzen sich sowohl Gaullisten als auch Sozialisten für die Aufstellung von Kameras ein, und im deutschen

Nordrhein-Westfalen verabschiedete eine rot-grüne Koalition ein Polizeigesetz, das auch die Ermächtigung zur Videoüberwachung vorsieht (Berliner Zeitung, 14.4.2000). Die Kameraüberwachung des öffentlichen Raumes ist – weitgehend unabhängig von den politischen Rahmenbedingungen – zu einem gemeinsamen europäischen Trend geworden.

Allerdings variieren die rechtlichen Rahmenbedingungen. Während in Großbritannien die Deregulierung des Planungsprozesses zur Verbreitung der Technik beitrug, ebnete in Deutschland die Novellierung der Polizeigesetze den Weg. In Frankreich ist die Registrierung von Systemen im öffentlich zugänglichen Raum Pflicht, während in Spanien nur behördliche Anlagen erfasst werden und in Großbritannien überhaupt keine Vorschriften diesbezüglich bestehen. In manchen Ländern ist das Betreiben privater Anlagen genau geregelt, während in anderen Ländern eher öffentliche Anlagen reguliert sind.

Die Überwachung des öffentlichen Raumes in ausgewählten Ländern

Vorreiter der Videoüberwachung des öffentlichen Raumes ist bekanntermaßen **Großbritannien**. Norris und Armstrong nennen die Briten »the most surveilled population in the world« (1999: 39). Seit 1985 das erste Pilotprojekt im Seebad Bournemouth anlief, breitet sich die Überwachung des öffentlichen Raumes mit exponentiellen Wachstumsraten aus. Im Oktober 1994 kündigte die Zentralregie-

rung die erste Finanzspritze zur Förderung von Closed Circuit Television (CCTV), so der englische Begriff, an (Norris/Armstrong 1999: 35). Bis März 2002 wird die Regierung voraussichtlich mehr als 300 Millionen Euro zur Finanzierung solcher Projekte ausgegeben haben. 1998 existierten bereits 440 innerstädtische CCTV-Netzwerke, und heute betreibt fast jede Stadt mit mehr als 500.000 Einwohnern ein solches (Coleman/Norris 2000: 150). Angesichts des Wachstums der Videoüberwachung in Großbritannien weist Graham (1998) auf die Ähnlichkeiten des gegenwärtigen Prozesses mit der Entwicklung heute selbstverständlicher städtischer Infrastrukturen wie Gas, Strom, Wasser und Telekommunikation in den Städten des 19. Jh. hin und sagt voraus, dass CCTV im Verlauf der nächsten 20 Jahre in Großbritannien zur fünften Säule städtischer Infrastruktur werden wird. Dieser Vermutung folgend sehen Norris und Armstrong (1999) mit der Integration der Systeme und der wachsenden Bedeutung automatisierter algorithmischer Überwachung die Architektur für eine »maximum surveillance society« heraufziehen. Obwohl Kritiker darauf hinweisen, dass die Ausbreitung der Videoüberwachung ohne große rechtliche Hürden erfolgte (Maguire 1998), halten Befürworter den Schutz der Menschenrechte für ausreichend und verweisen auf das neue Datenschutzgesetz (z.B. Henderson 2001). Ungeachtet dessen breitet sich die Überwachung weiterhin aus: Im August 2001 kündigte die Blair-Regierung einen neuen Geldregen in Höhe

von 125 Millionen Euro für weitere 250 Projekte an (BBC News, 21.8.2001).

Spitzenreiter auf dem Festland ist **Monaco**, das sein knapp zwei Quadratkilometer großes Territorium durch ein integriertes System von 60 modernen Kameras überwachen lässt, die sowohl Innenräume als auch Außenbereiche übersehen (Vitalis 1998, Nogala 1998: 110).

Frankreich begann mit der Videoüberwachung öffentlicher Räume 1994 in dem Pariser Vorort Levallois-Perret (Nogala 1998: 111). Im Januar 1995 verabschiedete das französische Parlament ein umstrittenes Sicherheitsgesetz, das unter anderem den Einsatz von Videokameras zum Schutz öffentlicher Gebäude und in Gebieten mit einem hohen Risiko von Eigentums- und Körperdelikten erlaubt (Vitalis 1998). Das Gesetz wurde in Reaktion auf eine Welle gewalttätiger sozialer Protesten im Frühjahr 1994 eingebracht (Tageszeitung, 8.10.1994). Seitdem müssen Systeme zur Videoüberwachung von den Präfekten der Départements nach der Beratung durch eine lokale Behörde genehmigt werden. Zwischen 1997 und 1999 haben 201 Städte die Genehmigung zur Aufstellung von Anlagen in »Hochrisikogebieten« bekommen, und 259 Gemeinden erhielten grünes Licht für die Sicherung öffentlicher Gebäude (Ocqueteau 2001).

In **Spanien** trat im August 1997 ein Gesetz zur polizeilichen Videoüberwachung in Kraft, über die seitdem die örtlichen Büros des Innenministeriums entscheiden. Dabei stützen sie sich auf Berichte einer Kommission, der ein Richter des obersten Gerichts der jeweiligen Region vorsitzt (Statewatch Bulletin, 7-10/1997, Vol.7, No.4-5). Hintergrund des Gesetzes waren Bemühungen, die Organisatoren von Demonstrationen für eventuell entstandene Schäden haftbar zu machen (Statewatch Bulletin, 9-10/1996, Vol.6, No.5). Damit legitimierte das Gesetz nachträglich Maßnahmen in baskischen Städten, wo Kameras aufgestellt worden waren, um Straßengewalt von ETA-Sympathisanten zu bekämpfen. Daneben findet sich Videoüberwachung in Spanien inzwischen aber auch in anderen Kontexten: Im September 2001 erhielt z.B. die Stadtver-

waltung von La Laguna auf Teneriffa die Genehmigung zur Videoüberwachung ihres Vergnügungsviertels (Canarias24.com, 30.9.2001).

Aus **Belgien** wurde bereits 1998 berichtet, dass es dem Trend in Frankreich folge. Umstritten war damals allerdings noch, ob die Überwachung des öffentlichen Raums rechtskonform sei (Nogala 1998: 111). In den **Niederlanden** reagierten in jüngster Zeit einige Kommunen mit der Aufstellung von Kameras auf steigende Kriminalitätsraten in Vergnügungsvierteln. Anfang 2001 unterhielten zwischen 20 bis 30 Gemeinden solche Projekte (Offens 2001).

In **Finnland** ist die Überwachung des öffentlichen Raums »de facto« unreguliert, so dass dieser sowohl von Kameras öffentlicher wie privater Akteure in den Blick genommen wird (Koskela 2000). **Schweden** verabschiedete 1998 ein Gesetz, das den Einsatz von Überwachungskameras im öffentlichen Raum regelt. Drei Jahre später schätzte Hårdh (2001), dass landesweit mindestens 30.000 Kameras öffentliche Orte überwachen. In Norwegens Hauptstadt Oslo startete die Polizei 1999 ein Pilotprojekt rund um den Hauptbahnhof. Obwohl das Projekt von den lokalen Geschäftsleuten widersprüchlich beurteilt wurde, nannte es die Polizei einen Erfolg, der es wert sei, ausgedehnt zu werden (Aftenposten, 18.9.2000 und 15.8.2001). In **Dänemark**, wo Videoüberwachung seit 1982 gesetzlich geregelt wird, ist zwar die Überwachung des öffentlichen Raumes durch Private verboten, aber die Polizei kann sogar ohne Information der Öffentlichkeit überwachen (Dänisches Gesetz über das Verbot von Videoüberwachung).

In **Deutschland** wurde das erste Pilotprojekt 1996 in Leipzig gestartet. Im Mai 2000 erklärte die Ständige Konferenz der Innenminister, dass sie »in dem offenen Einsatz von Videoüberwachungsmaßnahmen an Kriminalitätsbrennpunkten im öffentlichen Raum ein geeignetes Mittel« zur Wahrnehmung polizeilicher Aufgaben sehe (Ständige Konferenz der Innenminister 2000: 27). Gleichwohl wiesen einen Monat später Experten bei einer Anhörung im Innenausschuss des

Bundestages übereinstimmend darauf hin, dass Videoüberwachung einen Eingriff in die Privatsphäre darstelle und daher der rechtlichen Grundlage bedürfe (Frankfurter Rundschau, 6.7.2000). Ende 2001 haben alle Bundesländer mit Ausnahme Berlins ihre Polizei- bzw. Ordnungsgesetze entsprechend angepasst. Gegenwärtig existieren nur etwa ein Dutzend Systeme polizeilicher Videoüberwachung, aber der Zentralverband der deutschen Elektroindustrie (ZVEI) schätzt, dass etwa 200 Städte ähnliche Projekte planen (ZVEI 2001).

Videoüberwachung und europäisches Recht

Neben technischer Standardisierung, Marktinterventionen durch Forschungsförderung oder die Finanzierung von Anlagen zur Videoüberwachung mit Strukturfondsgeldern prägt die europäische Ebene Videoüberwachung durch die Setzung eines rechtlichen Rahmens. Vier europäische Rechtsnormen haben nach Weichert (2000) und Buttarelli (2000) Einfluss auf ihre Ausgestaltung – zwei internationale Verträge zwischen den 43 Mitgliedsstaaten des Europarates und zwei supranationale Rechtstexte der EU:

Die **Europäische Menschenrechtskonvention** des Europarates von 1950 garantiert mit Art. 8 das Recht auf die Respektierung der Privatsphäre, das damit de jure in letzter Instanz vor dem Europäischen Gerichtshof für Menschenrechte einklagbar ist. Nach Art. 8, Abs. 2 bedarf jeder Eingriff von Behörden in das Privatleben einer gesetzlichen Grundlage und konkreten Rechtfertigung, die im Schutz der nationalen, öffentlichen oder ökonomischen Sicherheit oder der Bekämpfung von Aufruhr und Kriminalität bestehen kann. Hinsichtlich der behördlichen Videoüberwachung des öffentlichen Raumes ist umstritten, ob dieser einer gesetzlichen Grundlage in Übereinstimmung mit Art. 8 bedarf oder nicht. Erst eine Entscheidung des Europäischen Gerichtshof für Menschenrechte würde wohl eine Klärung dieser umstrittenen Frage bringen.

Die **Europäische Konvention über die automatische Verarbeitung von personenbezogenen Daten des Europarates** von 1981 präzisiert die Vorgaben der Menschenrechtskonvention und reguliert – in der Regel – the »processing of any personal data relating to natural persons that have been collected in connection with surveillance activities« (Buttarelli 2000), wie es teilweise für Videoüberwachung zutrifft. Allerdings kann nach Art. 3 der Konvention jeder Unterzeichnerstaat den Ausschluss bestimmter Datenkategorien (z.B. in Verbindung mit nationaler Sicherheit) von der Anwendung der Konvention erklären. Damit regelt die Konvention weder das reine Filmen durch Videokameras noch die Aufzeichnung der Bilddaten, und selbst wenn Bilddaten weiterverarbeitet werden, liegt es im Ermessen der Staaten, ob diese Operationen unter die Anwendung der Konvention fallen. Wenn aber ein Land die Anwendung der Konvention auf die Verarbeitung von durch Videoüberwachung gewonnenen Bilddaten zulässt, wird diese durch die Art. 5 (Qualität der Daten), Art. 7 (Datensicherheit), Art. 8 (Recht auf Auskunft), Art. 10 (Sanktionen) und Art. 12 (Grenzüberschreitender Datenverkehr) geregelt (Buttarelli 2000).

Die **Datenschutzrichtlinie (95/46/EC)** der EU von 1995, die 1998 in Kraft trat, bindet alle 15 Mitgliedsstaaten der Union. Nach Art. 3 ist die Richtlinie anzuwenden auf personenbezogene Daten, die in einer »Datei« gespeichert sind – mit Ausnahme einer Weiterverarbeitung zum Zweck nationaler Sicherheit und den Aktivitäten im Bereich des Strafrechts. Art. 2 definiert eine »Datei« als »jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind«. D.h. dass die Richtlinie grundsätzlich nicht angewendet werden kann auf alle Formen polizeilicher Videoüberwachung sowie einfache Kamera-Monitor-Systeme ohne Datenspeicherung bzw. mit analoger Datenspeicherung ohne die Möglichkeit weiterer Auswertung. Sie kann aber angewendet werden auf alle nichtpolizeilichen digitalen Systeme, die mindestens die Möglichkeit der Zwischenspeicherung

bieten (Weichert 2000). Für diese Systeme regelt Art. 10 (Recht auf Information), dass betroffene Personen über die Identität der für die Datenverarbeitung Verantwortlichen ebenso aufgeklärt werden müssen wie über den Zweck, die Adressaten der Datenweitergabe und ihre Rechte. Weiterhin garantiert Art. 12 (Recht auf Auskunft), dass Betroffene über die Speicherung der Daten und den »logischen Aufbau der automatisierten Verarbeitung« informiert werden müssen und das Recht haben, die Löschung, Korrektur oder Nichtweitergabe zu verlangen. Während diese Vorschriften zur Transparenz der Nutzung entsprechender Systeme beiträgt, steht die Anwendung von Art. 14 (Recht auf Widerspruch) vor erheblichen praktischen Problemen, wenn die Videoüberwachung – so wie es häufig der Fall ist – automatisch geschieht. Art. 15 (Automatisierte Einzelentscheidungen) ist relevant für Systeme, die Methoden der biometrischen Datenverarbeitung anwenden, denn es ist untersagt, Personen einer »sie erheblich beeinträchtigenden Entscheidung« zu unterwerfen, »die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht«. Art. 20 (Vorabkontrolle) und 21 (Öffentlichkeit der Verarbeitungen) finden schließlich Anwendung, wenn die Datenverarbeitung spezifische Risiken für die Rechte und Freiheiten von Personen darstellen könnte. Solche Methoden bedürfen der Vorabprüfung, und es müssen die Identität der für die Verarbeitung Verantwortlichen, der Zweck der Verarbeitung, die angewandten Kategorien, Empfänger der Daten und die Maßnahmen zur Garantie der Datensicherheit öffentlich gemacht werden.

Die **Charta der Grundrechte** der EU von 2000 proklamiert in Art. 8 den Schutz personenbezogener Daten auf Grundlage o.g. Rechtsnormen. Der von der Charta garantierte Datenschutz kann allerdings unter Hinweis auf Art. 52 und durch eine entsprechende gesetzliche Grundlage eingeschränkt werden. Gegenwärtig ist die Charta nicht bindend für die EU-Mitgliedsstaaten, sondern stellt eine reine

Selbstverpflichtung des Europäischen Rates, der Kommission und des Parlamentes dar. So gilt sie nur für die Organe der EU, für die Mitgliedstaaten jedoch allein bei der Anwendung von Gemeinschaftsrecht. Ob und wie die Charta Videoüberwachung tangiert, wird erst die Zukunft zeigen.

Die europäische Diskussion

In jüngerer Zeit haben europäische Parlamentarier begonnen, Videoüberwachung zu thematisieren. »Wenn Menschen auf Reisen von Videokameras in ihren Gastländern gefilmt werden, werden sie in ihren Grundrechten verletzt.« erklärte Jo Leinen, sozialdemokratischer Abgeordneter des Europäischen Parlaments. Konsequenterweise forderte er, Videoüberwachung zum »Topthema« zu machen und kritisierte, dass sie nicht auf der Tagesordnung gestanden habe, als die Charta für Grundrechte diskutiert wurde (Frankfurter Rundschau, 26.1.2001).

Es war aber das Büro für Technikfolgenabschätzung (STOA) des Parlaments, das einen Bericht über »Technologies of Political Control« (Wright 1998) in Auftrag gab. Die Studie berichtet u.a. über neuere Entwicklungen der Überwachungstechnologien. Dabei hebt sie den dramatischen Wandel der visuellen Überwachung durch die wachsenden Kapazitäten zur Speicherung und Verarbeitung von Bilddaten hervor und sagt voraus, dass »the revolution in urban surveillance will reach the next generation of control once reliable face recognition comes in« (Wright 1998: 17). Daher empfiehlt sie:

1. Systeme zur Videoüberwachung in der EU allgemeinen und einheitlichen Regeln eines »Codes of Practice« zu unterwerfen, um eine regelmäßige Prüfung ihrer Nutzung zu gewährleisten und angemessene Beschwerdemöglichkeiten zu garantieren;
2. klar definierte Kriterien aufzustellen, wer videoüberwacht werden soll und wie die dabei gewonnenen Daten gespeichert, weiterverarbeitet und weitergegeben werden;

3. neue Überwachungstechnologien mit der entsprechenden Datenschutzgesetzgebung, insbesondere mit Artikel 15 der EU-Datenschutzrichtlinie, in Einklang zu bringen;
4. angesichts der problemlosen Manipulierbarkeit von digitalen Bilddaten neue Regeln aufzustellen, unter welchen Umständen sie als gerichtsverwertbare Beweismittel zugelassen werden;
5. Vereinbarungen, die den Gebrauch von elektronischen Aufzeichnungsgeräten durch Privatpersonen und Firmen regeln.

Obwohl Abgeordnete des Europäischen Parlaments ankündigten, dass Thema zur Sprache bringen zu wollen (Frankfurter Rundschau, 26.1.2001), waren es Parlamentarier beim Europarat, die zuerst in Aktion traten. Im März 2001 brachte eine überparteiliche Gruppe von zehn Abgeordneten aus fünf Ländern eine Initiative in der Parlamentarischen Versammlung des Rates auf den Weg. Mit ihrer »Motion for a Recommendation on Video Surveillance of Public Areas« fordern sie die Versammlung dazu auf, dem Ministerrat zu empfehlen, den Staatenbund dazu aufzurufen, mit der Folgeabschätzung von Videoüberwachung zu beginnen, rechtliche Vorkehrungen gegen ihre unkontrollierte Ausbreitung zu schaffen, ihren demokratischen Einsatz zu garantieren und klarzustellen, wie gesammelte Bilddaten aufgezeichnet, gespeichert und gebraucht werden dürfen (Behrendt u.a. 2001). Eine Entscheidung der Versammlung steht aus.

Bereits Ende 2000 hatte der Europarat einen Bericht zum Thema (Video)Überwachung (Buttarelli 2000) veröffentlicht, der auf die Gefahr hinweist, »that modern societies may inadvertently tend to replace or supplement control with the incitement to self-control and the repression of impulses«. Obwohl er die Bedeutung der Europäischen Konvention über die automatische Weiterverarbeitung von personenbezogenen Daten hervorhebt, kommt er daher zu dem Schluss: »Twenty years after the adoption [...] what really matters is for the Council of Europe to let its authoritative voice be heard once again.«

Es wäre nicht das erste Mal, dass eine Initiative des Europarates Diskussionen und Gesetzgebung auf nationaler Ebene anregt. So bestünde die vage Chance, die kritischen Grauzonen privater, analoger Videoüberwachung einzuhegen und ihre Instrumentalisierung zur sozialen Ausgrenzung zu thematisieren. Kaum zu erwarten ist aber, dass der Staatenbund das hoheitliche Handeln seiner Mitglieder reglementieren wird. Eine sinnvolle Begrenzung und kritische Kontrolle polizeilicher Videoüberwachung wird nur auf nationaler Ebene zu erreichen sein – ebenso wie eine Stärkung der Datenschützer, die angesichts der wachsenden Zahl von Überwachungskameras allein auf diesem Feld kaum mehr in der Lage sind, ihren Aufsichtsaufgaben nachzukommen. Ein europaweiter Austausch über Praktiken und Erfahrungen im Umgang mit Videoüberwachung könnte eine Hilfestellung bei diesen bieten.

Literatur

- Behrendt, W. u.a. (2001): Motion for a recommendation on video surveillance of public areas, Parliamentary Assembly of the Council of Europe, Doc.9008, 26.3.2001: <http://stars.coe.fr/doc/doc01/edoc9008.htm>
- Buttarelli, G. (2000): Protection of personal data with regard to surveillance. Report for the Project Group in Data Protection of the Council of Europe: <http://www.legal.coe.int/dataprotection/Default.asp?fd=reports&fn=RapButtarelliE.htm>
- Coleman, C. / Norris, C. (2000): Introducing criminology, Cullompton/Devon
- Dänisches Gesetz über das Verbot der Videoüberwachung, unauthorisierte deutsche Übersetzung des Unabhängigen Zentrums für Datenschutz Schleswig-Holstein: <http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/video/videogdk.htm>
- Graham, S. (1998): Towards the fifth utility? On the extension and normalisation of CCTV, in: Surveillance, closed circuit television and social control, hg. von C. Norris, J. Moran und G. Armstrong, Ashgate, S.89-112
- Hårdh, R. (2001): Country report on CCTV in Sweden, presentation at the conference »Video surveillance. A crime prevention instrument in European comparison« in Göttingen, 22.-24.2.2001
- Henderson, R. (2001): Country report on CCTV in Great Britain, presentation at the conference »Video surveillance. A crime prevention instrument in European comparison«, a.a.O.
- Koskela, H. (2000): »Safe to be afraid ...« Eine skandinavische Studie zur Videoüberwachung von Frauen, Interview von Volker Eick, in: Mieter Echo, Nr.278, März/April 2000
- Maguire, M. (1998): Restraining big brother? The regulation of surveillance in England and Wales, in: Surveillance, closed circuit television and social control, a.a.O., S.229-240
- Nogala, D. (1998): Social Control Technologies. Verwendungsgrammatiken, Systematisierung und Problemfelder technisierter sozialer Kontrollarrangements, Dissertation, Freie Universität Berlin
- Norris, C. / Armstrong, G. (1999): The maximum surveillance society. The rise of CCTV, Oxford
- Ocqueteau, F. (2001): Video surveillance in France. Regulation and impact in crime, presentation at the conference: »Video surveillance. A crime prevention instrument in European comparison«, a.a.O.
- Offens, H. A. (2001): Country report on CCTV in the Netherlands, presentation at the conference: »Video surveillance. A crime prevention instrument in European comparison«, a.a.O.
- Ständige Konferenz der Innenminister (2000): Zur Veröffentlichung freigegebene Beschlüsse der 161. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder am 5. Mai 2000 in Düsseldorf, Bonn
- Vitalis, A. (1998): Der öffentliche Raum im Fadenkreuz der Kameras, in: Le Monde diplomatique, 13.3.1998, S.22-23
- Weichert, T. (2000): Current legal issues on video surveillance, Contribution to the SECURITY Congress 2000, Oct. 9-12, 2000, Essen: http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/video/vidsec_e.htm
- Wege, A. (1999): Geschäft mit der Sicherheit. Videoüberwachung, in: rfe. Technik und Markt der CE-Branche, Nr.1-4/1999: http://www.rfe-online.de/_archiv/01/03/vw1.htm
- Wright, S. (1998): An appraisal of technologies of political control (consultation version), Working Document PE 166 499, STOA programme of the European Parliament, Luxemburg
- ZVEI (2001a): Pressemitteilung 37/2001: <http://www.zvei.de/news/Presseinformationen/2001-05/Pr037-2001.html>

Hubert Beste

Das Beispiel Videoüberwachung – eine neue Kultur der Kontrolle?

Um was es geht

Videoüberwachung ist auch hierzulande kein neues Phänomen, sondern kann auf eine mehr als dreißigjährige Geschichte zurückblicken. Das gilt für die Überwachung von Kundenräumen der Banken, von Kaufhäusern oder Einkaufszentren, von öffentlichen Gebäuden (z.B. Gerichte, Polizeipräsidien, Botschaften, Konsulate), Tankstellen und Parkhäusern oder von Flughäfen, Bahnhöfen, U- und S-Bahn-Stationen. Mit der starken Verbreitung der Geldautomaten in den späten 80er und frühen 90er Jahren wurde die Videoüberwachung zum selbstverständlichen Bestandteil der Organisation und Regelung des Kundenverkehrs. Darüber hinaus wird diese Kontrollform natürlich seit ihrer praktischen Handhabung als polizeiliche und geheimdienstliche Ermittlungsmethode eingesetzt. Zur Sicherung von Privathäusern, Produktionsabläufen oder Dienstleistungsbereichen wird in immer stärkerem Maße auf Videoüberwachung zurückgegriffen. Man kann heute ohne Umschweife behaupten, dass diese Methode in der fortgeschrittenen kapitalistischen Welt – und nicht nur dort – zu einem selbstverständlichen Sicherheits-, Sicherungs-, Kontroll- und Überwachungsinstrument avanciert ist. Sie wird daher auch nicht (mehr) in Frage gestellt, sondern als für wirksam und nützlich gehaltenes Optimierungsmittel eingesetzt. Was Videoüberwachung tatsächlich leistet oder leisten kann, und an welche Voraussetzungen und Bedingungen solche Leistungen geknüpft sind, ist allerdings eine andere Frage. Im vorliegenden Kontext steht jedoch eine spezifische Variante der Videoüberwachung zur Diskussion. Dabei geht es um die (polizeiliche) Überwachung

öffentlicher Räume (z.B. Fußgängerzonen, Parkanlagen, Marktplätze) zum primären Zweck der Kriminalprävention, aber auch zur Effizienzsteigerung repressiver Verbrechensbekämpfung. Eine Stärkung des allgemeinen Sicherheitsgefühls innerhalb der Bevölkerung steht daneben im Mittelpunkt der Bemühungen. Nicht zu unterschätzen sind auch die symbolischen Effekte. Die Videoüberwachung bietet für die politische und polizeiliche Seite überdies die Möglichkeit, ohne großen Aufwand öffentlich zu demonstrieren, dass die erforderlichen Sicherheitsmaßnahmen getroffen werden und die Sicherheit des Bürgers im Zentrum staatlicher Ordnungsaktivitäten steht.

Während diese Form der Videoüberwachung in Großbritannien (CCTV: Closed Circuit TeleVision) bereits seit den 90er Jahren flächendeckend praktiziert wird, sind diesbezügliche umfassende Aktivitäten einschließlich ihrer öffentlichen Diskussion in Deutschland erst in jüngster Vergangenheit aufgekommen. Entsprechend dürftig sind allgemeiner Informationsstand und einschlägige Datenlage. Es herrschen pauschale Pressemeldungen und polizeiliche Lagebeurteilungen vor, die in den weitaus meisten Fällen bei der kriminalpräventiven Wirksamkeit ansetzen (Rückgang der registrierten Kriminalität in den überwachten Zonen) und überdies ein verstärktes Sicherheitsgefühl der Bevölkerung in Rechnung stellen. Insofern sind sozialwissenschaftlich informierte Befunde, die sich auf die bundesdeutsche Situation erstrecken, bisher noch absolute Mangelware. Über die tatsächliche Wirksamkeit der Videoüberwachung, ihre Neben-, Begleit- und Folgeeffekte existieren derzeit nur sehr unzureichende und ungesicherte Befunde. Das

bezieht sich auch auf kriminalgeographische Ortseffekte: Lassen sich etwa kriminalpräventive Effekte für einen überwachten Raum in München nachweisen, muss dies nicht zwangsläufig für einen vergleichbaren Raum in Hamburg gelten. Für jede Großstadt läßt sich eine unverwechselbare Kriminalitätsmorphologie entwerfen, die nur für diesen urbanen Raum typisch ist und sich daher nicht ohne weiteres verallgemeinern läßt. Videoüberwachung greift aber in diese Morphologie ein und verändert sie dabei. Die Effekte können jedoch höchst unterschiedlich ausfallen, so wie etwa die Wirkungen eines bestimmten Medikaments, das verschiedenen Personen verabreicht wird. Zudem ergibt sich die Schwierigkeit der Messung von Vorher-Nachher-Effekten, die regelmäßig nicht hinreichend beachtet werden dürfte, wenn ausschließlich jene Räume untersucht werden, in denen bereits Kameras installiert sind. Es stellen sich also eine Reihe von Forschungsproblemen ein, die grundlegender Bearbeitung bedürfen. Um die soziale Bedeutung der Videoüberwachung abschätzen zu können, sollte sie zudem im Gesamtzusammenhang des Einsatzes avancierter Kontrolltechnologien (z.B. DNA-Analyse, elektronische Fußfessel, biometrische Kontrollverfahren, automatisierte Fingerabdruckidentifizierungssysteme) als Form eines »technical fix« betrachtet werden (Nogala 1998).

CCTV in Großbritannien

Der Alltag in den britischen Großstädten ist bereits heute durch flächendeckende Videoüberwachung gekennzeichnet, deren Ausweitung im Zuge Tony Blairs Machtübernahme sowie der »New Labour«-Strategie nochmals forciert wurde. Was die Effektivität

von CCTV betrifft, so fallen die Befunde nicht eindeutig aus. Einerseits wurden Verdrängungs- und Verlagerungseffekte gefunden, andererseits zeigte sich partiell aber auch ein deutlicher Rückgang der registrierten Kriminalität in den überwachten Räumen. Insgesamt ist davon auszugehen, dass Videoüberwachung zwar kriminalpräventive Effekte freisetzt, dass diese aber mit erheblichen Mehrbelastungen angrenzender, nicht-überwachter Räume erkauft werden, zumal Gewaltdelikte von dieser unmittelbaren Beeinflussung tendenziell am geringsten betroffen sind. Viel stärker schlägt indessen der Diskriminierungseffekt durch, da die Selektivität polizeilicher Intervention hinsichtlich bestimmter Verdachtsgruppen (besonders junge, farbige, männliche Migranten) durch CCTV noch verstärkt wird (Norris/Armstrong 1998).

Eine aktuellere Längsschnittstudie, die die öffentliche Einstellung gegenüber CCTV in Glasgow untersuchte, kommt denn auch zu differenzierteren Ergebnissen. Was gemeinhin als »Kriminalitätsfurcht« bezeichnet wird, konnte auch durch die Installation von Videokameras nicht merklich reduziert werden. Auf der anderen Seite fühlen sich etwa zwei Drittel der Befragten durch die Videoaufzeichnungen in ihren Rechten nicht verletzt. Die Zustimmungsraten steigen mit wachsendem Alter und sind bei Frauen deutlich höher als bei Männern. Auch die antizipierte Effizienz der Videoüberwachung wurde im Vergleich mit der klassischen Polizeipräsenz unterschiedlich gewertet. Während die Polizeipräsenz bei der Stärkung des Sicherheitsgefühls deutlich und bei der Erhöhung der Kriminalprävention leicht überwiegt, dominiert CCTV klar im Bereich der Kriminalitätsentdeckung. Es stellt sich in diesem Zusammenhang ganz allgemein die Frage, ob eine deutliche Senkung der Kriminalitätsfurcht überhaupt wünschenswert ist. Denn »normale Kriminalitätsfurcht« kann durchaus als funktionales oder kreatives Element städtischer Lebenskultur betrachtet werden. Warum sollte CCTV die Antwort auf die multiplen Stadtprobleme sein, die selbst durch die kontrolltechnische Aufrüstung der

Polizei in den vergangenen siebzig Jahren nicht gefunden wurde. Gerade weil CCTV als elektronisches Überwachungsauge fungiert, besteht die Gefahr, dass die spontane, natürliche Überwachung, die auf dem gegenseitig organisierten Kontrollverhalten der Individuen beruht, ausgehöhlt wird. Die Kontrollfunktion wird einem elektronischen Auge zugeschoben, das die Städter von ihrer sozialen Verantwortung entfremdet und im übrigen keineswegs eine Verminderung der registrierten Kriminalität erbringen muß (Ditton 2000).

Auch wenn die Vereinigten Staaten in vielerlei Hinsicht als »Testfeld« neuer Formen der Sozialkontrolle und neuer Kontrolltechnologien gelten, gibt es weltweit keinen Staat, der hinsichtlich der geschlossenen Videoüberwachung öffentlicher Räume mit Großbritannien Schritt halten könnte. Es bietet sich insoweit an, erstens die ausdrücklichen wie die symbolischen Funktionen von CCTV zu betrachten, zweitens die möglichen nicht-intendierten Konsequenzen zu bedenken und drittens die ökonomische Rationalität zu berücksichtigen. Denn die Videoüberwachung öffentlicher Räume gehorcht anderen Regelmäßigkeiten als etwa die entsprechende Überwachung polizeilicher Gewahrsamszellen oder halböffentlicher Räume wie Krankenhäuser oder Schulen. Öffentliche Befriedung wird primär nicht durch die Polizei hergestellt, so notwendig sie auch sein mag. Sie wird hergestellt durch ein weitgehend unbewußtes Netzwerk von Triebkontrollen und Verhaltensstandards, das innerhalb dieser Öffentlichkeit besteht. Keine Macht der Polizei könnte jene Zivilisierungsformen wieder aufbauen, die in ihrer angestammten Struktur zusammengebrochen sind. Außerdem sollte die Einführung der Videoüberwachung dazu dienen, das Image der Innenstädte zu verbessern, ihre Ausstrahlungskraft zu erhöhen, indem mißliebige soziale Gruppen oder politische Versammlungen einer verschärften öffentlichen Kontrolle zugeführt wurden. Hier greifen also unterschiedliche soziale, politisch-strategische, ökonomische und polizeiliche Zweckbestimmungen ineinander, die den rasanten Ausbau

von CCTV in Großbritannien befördert haben.

Im Verhältnis von CCTV und der Steuerung polizeilicher Kontrollarbeit eröffnet sich eine weitere Perspektive, die bisher kaum bedacht wurde. Wenn es richtig ist, dass sich die Spätmoderne durch die Trennung von Raum und Zeit auszeichnet, könnte sich durch CCTV die Möglichkeit ergeben, diese Separierung wieder aufzuheben und positiv zu wenden. Die panoptische Vision, die beim Kontrollunterworfenen einen Zustand permanenter Sichtbarkeit erzeugt, könnte allerdings auch in der Weise »umgedreht« werden, dass die Kontrolleure selbst (möglicherweise auch zufällig) ins Fadenkreuz des allgegenwärtigen Kontrollmediums geraten (Newburn/Hayman 2002, S. 155-167; Legnaro 2000, S. 204).

Entwicklungstendenzen der Videoüberwachung

Angeichts der gegenwärtigen Beschreibung der sicherheitspolitischen Lage in den fortgeschrittenen kapitalistischen Staaten, die insbesondere auch in Deutschland konturenscharf ausfällt, ist zu erwarten, dass die Bedeutung der Videoüberwachung innerhalb der neuen Politik innerer Sicherheit noch erheblich zunehmen wird. Denn die kontrolltechnische Aufrüstung der Sicherheitssysteme bietet einige Vorteile, die kaum von der Hand zu weisen sind: (1.) Sie stößt auf eine hohe allgemeine Zustimmung, die u.a. mit der Dominanz instrumenteller Vernunft zusammenhängt. (2.) Sie strahlt eine hohe Symbolkraft aus, die die technische Regulierung komplexer sozialer Probleme suggeriert. (3.) Sie vermittelt den Eindruck einer äußerst hohen Effizienz, der etwa durch die jüngsten Fahndungserfolge bei der Ermittlung von Sexualstraf Tätern (DNA-Analyse) unterstützt wird. (4.) Sie entspricht auf geradezu perfekte Weise dem Bild einer Sicherheitsgesellschaft, in der »Sicherheit« als zentrales Dispositiv verhandelt wird. (5.) Schließlich verdrängt ihre vermeintliche Nützlichkeit und Wirksamkeit jene Bedenken, die sich auf mögliche soziale Folgeschäden richten. Gegen die kontrollpoliti-

sche Rationalität, die dem Einsatz der Videoüberwachung innewohnt, läßt sich aus der Perspektive kritischer Kontrollforschung nur dann etwas entgegensetzen, wenn genau dieser Ratio-Charakter befragt wird. Denn die Installation von Videokameras ist lediglich das erste Glied in einer ganzen Kette von Entscheidungen und Maßnahmen, um die wirksame Anwendung sicherzustellen. Dabei ist vor allem nach der zugrundeliegenden Idee von sozialer Ordnung zu fragen, die mit dem Einsatz dieser Kontrolltechnik verbunden ist. Der Verweis auf ein formelhaftes »im Angesicht der Prävention« dürfte kaum hinreichend sein.

Die Einstellung gegenüber der Videoüberwachung in Deutschland wurde im Rahmen einer Vergleichsstudie bezüglich der Städte Dresden und Düsseldorf untersucht (Reuband 2001). Obwohl eine Videoüberwachung öffentlicher Straßen und Plätze in Düsseldorf nicht existiert, bejahten dies 43% der Befragten. Die Zustimmung zur Überwachungsform liegt in beiden Städten hoch: in Düsseldorf bei 66%, in Dresden gar bei 77%, wobei die Mißbrauchsgefahr eher niedrig eingestuft wird. Die Akzeptanz der Videoüberwachung wird vor allem durch Fremdenfurcht sowie das Vertrauen in die kontrollpolitische Arbeit bestimmt. Kriminalitätsfurcht spielt nicht die dominierende Rolle. Insgesamt kann davon ausgegangen werden, dass die Videoüberwachung auch hierzulande auf breite Zustimmung stößt, die in Ostdeutschland allerdings noch stärker ausgeprägt ist. Die symbolischen Effekte »irrtümlich angenommener Videoüberwachung« sollten dabei nicht unberücksichtigt bleiben.

Welches Fazit läßt sich aufgrund dieser knappen Bestandsaufnahme von CCTV nun ziehen? Die Entwicklung steckt in Deutschland noch in den Anfängen und hat bei weitem noch nicht jenen Entwicklungsstand Großbritanniens erreicht. Insoweit verbietet sich der Entwurf überzogener Bedrohungs- und Überwachungsszenarien. Gleichwohl kann vom Einsatz der Videoüberwachung, vor allem im Kontext flankierender kontrolltechnologischer Identifizierungs-

systeme, eine Gefährdung bürgerlicher Partizipations- und Freiheitsrechte ausgehen, die zukünftige Debatten noch stärker thematisieren dürften. Der dystopische Charakter, mit dem die Videoüberwachung oft in Verbindung gebracht wird, und der in den Bildern von Hochsicherheitsgesellschaften durchschlägt, sollte allerdings nicht überstrapaziert werden. Vielen Überwachungstechniken wohnt eine ambivalente, um nicht zu sagen janusköpfige Struktur inne. Das gilt in besonderem für die Videoüberwachung, die etwa auch gewalttätige Polizeieingriffe dokumentieren könnte. Eine realistische Einschätzung dieser Kontrolltechnik dürfte dahin gehen, sie als einen wichtigen Eckwert eines umfassenderen kontrollpolitischen »technical fix« zu bewerten. Die tiefgreifenden Veränderungen, die die Kriminalitätskontrolle in den vergangenen dreißig Jahren in der westlichen Hemisphäre durchgemacht hat, sind nur dann hinreichend zu verstehen, wenn wir die sozialen, kulturellen und politischen Kräfte betrachten, die diesen Wandel getragen und forciert haben. Dabei ist ein Aspekt ganz besonders zu beachten. Es gibt nicht die eine Antwort auf Kriminalität. Vielmehr steht ein ganzes Arsenal möglicher, mitunter auch durchaus widersprüchlicher Maßnahmen bereit, das aktiviert werden kann, um gesellschaftlich zu reagieren. Insofern zeichnet sich die »neue Kultur der Kontrolle« durch eine angewandte Mixtur alter, altbekannter Pönalcodierungen¹ und avancierter Kontrolltechnologien aus. Dazwischen ist ein versicherungstechnisches Risikomanagement geschaltet, das Kriminalität unter ökonomischen Kosten-Nutzen-Kriterien im Dreieck von Kontrolle, Strafe und Prävention handhabbar zu machen sucht (Garland 2001).

Literatur

- Ditton, J.: Crime and the City. Public Attitudes towards Open-Street CCTV in Glasgow, in: *British Journal of Criminology* (2000) 40, S. 692-709.
- Garland, D.: *The Culture of Control. Crime and Social Order in Contemporary Society*, Oxford 2001 (University Press).
- Legnaro, A.: Aus der Neuen Welt: Freiheit, Furcht und Strafe als Trias der Regulation, in: *Leviathan*, Heft 2/2000, S. 202-220.
- Newburn, T./Hayman, St.: *Policing, Surveillance and Social Control. CCTV and police monitoring of suspects*, Cullompton 2002 (Willan Publishing).
- Nogala, D.: Moderne Überwachungstechnologien. Zum Stand der Kunst, in: *Bürgerrechte & Polizei/CILIP* 60 (2/1998), S. 6-11.
- Norris, C./Armstrong, G.: Smile, you're on camera. Flächendeckende Videoüberwachung in Großbritannien, in: *Bürgerrechte & Polizei/CILIP* 61 (3/1998), S. 30-40.
- Reuband, K.-H.: Videoüberwachung: Was die Bürger von der Überwachung halten, in: *Neue Kriminalpolitik*, Heft 2/2001, S. 5-9.

1. Pönalcodierungen sind Codierungen, die das Strafrecht betreffen. (Anm. der Redaktion)

padelun und Wolfgang Föste

Chronologie der Dummheiten ...

Videoüberwachung und Datenschutz in Bielefeld

Einleitung¹

Brrrr..., es kommt schleichend. Kaum zu glauben, dass das Thema Videoüberwachung mit solcher Macht wieder über uns kommen würde. Ganz sicher würde sich doch genügend Widerstand finden, in der Bevölkerung, und Videoüberwachung würde nur aus vereinzelt Schaufechten phantasieloser Politikern bestehen.

Nixda. Es kommt schlimmer, als wir's uns bei unserem Lobeck'schen Überwachungsstudium² »Visuelle Kommunikation ist das ideale Studium um später Nachbarn überwachen zu können« je schwarz ausgemalt haben. Heute überspielen die Kameras keine analogen Signale an die Zentrale, sondern die Daten liegen sofort digital vor – und lassen sich nach allen Regeln der digitalen Kunst vollautomatisch oder manuell verarbeiten (per eMail versenden, kopieren, manipulieren, etc.).

Und was es vor allem so schwierig macht: Alle Argumente gegen Videoüberwachung klingen so blöde. Dabei braucht es gar keine Argumente dagegen. »Informationelle Selbstbestimmung« ist ein Grundrecht – das muss niemand immer wieder begründen.

Videoüberwachung ist Dumpfbakkenpolitik. Politik von Dumpfbakken für Dumpfbakken. Eine Versuchung für Menschen, denen die Illusion von Sicherheit wichtiger ist als Frieden. Kleingeister, deren gedankliche Gartenzwerge zu Riesen über dem eigenen Hori-

zont wachsen sollen. Ein Versuch, vor dem Frieden zu fliehen, der Tugenden bedingt.

Wer die Presselandschaft in Deutschland nach dem Wörtchen »Videoüberwachung« durchscannt³, findet immer mehr Ratssitzungen kleinerer Orte, die ihre müllprobleme⁴ auf dem schulhof⁵ mit Videoüberwachung lösen wollen.

Wie blöd so etwas aussehen kann, dokumentiert die kleine Chronologie aus Bielefeld, dem Oberzentrum der Mittelmäßigkeit.

Zur Chronologie ...

16. November 2000 Videoüberwachung im Ravensberger Park bleibt Einzelmaßnahme:

Beim Besuch der CDU-Landtagsabgeordneten aus Ostwestfalen-Lippe in Bielefeld war laut Westfalen-Blatt zu hören, dass die beschlossene Videoüberwachung im Ravensberger-Park die einzige Maßnahme dieser Art in NRW bleiben wird. »Die Widerstände bei SPD und Grünen sind zu groß«, sagte der Bielefelder Landtagsabgeordnete und CDU-Fraktionsvorsitzende im Bielefelder Stadtrat Rainer Lux.

7. Dezember 2000 Videokameras in Bielefelder Straßenbahnen:

Vier Straßenbahnwagen der Stadtwerke sollen bis Ende des Jahres mit Videokameras ausgestattet werden. Je nach Fahrzeugtyp sollen bis zu 14

Kameras eingebaut werden. Auf diese Weise sollen Vandalismus und andere Straftaten besser erkannt werden. Die Aufnahmen von Verdächtigen sollen der Polizei zur Aufklärung zur Verfügung gestellt werden. Laut Stadtwerke wird die Installation der Kameras 100.000 Mark kosten. Die Mittel kommen aus dem NRW-Programm »Service und Sicherheit im ÖPNV«. Die Videoaufnahmen werden auf Festplatte aufgenommen und normalerweise nach 24 Stunden gelöscht.

13. Dezember 2000 Grüne: Videokameras schwächen »Kultur des Hinschauens«



Überwachen und nicht hinschauen.

Gegen die geplante Videoüberwachung in Stadtbahnen sprechen sich die Grünen aus. Die Begründung, dass mit einer Videoüberwachung Vandalismus eingedämmt und Straftaten verhindert werden könnten, kann aus Sicht der Grünen nicht dazu her-

halten, Bürgerrechte einzuschränken. Anstatt Big Brother bei jeder Stadtbahn mitfahren zu lassen, sollte vielmehr der Einsatz der Sicherheits- und Servicekräfte verbessert und wenn nötig verstärkt werden, schreiben die Grünen in einer Presseerklärung. Durch den Einsatz von Videokameras erwiesen die Stadtwerke ihrer eigenen Aktion »Kultur des Hinschauens« einen Bärendienst. Denn Videoüberwachung führt erwiesenermaßen dazu, dass Menschen bei konkreten Anlässen weniger eingreifen. Man verlässt sich auf die trügerische Sicherheit, die die Videokameras vermitteln. Für die PDS wird Bielefeld zu einem Experimentierfeld zur flächendeckenden Installation von Kameras im »öffentlichen Raum«. Die Stadt werde schon jetzt mit hunderten von Video-

1. Die Einleitung schrieb padelun, FoeBuD e.V. (<http://www.foebud.org> und <http://www.bigbrotherawards.de>), die Chronologie stammt von Wolfgang Föste, Webwecker Bielefeld (<http://www.webwecker-bielefeld.de>).

2. Prof. Rolf Lobeck lehrt visuelle Kommunikation an der Gesamthochschule Kassel. Er hatte schon in den 70ern recht extreme Vorstellungen davon, wofür Medien wirklich nützlich sind.

3. Wenn Sie vom Durchscannen partizipieren wollen, schreiben Sie bitte eine leere Nachricht an ueberwachung-subscribe@ml.foebud.org - Sie bekommen dann fast täglich Meldungen zum Thema Videoüberwachung.

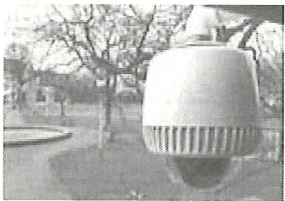
4. Dies ist eine Variable. Setzen Sie bitte ein Problem Ihrer Wahl ein.

5. Dies ist ebenfalls eine Variable. Setzen Sie bitte einen Ort Ihrer Wahl ein.

kameras allein im öffentlichen Raum »zugekleistert«, dies habe eine noch nicht abgeschlossene Erhebung der PDS über Videokameras in Bielefeld ergeben. Die PDS fordert, die Verschwendung von Steuergeldern sofort einzustellen, statt dessen solle mit dem Geld den Bau der Stadtbahn in Richtung Theesen zügig in Angriff genommen werden. Die PDS will symbolisch gegen die Videokameras in den Straßenbahnen vorgehen.

17. Januar 2001

Videokameras im Ravensberger Park installiert



Das Auge des Gesetzes wird nicht viel zu sehen bekommen.

Die Kameras zur Videoüberwachung im Ravensberger Park sind installiert. Der Medienrummel war groß, aber so

ganz ernst scheint die Presse das Projekt nicht zu nehmen. Der Reporter der Neuen Westfälischen philosophierte in seinem Bericht über die Installation von Lautsprechern im Park, dann könne man per Kamera ertappte Diebe gleich mit lauter Stimme ansprechen. Dieser Humor ist vielleicht auch ein gutes Zeichen – das Videoprojekt ist öffentlich schon tot, bevor es überhaupt begonnen hat. Im Vorfeld hatten die Zeitungen in Bielefeld allerdings so gut wie gar nichts zur Aufklärung über die Gefahren der Videoüberwachung beigetragen. In drei bis vier Wochen sollen die Kameras die Überwachung aufnehmen, so der Bielefelder Beigeordnete Peter Pohl. Die Bilder werden in eine nahe gelegene Polizeiinspektion übertragen und aufgezeichnet, wenn Verdacht einer Straftat besteht. Allerdings sind in letzter Zeit die Delikte im Park stark gesunken. Klaus Rees von den Grünen sieht in der Videoüberwachung »einen gravierenden Eingriff in die Persönlichkeitsrechte« der Bielefelder BürgerInnen. Einige Mitglieder des FoebuD begleiteten die Veranstaltung mit Protestplakaten.

Wurden die Kameras wieder abgebaut? Am heutigen Mittwoch ragten

an der Vorderseite der VHS nur ein paar Drähte in die kalte Winterluft und an der Villa Huelsmann war auch keine Kamera zu entdecken. Nur den Eingang der VHS überwacht ein tolles Exemplar.

15. Februar 2001

Videokameras – jetzt werden sie montiert

Die Presse aus nah und fern hatte sich leimen lassen. Vor ein paar Wochen war nur das Gehäuse einer einzigen der vier geplanten Überwachungskameras im Ravensberger Park installiert worden. Die Firma Siemens konnte nicht liefern. Dabei hätte es bleiben können. Der große Pressetermin war ein Schwindel, mit dem die Presse und ihre LeserInnen hinter Licht geführt worden sind. Big-Brother-Verhalten der Stadt im Umgang mit der Öffentlichkeit. Das müsste ein politisches Nachspiel haben. Jetzt kann Siemens aber doch liefern, so Stadtsprecher Dietmar Schlüter. Bis zum Wochenende sollen die Kameras da sein.

21. Februar 2001

Datenschutzbeauftragte kritisiert Videoüberwachung in Bielefeld

Die nordrhein-westfälische Datenschutzbeauftragte Bettina Sokol hat die zunehmenden Videoüberwachung von öffentlichen Plätzen und Einrichtungen kritisiert. Bei der Vorstellung des Datenschutzberichts am Dienstag in Düsseldorf erklärte sie, auch für die Polizeiüberwachung von Zentren der Kriminalität müssten strenge Maßstäbe angelegt werden. Sie forderte einheitliche Vorgaben für Verkehrsunternehmen, die in Bussen und Bahnen Kameras installieren. Sokol erklärte, solche Bilder dürften nach den Richtlinien des Datenschutzes normalerweise nicht aufgezeichnet und archiviert werden. Schilder sollten deutlich auf die Videoüberwachung hinweisen. Die Datenschutzbeauftragte kritisierte in ihrem Bericht außerdem die Überwachungspraxis einzelner Kommunen in NRW. So seien in einem städtischen Schwimmbad die Besucher in den Umkleidekabinen mit Kameras beobachtet worden. In diesem Fall müsse das Hausrecht unbedingt hinter den Schutz der Intim-

sphäre der Badegäste zurücktreten, forderte Sokol. Als nicht angemessen wertete sie auch ein Pilotprojekt, bei dem ein öffentlicher Park in Bielefeld als angeblicher Kriminalitätsbrennpunkt von den Behörden mit Kameras beobachtet werden soll. Die festgestellte Zahl der Verbrechen rechtfertige die Überwachung nicht. Auch die Übertragung von Bildern über Web-Cams ins Internet verletze dem Bericht zufolge oft Persönlichkeitsrechte. Wenn Rathäuser, Universitäten, Geschäfte oder Unternehmen zu Werbezwecken Live-Bilder ins Internet stellen, dürften darauf keine Personen oder Auto-Kennzeichen zu erkennen sein. Nur Übersichtsaufnahmen seien erlaubt. Bei einer Überprüfung habe man zahlreiche Verstöße festgestellt.

28. Februar 2001

Schwarzer Freitag für Bürgerrechte: Videoüberwachung im Ravensberger Park ist online



PDS-Mitglieder verhüllen eine Kamera.

Seit dem »schwarzen« Freitag, den 23. Februar, wird der Ravensberger Park nun durch vier Videokameras überwacht. Vier Kameras übertragen klare Bilder in eine Polizei-Wache am Kesselbrink. Symbolisch hatten Mitglieder der PDS eine

der Kameras vor der Stiftung Huelsmann verhüllt. Im Stadtrat applaudierten die bürgerlichen Parteien der Bekundung von Kulturdezernent Dr. Albrecht Peter Pohle, dass die Kameras nun arbeiteten. Klaus Rees von den Grünen wies darauf hin, dass die NRW-Landesdatenschutzbeauftragte für die Überwachung keine rechtliche Grundlage sehe und prophezeite, dass die Kameras nach einer Klage durch eine BürgerIn rasch wieder abgebaut werden müssten. Er appellierte an OB David und Polizeipräsident Kruse, schon jetzt die Kameras abzubauen. Pohle sagte in der Sitzung, dass es in Bielefeld außer diesen vier Kameras keine weitere Videoüberwachung nach Polizeirecht gebe. Es war in der Ratssitzung auch zu hören, dass die Stadtwerke nun ab April Straßenbah-

nen mit Videoüberwachung einsetzen werden.

9. März 2001

Rollende Videokameras in Bielefeld

Jetzt ist es so weit. Die Stadtwerke gehen mit Überwachungskameras in ihren Stadtbahnen ins Rennen. Seit dem 8. März 2001 fährt eine erste Straßenbahn mit Videokameras auf der Linie 4 zwischen den Haltestellen Rathaus und Universität. Die gespeicherten Aufnahmen werden für 24 Stunden aufbewahrt und danach gelöscht. Einen Tag darauf startet ein zweiter Straßenbahnwagen mit Videokameras, der auf allen Linien der Stadtbahn in Bielefeld verkehren soll.

21. März 2001

Bielefeld ist die sicherste Großstadt in NRW –

warum dann die Videoüberwachung im Ravensberger Park?

Laut NRW-Kriminalstatistik ist Bielefeld die sicherste Großstadt des Landes. Noch vor Gelsenkirchen und Hagen. In Bielefeld wurden im Jahr 2000 23.682 Straftaten verübt. 1.441 weniger als im Jahr zuvor. Ein Rückgang von 5,7 Prozent. Bei den Wohnungseinbrüchen ist die Zahl sogar um 24,7 Prozent, bei Raubüberfällen um 13,5 und bei den Straßenkriminalität um 9,3 Prozent gesunken. Es gab nur wenige schwere Gewaltdelikte in Bielefeld. Beunruhigend ist nur, dass die Zahl der Täter unter 21 bei den Gewaltdelikten überproportional gestiegen ist. Wenn sich die Sicherheitslage in Bielefeld so hervorragend darstellt, dann ist es nicht verständlich, warum gleichzeitig ein innenstadtnaher Park als »Kriminalitätsschwerpunkt« deklariert wird, um nach Polizeigesetz NRW eine Videoüberwachung genehmigt zu bekommen. Laut einer jüngst von der Polizei selbst verteilten Statistik wurden im gesamten Jahr 2000 im Ravensberger Park 43 Straftaten, davon 6 erhebliche, verübt. Im Vergleich zu den Straftaten, die im letzten Jahr in Bielefeld verübt wurden, sind das noch nicht einmal 2 Promille. Der Fraktionsgeschäftsführer der Grünen Klaus Rees fordert daher: »Die Videoüberwachung muss sofort eingestellt und die Kameras

müssen sofort wieder abgebaut werden!« Sie sei nach der Zahlenlage nicht verhältnismäßig. Rees kündigte an, dass die Grünen die innenpolitische Sprecher in der Landtagsfraktion ihrer Partei in Düsseldorf bitten werden, auf einen Widerruf der Genehmigung des Bielefelder Modellversuchs der Videoüberwachung hinzuwirken.

4. April 2001

Demonstration gegen Videoüberwachung

Ganz plötzlich klebten da so kleine unscheinbare Aufkleber auf den Türen am Hauptbahnhof: 3S – Sicherheit, Sauberkeit, Staatsgewalt. Tatsächlich bedeutet das, dass die Videoüberwachung auch am Bielefelder Hauptbahnhof eingezogen ist. Und nicht nur im Bahnhof, sondern auch außen am Gebäude hängen diese undurchsichtigen Domekameras. Dieser Tropfen brachte das Fass zum Überlaufen: Der FoeBuD meldete eine Demonstration an. Diese fand am 23.3.2001 bei strömenden Regen statt. Aktivisten, als Aliens verumumt verteilten Flugblätter – der Kommunikationsbedarf mit der Bevölkerung war unerwartet hoch. Eine Dokumentation und Bilder finden sich bei FoeBuD. Interessantes Detail am Rande: Während die Überwachungszentrale im Hauptbahnhof bereits 1999 ausgebaut worden ist, hat der lang angekündigte Bahnhofsumbau und Tunneldurchstich bis heute nicht stattgefunden. Ein Schelm, der Gutes dabei denkt...

12. April 2001

Bahn AG überwacht aus Bielefeld ganz OWL mit Videokameras



Big Brother Bahn

nun vom Bielefelder Hauptbahnhof aus Bahnstationen in Ostwestfalen-Lippe überwachen. Bis August soll die Ausrüstung der 76 Bahnstationen in OWL beendet sein. Die neue Zentrale für Service, Sicherheit und Sauberkeit (Bahn-Jargon: »3-S«) wurde vergangene Woche in Betrieb genommen. Die

Rund um die Uhr können Mitarbeiter der deutschen Bahn AG

Daten gelangen per Telefonleitung in die Bielefelder Videoüberwachungszentrale. Die Bahn AG baut ihre Videoüberwachung in einer Zeit aus, in der immer mehr Datenschützer vor der unkontrollierbaren Videoüberwachung warnen.

8. Juni 2001

Anti-Video-Happening im Ravensberger Park

Sie stülpten der Kamera bei der Villa Huelsmann einen Pappkarton über und drückten auf Transparenten und in Spontan-Darbietungen ihren Protest gegen die Videoüberwachung im Ravensberger Park aus. 50 junge Leute einer Veranstaltung gegen Globalisierung im AJZ kamen am vorigen Samstagabend zu diesem friedlichen Protest im Ravensberger Park zusammen. Die Polizei durch die Kameras informiert beobachtete das Geschehen.

11. Juli 2001

Partnerstadt Rochdale wird streng videoüberwacht

England ist das Mutterland der Videoüberwachung. Davon konnte sich jetzt auch der Bielefelder Polizeioberrat Thomas Kubera in Rochdale überzeugen. Eine Bielefelder Delegation unter der Leitung von Horst Grube, Bezirksvorsteher Mitte, besuchte kürzlich die britische Partnerstadt und diskutierte dort über »Recht und Ordnung in Rochdale«. Kubera, Leiter der Polizeiinspektion Ost, berichtete nun in einem Pressegespräch, dass in Rochdale 17 öffentliche Kameras in Betrieb seien, von denen die ganze Stadt (92.000 EinwohnerInnen) erfasst werden könne. Acht Beamte der Stadtverwaltung lassen dort die Kameras rund um die Uhr laufen. Die Videos werden 28 Tage aufbewahrt, so Kubera. Der Datenschutzbeauftragte könne sich die Bilder jederzeit ansehen. Aber nicht nur über den Dächern von Rochdale, sondern auch in den sieben städtischen Hochhäusern sind an den Eingängen, auf Fluren und in Liften Überwachungskameras installiert. Kubera: »Das Vertrauen der Briten in die staatlichen Institutionen ist sehr groß. Man glaubt, dass zum Beispiel Stadtverwaltung und Polizei zum Wohle aller arbeiten.« Gerade aber in England

kommt es immer wieder zu erheblichen Pannen mit den aufgenommenen Videos, wie auf der Veranstaltung Public Domain im Oktober letzten Jahres berichtet wurde.

8. Oktober 2001

Public Domain 112: Wie kann man sich mit Technik gegen elektronische Übergriffe wehren?

Marit Köhntopp, Datenschützerin aus Kiel, stellte auf der 112. Public Domain⁶ des FoBuD e.V. verschiedene Techniken und Werkzeuge vor, mit denen man seine Botschaften im Internet schützen kann, z.B. Verschlüsselung von elektronischer Post, Steganographie, Anonymisierungsdienste und Systeme für ein Identitätsmanagement. Eine Debatte passend zur heute brisanten Frage nach dem Zugriff auf persönliche Daten und dem Schutz der Privatsphäre im elektronischen Datenverkehr. Auf der Internetseite von Marit Köhntopp⁷ finden sich interessante Hinweise zu Publikationen und sind wichtige Begriffe der Debatte erklärt, z. B. Steganographie.

Auch das Bundesministerium für Wirtschaft und Technologie bietet zusammen mit dem Bundesministerium des Inneren eine Website⁸ zur Sicherheit im Internet mit monatlichem Newsletter an.

15. Oktober 2001

Videokameras & Bildungspolitik: PDS äußert sich kritisch

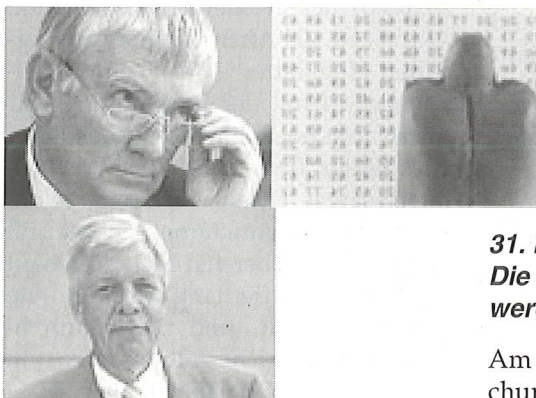
Die Bielefelder PDS hat gefordert, die Überwachungskameras im Ravensberger Park abzubauen. Sie seien ein untauglicher Versuch, die Sicherheit auf öffentlichen Straßen und Plätzen zu erhöhen. Die Partei führt ihr Votum auch auf den Rückgang herausragender Straftaten im Ravensberger Park zurück. Ebenfalls kritisch sieht die PDS die beabsichtigten Schließungen von Stadtteilbibliotheken. Gerade jüngere Menschen würden von der Maßnahme betroffen.

Universität Bielefeld muss Daten von Studenten zur Rasterfahndung herausgeben

Das Land NRW hat, nach Angaben des Universitätsprechers Gerhard Trott, die Universität Bielefeld aufgefordert, Daten männlicher Studenten bestimmter Geburtsjahrgänge zu übermitteln. Die Universität kommt dieser Forderung nach. Trott sieht die Verunsicherung unter den Studenten, da Daten auch derjenigen herausgegeben werden, die in keinerlei Verbindung mit den Geschehnissen in den USA stehen. Martin Lücke, der Vorsitzende des AStA forderte die Universität auf, die Betroffenen über die Weitergabe ihrer Daten zu informieren.

26. Oktober 2001

Verleihung des BigBrotherAwards am 26. Oktober 2001 in Bielefeld: Ausgezeichnete Minister



Schily and Müller are watching you.

In Zeiten, in denen der Datenschutz hart unter Druck gerät, erhielt die Bundesregierung am 26. Oktober 2001 gleich zwei der ungeliebten Preise für »Datenkraken« des alljährlich in Bielefeld verliehenen BigBrotherAwards. An Bundesinnenminister Otto Schily wurde der Hauptpreis verliehen, weil er im Zuge der Terrorismusbekämpfung für »den Abbau von Bürgerrechten, Datenschutz und Informationeller Selbstbestimmung« eintrete, wie es in der Preisbegründung u.a. heißt. In der Kategorie Kommunikation erhielt Bundeswirtschaftsminister Dr. Werner Müller für die »Telekomüberwa-

chungsverordnung« den Award, weil mit ihr eine technische Infrastruktur geschaffen worden sei, die durch fest installierte Geräte bei Telekommunikationsanbietern eine Überwachung quasi per Knopfdruck ermögliche. Weitere Preise gingen an: die Firmen Informa Unternehmensberatung GmbH aus Pforzheim (Kategorie: Business und Finanzen), RealNetworks GmbH aus Hamburg (Kategorie: Spyware) und ProtectCom Deutschland aus Saarbrücken (Kategorie: Arbeitswelt). Traurig, aber wahr: Das Hans Ehrenberg-Gymnasium in Bielefeld-Sennestadt erhielt einen Regionalpreis für seine SchoolCard mit Fingerabdruck. Da waren die Youngster und ihre Pauker schon weiter als der Bundesinnenminister. So sollte die junge Generation nicht in die digitale Zukunft starten. Die SchoolCard leiste dem »Abbau der Privatsphäre unter dem Deckmantel der Innovation« Vorschub, meinte die Jury.

31. März 2002

Die Kameras im Ravensberger Park werden abgeschaltet

Am 31. März werden die Überwachungskameras im Ravensberger Park abgeschaltet. Das teilte der Bielefelder Polizeipräsident in der Sitzung des Hauptausschusses der Stadt Bielefeld mit. Angeblich sei der Einsatz der Kameras so erfolgreich gewesen, dass auf sie nun verzichtet werden könne.

6. <http://www.foebud.org/pd/pd112/index.html>

7. <http://www.koehntopp.de/marit/>

8. <http://sicherheit-im-internet.de/home/home.phtml>

Harald Stelljes

Videoüberwachung in Großwohnanlagen

Ausgangslage und Entstehung

Ein Wohnungsunternehmen in Bremen beabsichtigte im Jahre 1999, seine Großwohnanlagen mit Videokameras zu überwachen. Mit dieser Maßnahme sollten Sachbeschädigungen (z.B. Brände in Tiefgaragen, Beschmierungen und Zerstörungen in Eingangsbereichen) verhindert oder zumindest verringert werden. Es hat die Aufsichtsbehörde nach dem Bundesdatenschutzgesetz, den Landesbeauftragten für den Datenschutz, gebeten, die Zulässigkeit einer derartigen Videoüberwachung zu bewerten.

Vorführung der Anlage

Dazu hat das Unternehmen den Vertretern der Aufsichtsbehörde ein digitales Videosystem vorgeführt, das von einem Sicherheitsdienst eingesetzt werden sollte.

Die Demonstration hat deutlich gemacht, dass Überwachungsanlagen dieser Qualität in der Lage sind, Bilder und Ausschnitte von nicht gekannter und nicht erwarteter Güte und Präzision zu liefern. Die Vorführung mit den vielfältigen technischen Möglichkeiten, z.B. die Alarmschaltung, die Voralarmschaltung, die digitale Bildbearbeitung, die Aufhellung dem bloßen Auge als dunkler Bereich nicht erkennbarer Ausschnitte, der um 360 Grad rundum schwenkbare Überwachungsausschnitt oder der beeindruckende Zoombereich, haben deutlich gezeigt, wie intensiv die Überwachung eines Lebensbereiches werden kann.

Ausmaß der vorgeführten Technik

Diese beinahe unbegrenzten Möglichkeiten der Überwachung und Herstel-

lung von Bildern erschweren die Aufklärung und Benachrichtigung der überwachten Personen erheblich. Ein bloßer Hinweis darauf, dass ein gewisser Bereich videoüberwacht wird, würde bei den Betroffenen keineswegs die Vorstellung entstehen lassen, dass mit derartiger Präzision und Erfassungstiefe gearbeitet werden kann, wie sie in der Vorführung vorgestellt worden sind.

Bedenkt man die Reaktionen der Bevölkerung auf die beabsichtigte Durchführung einer Volkszählung im Jahre 1983, so sind entsprechend heftige Reaktionen gegenüber dieser Technik nicht auszuschließen, wenn den Betroffenen bekannt wird, wie total und genau eine solche Videoüberwachungsanlage rund um die Uhr alle menschlichen Verhaltensweisen in ihrem Erfassungsbereich erheben und festhalten kann. Denn es geht – wie im Falle der Volkszählung – auch bei der Videoüberwachung um einen Eingriff in das grundrechtlich geschützte informationelle Selbstbestimmungsrecht der von der Videoüberwachung Betroffenen.

Damalige Rechtslage

Wie sah nun zum damaligen Zeitpunkt – also vor Inkrafttreten des neuen § 6b Bundesdatenschutzgesetz (BDSG) – die Rechtslage aus? In dem Moment, in dem Bilder begrenzt oder auf Dauer gespeichert und nach bestimmten Kriterien personenbezogen ausgewertet werden können, z.B. eine Serie von Kfz-Kennzeichen, Bilder von Hauseingängen mit Hausnummern und Bewohnern o.ä. wäre auf solche Sammlungen das damals geltende Bundesdatenschutzgesetz (BDSG) anzuwenden. Die Anwendung ist unmittelbar verknüpft mit der Form und Dauer der Speicherung, der systematischen Sammlung von

Bildern und den Möglichkeiten der Auswertung.

Angesichts der vielfältigen und intensiven Möglichkeiten der Überwachung, die das vorgeführte System bietet, würde es den tatsächlichen Umständen aber nicht gerecht, wenn man auf alle Vorgänge die allgemeinen Bestimmungen des damaligen BDSG anwenden würde. Das BDSG war seinerzeit weder den neuen Bedingungen angepasst worden, die die EU-Datenschutz-Richtlinie setzt, noch hat der Gesetzgeber bei Erlass dieser Vorschriften im Jahre 1990 jemals auch nur im entferntesten an die dramatische technische Weiterentwicklung im Videobereich und die Verknüpfung dieser Technik mit einem Computer sowie an die Möglichkeiten moderner Bildbe- und -verarbeitung gedacht.

Eine rechtliche Gestaltung des Einsatzes derartiger Videotechnik kann daher datenschutzrechtlich nur in einer bereichsspezifischen Regelung getroffen werden. Eine rudimentäre Regelung war seinerzeit diesbezüglich mit § 6b BDSG-Novelle in der Diskussion. Erst Ende Mai 2001 ist eine Regelung zur Videoüberwachung als § 6b BDSG in Kraft getreten.

Aus damaliger Sicht verblieb nur die Verpflichtung des Wohnungsunternehmens, das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz, insbesondere das Recht am eigenen Bild der betroffenen Dritten (Mieter, deren Besucher, Postboten und sonstige Personen) zu wahren (z.B. §§ 242, 823 und 1004 Bürgerliches Gesetzbuch-BGB). Diese Regelungen sind jedoch nicht so präzise, dass sie eine klare Einschätzung zulassen, ob der Einsatz der vorgeführten Technik rechtlich zulässig wäre. Es gibt zwar Rechtsprechung zur Anwendung einfacher Videotechnik mit analoger Aufzeichnung, nach

der der Einsatz solcher Videotechnik zum Schutz des eigenen Grundstücks in seinen Grenzen akzeptiert werden kann (siehe Abschnitt zur BGH-Rechtsprechung).

Allerdings geht in dem hier zu behandelnden Fall der öffentlich gewidmete Raum nahtlos über in die im Eigentum des Wohnungsunternehmens stehenden Zuwegungen und Flächen. Anders als die nachbarlich durch Zäune und Pforten abgegrenzten Grundstücksflächen von Einfamilienhäusern stellen die vom Wohnungsunternehmen gehaltenen Flächen quasi öffentliche Flächen dar, weil sie jedermann zugänglich sind. Aber auch die bei der Vorführung verwendete Technik ist keinesfalls mit der von der Rechtsprechung bewerteten herkömmlich eingesetzten Videotechnik mit festen Brennweiten und analoger Aufzeichnung vergleichbar.

Rechtsprechung des Bundesgerichtshofs (BGH)

Der BGH formuliert in seinem Urteil vom 25. April 1995 (Az.: VI ZR 272/94 (KG)), dass auch die Herstellung von Bildnissen einer Person, insbesondere die Filmaufzeichnung mittels Videogerät, in der Öffentlichkeit zugänglichen Bereichen – auch ohne Verbreitungsabsicht – einen unzulässigen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellt. Im vom BGH entschiedenen Fall überwachte ein Hauseigentümer gezielt und regelmäßig ein bestimmtes Stück eines öffentlichen Weges über längere Zeiträume. Die Überwachung war darauf angelegt, Benutzer des Weges in einer Vielzahl von Fällen abzubilden und aufzuzeichnen. Dabei sei es um den Zugangsweg zu Wohngrundstücken, darunter demjenigen der Kläger, gegangen. Der BGH weist in diesem Zusammenhang darauf hin, dass die Kläger der Videoaufnahme nicht ausweichen können, wenn sie sich auf dem Weg von oder zu ihrem Grundstück befinden. Die Kläger können weder beeinflussen, wann sie bei solchen Gelegenheiten aufgenommen werden, noch können sie feststellen, ob solche Aufzeichnungen gefertigt worden sind oder nicht. Sie müssten daher, wenn sie den Weg benutzen, ständig mit der der Überwachung die-

nenden Aufzeichnung ihres Bildes rechnen.

Der BGH stellt daher fest, dass derartige Maßnahmen eine **schwerwiegende** Beeinträchtigung des allgemeinen Persönlichkeitsrechts der Kläger bewirken. Denn diese müssen sich praktisch stets, wenn sie von ihrem Haus kommend oder zu ihrem Haus gehend den öffentlichen Zugangsweg benutzen, in einer jede ihrer Bewegung geradezu dokumentierenden Weise kontrolliert fühlen. Auf dem jeweiligen Videofilm ist nicht nur festgehalten, wann, wie oft und in welcher Begleitung sie den Weg begangen haben, sondern auch in welcher Stimmung, mit welchem Gesichtsausdruck etc. sie dies getan haben. Die hierin liegende Beeinträchtigung der Kläger werde nicht dadurch gemindert, dass die beklagte Partei die Videoaufzeichnung nach Überprüfung wieder lösche.

Die BGH-Entscheidung macht deutlich, dass die Installation und Inbetriebnahme der vorgeführten Videoüberwachungsanlage mit erheblichen rechtlichen Risiken verbunden ist, solange der Gesetzgeber keine klaren Vorgaben gemacht hat, unter welchen Bedingungen und in welchem Umfang zum Schutze anderer Rechtsgüter in die allgemeinen Persönlichkeitsrechte Dritter eingegriffen werden darf.

Empfehlung der Aufsichtsbehörde

Angesichts dieser Rechtslage hat die Aufsichtsbehörde das Wohnungsunternehmen gebeten, noch einmal zu überprüfen, ob eine derartige Videoüberwachungsanlage eingeführt werden soll, oder ob andere, weniger gravierende Maßnahmen zum Schutz der Anlagen des Wohnungsunternehmens und zur Sicherheit der Bewohner getroffen werden können.

Sollte sie sich dennoch für den Einsatz einer solchen Videoüberwachungsanlage entscheiden, würden die rechtlichen Bedenken gegen den Einsatz einer solchen Anlage jedenfalls in dem Maße geringer, als die Überwachungsanlage durch technische Vorwahl so ausgestaltet würde, dass zwar Personen an sich und deren

Handlungen über den Bildschirm wahrnehmbar wären, die einzelne Identität der Personen aber nicht individualisiert und personenbeziehbar erkannt werden kann.

Ebenso sollte das System so voreingestellt sein, dass nach sehr kurzen Intervallen die gespeicherten Bildsequenzen, die keinen Grund zum Einschreiten der Sicherheitskräfte geben, überschrieben oder gelöscht werden. Bereits eine so eingestellte Anlage würde es dem Sicherheitsdienst ermöglichen, sein Personal zu erkennenen Brennpunkten zu beordern. Soweit Bilder zu Beweis Zwecken weiter gespeichert bleiben sollen, sind Regelungen zur Zweckbindung, zum Zugriffsschutz und Befugnisse der Herausgabe an Dritte festzulegen.

Außerdem konnte man anlässlich der vorgenannten Vorführung vom Standort der Probeinstallation hoch über den Dächern der Wohnanlage schräg nach unten in alle Fenster der umliegenden Wohnungen blicken. Aus diesem Grunde hat die Aufsichtsbehörde darauf hingewiesen, dass eine Wohnraumüberwachung ebenso wenig in Betracht kommen kann, wie die Überwachung öffentlicher, nicht im Eigentum des Wohnungsunternehmens stehender Flächen. Keine Bedenken bestehen, wenn nach Anbringung entsprechender Hinweisschilder die im Eigentum des Wohnungsbauunternehmens befindliche Tiefgarage videoüberwacht würde.

Öffentliche Veranstaltung

Inzwischen hat eine von der beabsichtigten Videoüberwachung betroffene Stadtteilgruppe darüber öffentlich diskutiert. Die Meinungen der Bewohner waren sehr unterschiedlich. Während einige die Videoüberwachung zur Verbesserung der eigenen Sicherheit begrüßten, haben andere Bewohner die Befürchtung geäußert, sie würden nunmehr überwacht und könnten sich nicht mehr frei bewegen. Das Wohnungsunternehmen hat dazu erklärt, vor dem Einsatz des Videoüberwachungssystems ein Konzept vorzulegen, das die Empfehlungen der Aufsichtsbehörde enthält und mit ihr abgestimmt ist. Über die Veranstaltung ist sehr ausführlich in den Medien berichtet worden.

Realisierung derzeit nicht vorgesehen

Im September 2000 teilte der Datenschutzbeauftragte des Wohnungsunternehmens mit, die Videoüberwachung ruhe bis zu einer Entscheidung über die weitere Entwicklung des betroffenen Stadtteils.

Vorgesehen ist nämlich, durch städtebauliche Maßnahmen den Stadtteil erheblich aufzuwerten mit dem Ziel, dort die Lebens- und Wohnqualität zu verbessern. Inwieweit nach Abschluss dieser Maßnahmen auf die vorgesehene Videoüberwachung verzichtet werden kann, werde erst dann entschieden. Zugesagt worden ist

jedenfalls, dass die Aufsichtsbehörde darüber unaufgefordert unterrichtet wird. Bis zum Redaktionsschluss (Januar 2002) hat sich kein neuer Sachverhalt ergeben.

Rolf P. Würtz

Technik und Leistungsfähigkeit automatischer Gesichtserkennung

Zusammenfassung

Nach einem allgemeinen Überblick über Aufgaben und Probleme des Computersehens wird diskutiert, warum es schwierig ist, die Leistungsfähigkeit solcher Systeme objektiv zu messen. Es folgt eine Einführung in die Technik der automatischen Gesichtserkennung. Danach werden die Ergebnisse des FERET Tests beschrieben, bei dem Gesichtserkennungssysteme unabhängig auf einer großen Datenbasis verglichen wurden. Die Schlussfolgerung ist, dass die derzeitigen Systeme für den praktischen Einsatz noch nicht tauglich sind, es aber durch die intensive Forschungs- und Entwicklungstätigkeit recht bald werden könnten.

Einleitung

Durch die geplante Anwendung biometrischer Merkmale und eine erhöhte Nachfrage nach automatisierter Überwachung ist die automatische Personenerkennung in den vergangenen Monaten ins Zentrum des Interesses gerückt. Unabhängig von den dadurch aufgeworfenen gesellschaftlichen, rechtlichen und politischen Fragen soll dieser Artikel den Stand der Technik skizzieren und die Leistungsfähigkeit der existierenden Systeme

bewerten. Dazu ist es erforderlich, einige allgemeine Bemerkungen zu Problematik und Technologie des automatischen Bildverstehens oder Computersehens zu machen.

Die Aufgabe dieses Wissenschaftszweiges ist es, aus Kamerabildern sinnvolle Rückschlüsse auf Objekte in der Welt zu ziehen. Die Anwendungen sind vielfältig und umfassen z.B. industrielle Qualitätskontrolle, automatische Auswertung von Satellitenbildern, intuitive Mensch-Maschine-Schnittstellen, Serviceroboter und Überwachung. Innerhalb der Informatik ist Computersehen für die Künstliche Intelligenz von eminenter Bedeutung, da es letztendlich Maschinen in die Lage versetzen soll, Information aus der Umwelt autonom, d.h. ohne menschliche Mithilfe, aufzunehmen und weiter zu verarbeiten.

Dieses Gebiet hat sich in den vergangenen Jahren stark auf die Verarbeitung von Bildern und Bildfolgen von Personen konzentriert. Der Anteil solcher Publikationen an allen im Computersehen ist zwischen 1991 und 1999 von unter 2% auf über 9% angestiegen – zusätzlich zur allgemeinen Steigerung der jährlichen Gesamtzahl. Zum Einen haben sowohl die verfügbare Hardware als auch die Methoden in diesem Zeitraum eine

starke Leistungssteigerung erfahren. Zweitens ist ein großer Teil dieser Forschung drittmittelfinanziert, was bedeutet, dass es ein deutliches politisches und ökonomisches Interesse an dieser Forschung gibt. Drittens haben sich die politische Landschaft und das öffentliche Meinungsbild so verändert, dass computergestützten Überwachungsmethoden nur noch mit geringem Misstrauen begegnet wird. Besonders in Großbritannien – aber in zunehmenden Maße auch in Deutschland – hat inzwischen die Hoffnung auf Kriminalitätsbekämpfung durch Videoüberwachung gegenüber der Furcht vor unangemessener Kontrolle durch öffentliche oder private Instanzen die Oberhand gewonnen.

Innerhalb der Informatik nimmt das Computersehen (wie alle Versuche, aus Sensordaten symbolische Information zu extrahieren) eine Sonderstellung ein, da die Aufgaben sehr schlecht zu formalisieren sind. Oft sind Aussagen aus den Bildern nur mit Hilfe von zusätzlichen Annahmen möglich. Das menschliche Gehirn ist sehr gut in der Lage, plausible Annahmen zu machen, um zu einer richtigen Interpretation der Bilddaten zu kommen. Folglich gibt es grundsätzlich nur eine Möglichkeit, die Leistungsfähigkeit eines Systems zum

Computersehen zu evaluieren. Bilder oder Bildfolgen müssen unter möglichst kontrollierten Bedingungen aufgenommen werden, und ein Mensch muss entscheiden, welche Aussagen über die Bilder zutreffend sind. Keinesfalls kann die Bewertung eines Algorithmus ohne Rückgriff auf menschliche Wahrnehmung geleistet werden.

Diese Situation erschwert objektive Leistungsmessungen ungemein. Normalerweise erfolgt die Auswahl der Daten, auf denen ein neu entwickelter Algorithmus getestet wird, durch dieselbe Arbeitsgruppe, die auch die Entwicklung durchführt. Da die Leistungsgrenzen eines Algorithmus nur schwer publizierbar sind und alle wissenschaftlichen Einrichtungen unter starkem Publikationsdruck stehen, gibt es eine Tendenz, Fehlschläge unter den Tisch fallen zu lassen. Daher ist zu erwarten, dass die Qualität von Algorithmen bei Anwendung auf neues Datenmaterial hinter der veröffentlichten Leistungsfähigkeit zurückbleibt. Aus den Entwicklungsabteilungen von Firmen sind keine objektiven Zahlen über die Leistung von Systemen verfügbar. Die zugehörigen Werbeabteilungen unterliegen einem noch weit höheren Zwang zur Schönfärberei als wissenschaftliche Institutionen. Generell kann man daher davon ausgehen, dass veröffentlichte Leistungsdaten im Computersehen das unter günstigsten Bedingungen erreichbare Optimum widerspiegeln.

Funktionsweise von Gesichtserkennungssystemen

Die technische Problematik der Identifikation von Personen soll nun anhand der Gesichtserkennung aus Kamerabildern aufgezeigt werden. Für andere Biometrieverfahren, wie z.B. Fingerabdruckerkennung, Iriserkennung, Sprecheridentifikation, Erkennung der Gangart ist die Grundproblematik die gleiche, die Lösungsansätze aber z.T. sehr verschieden.

Das Problem der Erkennung von Personen aus Kamerabildern besteht darin, dass – je nach Aufnahmebedingungen – ein und dasselbe Gesicht sehr unterschiedliche Bilder erzeugen

kann. Die Unterschiede können u.a. auf folgende Veränderungen zwischen zwei Aufnahmen zurückgeführt werden:

- Position des Gesichtes im Bild
- Abstand von der Kamera bzw. Vergrößerungsfaktor
- Kopfausrichtung
- Gesichtsausdruck
- Hintergrund
- teilweise Verdeckung
- Beleuchtung
- Kameratyp und -einstellung.

All diese Veränderungen müssen durch ein Gesichtserkennungssystem aufgefangen werden, um die Identität der Gesichter in zwei verschiedenen Bildern verlässlich festzustellen. Man spricht daher von invarianter Erkennung.

Die meisten dieser Veränderungen können durch Lösung des sog. Korrespondenzproblems [8] aus den Bildern »herausgerechnet« werden. Es bezeichnet die Aufgabe, zu jedem Punkt in einem Bild den zugehörigen Punkt im anderen zu finden, also z.B. das linke Auge dem linken Auge zuzuordnen. Die größte Schwierigkeit besteht darin, dass das Abbild einzelner Punkte bei verschiedenen Aufnahmen recht verschieden ausfallen kann. Dies gilt insbesondere bei Beleuchtungsänderungen, anderer Kamera und bei Kopfdrehungen. Andererseits können verschiedene Punkte relativ ähnlich ausfallen, so dass nur mit Hilfe zusätzlicher Annahmen, wie z.B. ungefähre Anordnung verschiedener Punkte sinnvolle Schätzungen der wahren Korrespondenzen gemacht werden können [1,8]. Diese Korrespondenzschätzungen werden durch alle Veränderungen im Bild mehr oder weniger gestört, und das Zusammenkommen mehrerer Veränderungen, wie z.B. Kopfdrehung und Beleuchtung führt häufig dazu, dass sie grob falsch werden.

Wenn das Korrespondenzproblem näherungsweise gelöst ist, kann die Bildinformation in der Nähe der jeweils zusammengehörigen Punkte verglichen werden. Die Gesamtähnlichkeit aller Punktepaare ergibt dann eine Ähnlichkeit der beiden Gesichter. Bei hoher Ähnlichkeit kann geschlossen werden, dass beide Bilder dieselbe

Person zeigen. Diese Entscheidung wird Verifikation genannt, da entschieden werden kann, ob die behauptete Identität zu einer gegebenen Person mit den Bilddaten übereinstimmt.

Da die Struktur aller Gesichter sehr ähnlich ist, kann das Korrespondenzproblem auch für Gesichter verschiedener Personen gelöst werden. Die Gesamtähnlichkeit kann dann direkt als Ähnlichkeit der Gesichter interpretiert werden. Auf diese Weise kann jedes Gesicht in einer Datenbank mit einem aktuellen Kamerabild verglichen und so die Identität einer Person festgestellt werden. Diese Aufgabe ist schwieriger als die Verifikation.

In beiden Fällen muss eine Entscheidungsschwelle willkürlich gesetzt werden, damit das System Identität zwischen den abgebildeten Gesichtern feststellen kann, falls die Ähnlichkeit über dieser Schwelle liegt. Liegt die Schwelle sehr niedrig, werden viele Bilder als gleich beurteilt, die in Wirklichkeit verschiedene Personen zeigen. Diese Entscheidungen werden als »falsch positiv« bezeichnet. Liegt die Schwelle sehr hoch, werden korrekte Identitäten durch das System zurückgewiesen (»falsch negative« Entscheidung). Der mit der Entscheidungsschwelle zu vergleichende Wert wird meist in komplizierterer Weise berechnet als hier skizziert, der Gebrauch einer Schwelle ist jedoch allen Verfahren gemeinsam. Das zu erwartende Verhältnis der »falsch positiven« zu »falsch negativen« Entscheidungen kann mit ihrer Hilfe eingestellt werden.

Da die Korrespondenzschätzung aufwendig und fehleranfällig ist, ist es für die Effizienz eines Verfahrens entscheidend, dass die Datenbasis zur Identifikation so organisiert ist, dass die Anwendung der Korrespondenzsuche minimiert und der eigentliche Vergleich sehr schnell und effizient ausgeführt werden kann. Zwei wesentliche Techniken sind hier Eigengesichter [6] und Bündelgraphen [7].

Diese Verfahren sind nur auf Bilder anwendbar, die ausser dem Gesicht wenig Hintergrund enthalten. In praktischen Szenarien müssen sie durch weitere Komponenten ergänzt werden, die aus Bildern oder Videose-

quenzen für Erkennung oder Identifikation geeigneten Teilbereiche herauszufiltern. Ein solches System, dessen Kern die Bündelgraphentechnik ist, ist in [2] beschrieben.

In dieser Einführung wurden grob die Probleme umrissen, die bei jedem Gesichtserkennungssystem gelöst werden müssen. Gegenwärtig gibt es mehrere konkurrierende Verfahren, die das Schwergewicht auf die eine oder andere Anforderung legen. Es dürfte deutlich geworden sein, dass ein System zum praktischen Einsatz eine komplexe Kombination mehrerer Verfahren sein muss, und seine Gesamtqualität nur mit sehr langwierigen Testreihen in echten Umgebungen festgestellt werden kann.

Unabhängige Leistungsuntersuchungen

Da Software zur Personenerkennung normalerweise nicht öffentlich verfügbar ist, die Leistungsfähigkeit aber von einer Unzahl von Details abhängt, sind nach wissenschaftlichen Standards objektive Leistungsmessungen derzeit kaum zu erreichen. Die Verfügbarkeit von Gesichtsdatenbanken macht es möglich, dass verschiedene Entwicklergruppen ihre Algorithmen auf ein und denselben Datensatz testen. Dies behebt die Schwierigkeit, die Leistung eines Algorithmus zu bewerten nur unvollkommen, da im Laufe der Entwicklung viele kleine Entscheidungen gefällt und Parameter optimiert werden. Dadurch wird der Algorithmus im Laufe der Entwicklung wissentlich oder unbewusst darauf optimiert, mit den bekannten Daten gut zu funktionieren. Die Erkennungsraten fallen bei Anwendung auf neue Daten teilweise drastisch.

Eine Anstrengung, diese Probleme für den Fall der Personenidentifikation aus Gesichtsbildern zu lösen, wurde von dem US-amerikanischen Verteidigungsministerium (DoD) in den Jahren 1993 bis 1998 unternommen. Im Rahmen des »Counterdrug Technology Development Program« wurde eine Datenbank von 14126 Gesichtsbildern von 1199 Personen erstellt. Ein kleiner Teil der Datenbestände wurde verschiedenen For-

scherguppen für die Systementwicklung zur Verfügung gestellt. Nach abgeschlossener Entwicklung wurden die Systeme in kontrollierter Weise auf die Gesamtdaten angewandt und die Ergebnisse von einer unabhängigen Stelle ausgewertet [4,9].

Um die verschiedenen Modalitäten so gut wie möglich abzubilden, wurden die Testbilder eingeteilt in solche, die am gleichen Tag wie das Datenbankbild derselben Person aufgenommen wurden, und zwar mit identischer (FB) bzw. veränderter Beleuchtung (FC), Bilder die in mehreren Tagen Abstand (duplicate I) und mit mindestens einem Jahr Abstand (duplicate II) zu den Datenbankbildern aufgenommen wurden.

Das erste Ergebnis der Studie war, dass die meisten Systeme überhaupt nicht in der Lage waren, das Korrespondenzproblem zufriedenstellend zu lösen. Daher wurde ein vereinfachter teilautomatischer Test angeboten, bei dem zusätzlich zu den Bildern die handmarkierten Augenpositionen gegeben waren. Die Erkennungsraten in diesem Test variierten in folgenden Bereichen FB: 87% – 97%; FC: 33% – 82%; duplicate I: 33% – 60%; duplicate II: 9% – 54%.

Am praxisnahen vollautomatischen Test ohne handmarkierte Zusatzinformation haben überhaupt nur zwei Forschungsgruppen teilgenommen, und zwar ein Team vom MIT und ein gemeinsames von der Universität Bochum und der University of Southern California in Los Angeles. Deren Ergebnisse sind: FB: 87%, 95%; duplicate I: 50%, 67%. Die eigene Eitelkeit verbietet es zu verschweigen, dass die jeweils besseren Werte von dem an der Ruhr-Universität Bochum und USC gemeinsam entwickelten Verfahren erreicht wurden. Die Werte der vollautomatischen Tests für die schwierigen Fälle FC und duplicate II werden in der Studie nicht genannt.

Über die einfachere Verifikationsaufgabe wird in [3] berichtet, dass bei einer Einstellung der Erkennungsschwelle auf 2% »falsch positiver« Entscheidungen folgende Fehlerraten gemessen wurden: FB: 0,4%; FC: 9%; duplicate I: 11%; duplicate II: 43%. Das zeigt die Leistungsfähigkeit in nicht

sicherheitskritischen Bereichen auf, wo 2% Durchlässe unter falschen Voraussetzungen nicht bedrohlich sind. Anders ausgedrückt: geht man davon aus, dass pro Tag 10000 Zugänge durch Verifikation kontrolliert werden, von denen 100 Betrugsversuche sind, so werden – nach dem Stand der Technik von 1996 – zwei der Betrugsversuche gelingen und ca. 1000 Personen abgewiesen werden. Dies ist kein akzeptables Ergebnis für ein vollautomatisches System.

Alle Ergebnisse des Tests zeigen, dass Gesichtserkennung bei kurz hintereinander im gleichen Raum mit der gleichen Kamera und der gleichen Beleuchtung aufgenommen Bildern sehr gut funktioniert. Das Problem der Beleuchtungsvariation ist technisch völlig ungelöst. Das gleiche gilt für die wenig kontrollierbaren Veränderungen in Gesichtern, die sich im Laufe der Jahre ergeben. Die menschliche Erkennung ist durch eine Unmenge von Erfahrung optimiert, über diese Veränderungen hinwegzusehen und Personen invariant zu erkennen. Für das Computersehen bleibt hier ein sehr weites Forschungsfeld zu bearbeiten.

Als Beispiel eines direkten Praxis-tests sei noch das Beispiel eines installierten Überwachungssystems in der Stadt Tampa in Florida angeführt. Die Amerikanische Bürgerrechtsvereinigung (ACLU) berichtet in einer kürzlich erschienenen Veröffentlichung [5], dass dieses System dazu gedacht war, bekannte Verbrecher auf Videofilmen von Straßen und öffentlichen Plätzen zu identifizieren. Die Erkennungsprotokolle sind nach amerikanischem Recht öffentlich, und die Ergebnisse werden von der ACLU wie folgt zusammengefasst:

Das System aus mehreren Dutzend Kameras wurde am 29.06.2001 installiert. Es hat kein einziges der gespeicherten Gesichter von Verdächtigen korrekt wiedererkannt, geschweige denn zu einer Verhaftung geführt. Es wurde am 11.08.2001 abgeschaltet und wurde seither nicht mehr benutzt. Während der Laufzeit hat es sehr viele »falsch positive« Meldungen produziert, einschließlich der – für Menschen eindeutig erkennbaren – Verwechslung von Frauen und Männern. (vgl. [5])

Natürlich ist unbekannt, wie viele der Gesuchten tatsächlich jemals an der Kamera vorbeigekommen sind, aber es darf doch geschlossen werden, dass das System noch nicht ganz praxisreif war. Die Verwechslung von Männern und Frauen weist auch auf die Tatsache hin, dass die Funktionsweise technischer Gesichtserkennung sich sehr stark von der menschlichen unterscheidet.

Diskussion

Wie im ganzen Gebiet des Computersehens fallen derzeitige Systeme zur automatischen Personenerkennung noch sehr weit hinter dem technisch wünschenswerten zurück. Insbesondere der Einsatz im Freien oder in Räumen mit nennenswerten Fensterflächen muss heute noch am Problem der Beleuchtungsvariation scheitern. Für dessen Lösung ist mehr Rechenleistung oder einfache Systemoptimierung nicht ausreichend, vielmehr bedarf es deutlicher Durchbrüche in der Methodik. Systeme zur Verifikation, d.h. zur Überprüfung einer behaupteten Identität, haben wohl den höchsten Reifegrad erreicht. Dennoch sind sie für einen vollautomatischen Einsatz höchstens bedingt geeignet.

Die oben zitierten Zahlen sprechen eine deutliche Sprache. Sie belegen, dass automatische Gesichtserkennung eine aufstrebende Technologie

ist, die in den vergangenen Jahren beachtliche Erfolge verzeichnen konnte. Andererseits ist sie noch weit davon entfernt, unter realen Bedingungen robust zu funktionieren.

Zweifellos sind die Erkennungssysteme in den seit dem FERET-Test vergangenen Jahren deutlich verbessert worden. Verlässliche Zahlen hierzu liegen nicht vor, da ein guter Teil der Optimierungen von Firmen an eigenen Systemen gemacht werden, die unabhängigen Tests erst nach Kauf zugänglich sind. Ergebnisse von neueren unabhängigen Tests sind meines Wissens nicht publiziert.

Für die Diskussion über die Einführung von Biometriesystemen sind diese Resultate zweischneidig. Einerseits dürfte klar sein, dass derzeit nur wenig Vertrauen in Gesichtserkennungssysteme gesetzt werden sollte. Andererseits wäre es falsch, die notwendige gesellschaftliche Diskussion um die Abwägung zwischen Privatsphäre und Sicherheit mit Hinweis auf mangelnde Funktionsfähigkeit zu vertagen. Ich habe nur sehr geringe Zweifel daran, dass diese Funktionsfähigkeit weiter rapide ansteigen wird. Wenn leistungsfähige Personenerkennungssysteme überall preisgünstig zu haben sind, könnte es leicht zu spät sein darüber nachzudenken, ob, wo und unter welchen Umständen die Bürger sie haben wollen.

Literatur

- [1] M. Lades, J. C. Vorbrüggen, J. Buhmann, J. Lange, C. von der Malsburg, R. P. Würtz und W. Konen. Distortion invariant object recognition in the dynamic link architecture. *IEEE Transactions on Computers*, 42(3):300–311, 1993.
- [2] H. S. Loos. Suchbilder – Computer erkennt Personen in Echtzeit. *c't*, (15):128–131, 2000.
- [3] P. J. Philips, A. Martin, C. Wilson und M. Przybicki. An introduction to evaluating biometric systems. *IEEE Computer*, 33(2):56–63, 2000.
- [4] P. J. Philips, H. Moon, S. A. Rizvi und P. J. Rauss. The FERET evaluation methodology for face-recognition algorithms. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(10):1090–1104, 2000.
- [5] J. Stanley und B. Steinhardt. Drawing a blank: The failure of facial recognition technology in Tampa, Florida. Technischer Bericht, American Civil Liberties Union, 2002. http://www.aclu.org/issues/privacy/drawing_blank.pdf.
- [6] M. Turk und A. Pentland. Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1):71–86, 1991.
- [7] L. Wiskott, J.-M. Fellous, N. Krüger und C. von der Malsburg. Face recognition by elastic bunch graph matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(7):775–779, 1997.
- [8] R. P. Würtz. Object recognition robust under translations, deformations and changes in background. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(7):769–775, 1997.
- [9] Zur Gesichtsdatenbank und dem FERET-Test siehe: <http://www.dodcounterdrug.com/facialrecognition/Feret/feret.htm>

Thilo Weichert

Videoüberwachungsregelung auf dem Prüfstand

Betroffenheit

Man kann über Statistiken verschiedener Meinung sein, glauben muss man – einem Sprichwort folgend – an ihre Richtigkeit nur, wenn man sie selbst gefälscht hat. Doch ist es auch eine Erfahrung jedes Datenschützers, dass sich Sensibilität für Überwachungsmaßnahmen erst einstellt, wenn man selbst direkt betroffen ist. Dass Frei-

heit auch immer die Freiheit des anderen ist, trifft zwar die historische Erfahrung, nicht aber die Befindlichkeit der Menschen. Und so kommt folgenden Zahlen wohl eine gewisse Aussagekraft zu: Nach einer Umfrage im Auftrag des *Spiegels* eine Woche nach dem Terroranschlag in den USA am 11.09.2001 antworteten von ca. 1000 Befragten auf die Frage: »Welche

Einschränkungen wären Sie bereit hinzunehmen?« 67% positiv auf den Vorschlag: »Umfassende Videoüberwachung von öffentlichen Straßen und Plätzen«. Nur 30% waren dagegen.¹ Kurz zuvor hatte Prof. Opaschowski im Auftrag der Datenschutzbeauftragten zum zweiten Mal

1. Der Spiegel 39/2001, 31.

eine etwas differenziertere repräsentative Umfrage zur Videoüberwachung bei 2000 Personen durchgeführt. Danach meinten im Jahr 2001 75% der Befragten, Überwachungskameras seien »in Ordnung«. 1998 waren es noch 83%. Nur 9% waren grundsätzlich gegen Videoüberwachung. 50% sprachen sich für Videoüberwachung der Innenstädte durch die Polizei aus; nur noch 29% hielten es für richtig, wenn mehrere Kameras ihren Weg durch die Innenstadt mitverfolgen. Während ältere Menschen dieser Kontrollmaßnahme eher positiv gegenüber standen, waren Junge kritischer als der Durchschnitt.² Die Botschaft dieser Umfrage bestätigt die Eingangsthese: Je näher technische Überwachung einem selbst auf die Pelle rückt, desto weniger ist man von ihr begeistert.

Doch wird das Feld der öffentlichen Meinung gut bestellt: Mit jedem spektakulären Angriff auf die öffentliche Sicherheit kann die Bereitschaft zur Hinnahme von Überwachung gesteigert werden. In Großbritannien – dem El Dorado für Videoüberwacher – waren dies der blutige Bombenanschlag auf das Londoner Kaufhaus Harrods 1983, die Entführung und Ermordung des kleinen James Bulger im Jahr 1993 und die Anschläge irischer Terroristen.³ Ob in Deutschland die Anschläge auf World Trade Center und Pentagon in den USA einen ähnlichen Effekt auslösen werden, wird sich noch erweisen. Jedenfalls wird die Videoüberwachung nunmehr als adäquates Mittel zur Verhinderung terroristischer Anschläge angepriesen. Dass es damit nicht weit her ist, erweisen die Erfahrungen in Großbritannien, wo die Kriminalität nicht, geschweige denn der Terrorismus damit zurück gedrängt werden konnte. Eine rationale Einschätzung einer Überwachungsmaßnahme setzt voraus, den Umfang der Überwachung und dessen gesellschaftliche Wirkungen einschätzen zu können. Mehr Transparenz ist hierfür nötig. Während jedoch das Dickicht der Kameraüberwachung immer unüber-

sichtlicher wird, bleiben die Aufklärungsmaßnahmen hierüber auf der Strecke. Die Chance, dies ein wenig zu verändern, wurde mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) im Frühjahr 2001 vorläufig vertan.

Gesetzgebung

Bis zum 23.05.2001 war die seit mehr als 40 Jahren praktizierte Methode Kameraüberwachung⁴ gesetzlich weitgehend ungeregt. Dieser Zustand war bei dieser geradezu klassischen Methode zur Enteignung des Rechts auf informationelle Selbstbestimmung absolut unbefriedigend. Der Rückgriff auf das Kunsturhebergesetz aus dem Jahr 1907 und auf das Recht am eigenen Bild als Konkretisierung des allgemeinen Persönlichkeitsrechtes war angesichts der Entwicklung der Videotechnik und deren Einsatzfelder nicht mehr hinnehmbar. Die Datenschutzbeauftragten meldeten daher Regelungsbedarf an, dem niemand widersprechen konnte. Einige Landesgesetzgeber hatten schon früher diese Maßnahme in ihren Datenschutz- und Polizeigesetzen vorgesehen. Doch fehlte es weiterhin an einer Leitnorm auf Bundesebene und einer Eingrenzung in dem besonders problematischen Bereich der Privatwirtschaft.

Bei der Debatte um die Novellierung des Bundesdatenschutzgesetzes (BDSG) ergab sich die Notwendigkeit einer Reform in zwei Stufen. Von Anfang an war die Regelung der Videoüberwachung in der ersten Stufe im Gespräch. Doch enthielten die Entwürfe bis ins Jahr 2000 hinein keine adäquate Antwort auf diese Diskussion. Insbesondere Bündnis 90/Die Grünen, die schon 1997 einen Vorschlag im Bundestag eingebracht hatten,⁵ drängten gemeinsam mit den Datenschutzbeauftragten⁶ für eine Aufnahme. Erst nachdem praktisch sämtliche anderen Punkte der BDSG-

Novelle geklärt schienen, zeigte der Gesetzgeber im Sommer 2000 die Bereitschaft zu einer Berücksichtigung in der ersten Stufe.⁷ Das neue BDSG trat am 23.05.2001 mit einer Videoregelung in § 6b in Kraft.⁸ Sie zwingt zu einer Totalrevision der bisherigen Überwachungspraxis. Die Überwachungszwecke müssen präzise festgelegt werden. Es muss ein Hinweis in der Öffentlichkeit erfolgen. Nur in begründeten Sicherheitsfällen ist eine Zweckänderung zulässig. Im Fall der Identifizierung von Einzelpersonen sind diese zu benachrichtigen. Eine frühestmögliche Löschung wurde zur Pflicht. Dessen ungeachtet hat sich kurzfristig keine wesentliche Veränderung in der Praxis feststellen lassen. Dies gilt v.a. für die Pflicht zum Kenntlichmachen (§ 6b Abs. 2 BDSG). Dieses Vollzugsdefizit liegt nicht nur an der mangelnden Bekanntgabe des neuen BDSG allgemein und dessen § 6b im Speziellen.⁹

Vollzugsdefizit: Hinweispflicht

Das feststellbare Vollzugsdefizit ist wohl zu erklären mit bisher ungenügenden Kontrollen durch die Datenschutz-Aufsichtsbehörden. Eine Ursache mangelnden Respekts vor der Hinweispflicht liegt aber sicher auch daran, dass die Betreiber bei einem Verstoß keine spürbaren Sanktionen befürchten müssen. Tatsächlich hat der Gesetzgeber vergessen, den Verstoß gegen § 6b Abs. 2 BDSG in den Bußgeldkatalog des § 43 BDSG aufzunehmen. Dies ist angesichts der späten Einfügung der Regelung nicht verwunderlich und angesichts der überkomplexen Gesetzestechnik beileibe nicht der einzige handwerkliche Fehler im neuen BDSG. Die Aufsichtsbehörden können lediglich das Anbringen von Hinweisen auf die Videoüberwachung als eine technisch-organisatorische Maßnahme nach § 9 BDSG, um »den besonderen Anforderungen des Datenschutzes gerecht« zu werden, nach § 38 Abs. 5 BDSG anordnen. Fehlen also Schilder mit den

2. Opaschowski, Der gläserne Konsument, Die Zukunft von Datenschutz und Privatsphäre in einer vernetzten Welt, Hamburg 2001.

3. DatenschutzNachrichten (DANA) 1/1999, 6.

4. Zur Geschichte ausführlich: Deutsche Vereinigung für Datenschutz (DVD, Hrsg.), Videoüberwachung, DANA-Sonderheft 3/4-1988, 7 ff.

5. §33 des Entwurfs v. 14.11.1997, BT-Drs. 13/9082.

6. Entschließungen der DSB-Konferenz, z.B. 54. v. 23./24.10.1997 od. 59. v. 14./15.03.2000, 18. TB BfD S. 21 f., 26, 112 f., 223 f.

7. Mein dort vorgestellter Regelungsvorschlag ist abgedruckt in DuD 2000, 669.

8. BGBl. I 2001, S. 909 f.

9. Dazu kritische DVD-PE, DANA 2/2001, 2.

gesetzlich geforderten Hinweisen auf Videoüberwachung, so kann deren Installation per Verwaltungsakt durchgesetzt werden.

Nicht nur der Vollzug des § 6b BDSG ist ein Problem, sondern auch die Regelung selbst. Diese weist insbesondere folgende zwei Defizite auf: 1. die uferlose Weite der Erlaubnistatbestände und 2. der Verzicht auf die Meldepflicht.

Die Legitimation durch mehr als Sicherheit

Nach § 6b Abs. 1 legitimieren die »Aufgabenerfüllung«, das »Hausrecht« oder »berechtignte Interessen für konkret festgelegte Zwecke« den Kameraeinsatz. Insbesondere die beiden letztgenannten Begriffe sind derart weit, dass mit ihnen keine vernünftige rechtsstaatliche Begrenzung vorgenommen werden kann. Als zusätzliche Anforderung muss daher verlangt werden, dass die Videoüberwachung der »Gewährleistung von Sicherheit« dient.¹⁰ Bis heute konnte niemand ein Beispiel für eine legitime Videoüberwachung vortragen, das nicht auf den Schutz von subjektiven Rechten, also v.a. den Schutz von Personen und Sachen ausgerichtet wäre. Egal, wer für die Maßnahme verantwortlich ist: Polizei, öffentliche Stellen, private Sicherheitsdienste, Bahnabfertigungsdienste, Ladenbesitzer – in jedem Fall ist Voraussetzung für die Videoüberwachung, dass gesetzlich geschützte Güter vor Schaden bewahrt oder eine erfolgte Schädigung verfolgt und sanktioniert werden sollen. Notwendige und zugleich hinreichende Voraussetzung ist schon heute, dass als Zweck »Sicherheit« angestrebt wird. Die Regelung des § 6b fordert für jeden einzelnen Kameraeinsatz eine Abwägung mit den schutzwürdigen Belangen der Betroffenen. Im Rahmen einer grundrechtskonformen Auslegung dieser Norm reduziert sich die Zulässigkeit auf diesen Zweck. Dass dies nicht so im Gesetz steht, hat die ärgerliche Folge, dass weitergehende Gelüste bei den Videosystem-Produzenten und -Betreibern geweckt werden, die diese

auch in ihren Hochglanzbroschüren offen präsentieren. Derartige Wünsche können aber bei einer datenschutzrechtlichen Auslegung des § 6b Abs. 1 BDSG nicht befriedigt werden dürfen.

Kontrollfragen können dies verdeutlichen: Soll die »Aufgabenerfüllung« z.B. der Bundeswehr es legitimieren, à la »Cityserver«¹¹ die gesamte Bundesrepublik zu videokartieren? Soll der Umstand, dass das »Hausrecht« in einer öffentlichen Ladenpassage bei einem privaten Unternehmer zur Kamerakontrolle genügt, die Aufnahme von Passanten per Webcam und die Übertragung dieser Bilder über das Internet für Werbezwecke legitimieren? Den buntesten Vogel schoss der Gesetzgeber mit dem Versuch der Eingrenzung der erkanntermaßen weiten »berechtignten Interessen« ab durch die Forderung nach deren »konkreten Festlegung«. Wo wird der Zweck »festgelegt«? Jedenfalls nicht bei einer Meldung gegenüber der Datenschutz-Aufsichtsbehörde, denn diese hat der Gesetzgeber unterschlagen! »Werbung« ist ebenso ein berechtigtes Interesse wie z.B. »Spaß haben«. Die Betreiber sind die einzigen, die zunächst die Abwägung vornehmen müssen. Diesen werden noch viele andere »berechtignte Interessen« einfallen, die sie dann konkret im Geheimen »festlegen«!

Videoüberwachung erfolgt nicht gezielt personenbezogen, sondern raumbezogen. Sie ist aber – deshalb ist sie grundrechtsrelevant – mit mehr oder weniger großem Aufwand personenbeziehbar. Die Zwecke bleiben vage. Dies hat zur Folge, dass in einer noch nicht direkt personenbezogenen Form massenhaft Daten auf Vorrat erhoben und oft genug auch gespeichert werden. Diese durch Technikeinsatz verursachte Gefährdungslage für das Persönlichkeitsrecht bedarf der Rechtfertigung durch eine Gefährdungslage für andere Rechte. Und präzise diese Gefährdungslage kann mit dem Terminus »Gewährleistung von Sicherheit« eingegrenzt werden.

Für eine Meldepflicht

Eine noch größere Sünde als bei der materiellen Regelung in Absatz 1 beging der Gesetzgeber mit seinem Verzicht auf die Meldepflicht. Selbst die Datenschutzbeauftragten des Bundes und der Länder verwarfen diesen Vorschlag als nicht praktikabel. Dem gegenüber müssten eigentlich die Gründe für eine Meldepflicht überzeugen.¹²

Es sollte doch ein generelles Datenschutz-Anliegen sein, flächendeckende Videoüberwachung öffentlicher Räume schon im Ansatz zu verhindern. Dies lässt sich allein mit materiell-rechtlichen Regelungen nur unzureichend bewirken. In Anknüpfung an das Transparenzgebot der EU-DSRL kann hier der demokratische Meinungsbildungsprozess wirksam gemacht werden. Um diesen in Gang zu setzen, müssen die BürgerInnen die Möglichkeit erhalten, sich auf dem Weg über die Nachfrage bei der verantwortlichen Stelle oder bei der zuständigen Datenschutzkontrollinstanz genauere Informationen über die Überwachung zu beschaffen.

Die besondere gesamtgesellschaftliche Gefahr von Überwachung liegt darin, dass es durch deren technische Qualität und Vernetzung sowie durch deren quantitative Zunahme zumindest in den besonders von Menschen frequentierten Ballungsräumen immer weniger unbeobachtete Räume gibt. Dies kann bis zu einer allgegenwärtigen technischen Beobachtung führen. Eine solche Überwachungsinfrastruktur wäre nach der geltenden Rechtsprechung des Bundesverfassungsgerichtes verfassungswidrig. Unabhängig davon, dass es für die jeweiligen einzelnen Kameraeinsätze eine gute Begründung geben kann, muss eine Gesamtbewertung vorgenommen werden können. Als übergreifendes Frühwarnsystem und zur Überprüfung der Normeffizienz der Befugnisregelung könnte mit Hilfe der Meldepflicht ein Überblick über das gesamte Ausmaß der Überwachung hergestellt werden. Dieser Überblick kann den Parlamenten als Entscheidungslage zur Verfügung gestellt werden. Zugleich könnten damit Anfragen von

10. Weichert DuD 2000, 666 f.

11. Vgl. DANA-aktiv 1/1999, DANA 2/1999, 29 ff, 52.

12. Aus DuD 2000, 667 f.

besorgten BürgerInnen oder Beschwerden kurzfristig und kompetent beschieden werden. Die Datenschutzkontrollinstanzen sind zumeist gesetzlich verpflichtet, regelmäßig Tätigkeitsberichte zu veröffentlichen (z.B. § 26 Abs. 1 BDSG) sowie zu Fragen des Datenschutzes zu beraten (z.B. § 26 Abs. 2, 3 BDSG). Das Rohmaterial hierfür kann aus den Meldungen erlangt werden.

Durch eine Anzeigepflicht wird der Betreiber einer Videoanlage dazu angehalten, im Einzelfall eine Interessenabwägung durchzuführen. Die Vorabkontrolle (Art. 20 EU-DSRL; § 4d Abs. 5 BDSG) sowie Anzeige- und Veröffentlichungspflichten (Art. 21 EU-DSRL) zwingen den Betreiber vor Einrichten eines Überwachungssystems zu einer rationalen Begründung der konkreten Erforderlichkeit. Im Rahmen der Vorabkontrolle muss ein Sicherheitskonzept erstellt werden. Wird dies unterlassen und erscheint die Anzeige der Datenschutzbehörde aus datenschutzrechtlichen Gründen problematisch, so kann und wird diese den Einsatz überprüfen und u.U. beanstanden.

Dem Vorschlag einer Meldepflicht wird nun entgegengehalten, der dadurch verursachte Aufwand sei übermäßig und die bürgerrechtlich positiven Wirkungen seien nicht einschätzbar. Tatsächlich hat die notorische personelle Unterbesetzung und die Mittelknappheit bei den Datenschutz-Aufsichtsbehörden zur Folge, dass diese mit ihren Ressourcen so effektiv wie möglich haushalten. Zugegeben ist auch, dass datenschutzrechtliche Registrier- und Meldepflichten bisher hohen Aufwand und wenig bürgerrechtlichen Nutzen brachten. Dieser hohe Aufwand bei ungenügendem Nutzen sämtlicher bisherigen Meldepflichten basierte u.a. darauf, dass nicht die technischen Möglichkeiten genutzt wurden, die im Interesse von Transparenz und Bürgerrechtsschutz möglich wären.

Wer den Aufwand und die Kosten der Installierung einer Videokamera nicht scheut, den dürfte der Zusatzaufwand des Ausfüllens und des Versendens eines Formulars nicht schrecken, in dem lediglich folgende Angaben gemacht werden müssen: Name und Adresse des Betreibers der Stelle

und bzw. des Verantwortlichen, Standort, Zweck, Schwenk- und Zoombarkeit, Vernetzung (Datenempfänger), automatisierte Auswertungsformen, Dauer der Bildaufbewahrung. Diese Angaben können in einem Online-Formular eingetragen und elektronisch versandt werden. Dieser Arbeitsaufwand kostet den Betreiber pro Kamera keine 10 Minuten. Sicherheitsanforderungen (z.B. bzgl. Verschlüsselung) müssen beim Versand der Meldungen keine gestellt werden, da hier keine geheimen oder vertraulichen Daten mitgeteilt werden. Die Verwendung digitaler Signaturen wäre hierbei wünschenswert, ist aber auch nicht dringend nötig. Die Aufsichtsbehörden können die per Email erhaltenen Meldungen einfach sammeln und online im Internet zum Abruf zur Verfügung stellen. Der dabei entstehende Aufwand könnte bei kluger technischer Gestaltung für den Einzelfall fast auf Null reduziert werden. Will eine Aufsichtsbehörde einen zusätzlichen Nutzen bewirken, könnte sie eine – auch weitestgehend automatisiert erfolgende – Auswertung bereitstellen: z.B. eine Straßenkarte der betroffenen Gemeinden und Städte, auf der sämtliche Kamerastandorte verzeichnet sind.

Wir hätten es dabei mit einer Privacy Enhancing Technologie (PET) ganz neuen Types zu tun. Notwendig wäre lediglich dessen einmalige programmtechnische Entwicklung, die von allen Aufsichtsbehörden genutzt werden könnte und im Interesse der Einheitlichkeit für alle Seiten auch sollte. Solange noch nicht alle Anwender von Video-Technologie Internet-Technologie nutzen, müsste wohl kurzfristig auch eine konventionelle Form der Meldung zugelassen werden, die einen – bewältigbaren – zusätzlichen Aufwand durch die manuelle Erfassung bei den Aufsichtsbehörden auslösen würde.

Ausblick und Überblick

Der wesentliche rechtliche Aspekt bei der normativen Einhegung von Videoüberwachung muss darin gesehen werden, dass Videoüberwachung das Pilotprojekt für die anlasslose technische Überwachung potenziell der gesamten Bevölkerung ist. Ähnliche

Begehrlichkeiten werden derzeit schon im Hinblick auf die Internet-Überwachung geäußert, wenn ernsthaft die Totalspeicherung aller Netzaktivitäten für eine Dauer von 6 Monaten oder gar von 7 Jahren gefordert wird.¹³ Selbst im Bereich der Gentechnik erdreisten sich PolitikerInnen, Datenbestände der gesamten (männlichen) Bevölkerung zu fordern.¹⁴ Die Terroranschläge in den USA brachten nun die Forderung des Fingerabdrucks auf Ausweisen und damit zwangsläufig eine zentrale Fingerabdruckdatei für alle BundesbürgerInnen. Angesichts zunehmender Videoüberwachung sollten sich die Überwachungspolitiker überlegen, ob es vielleicht nicht noch raffinierter wäre, eine bundesweite Bild- bzw. Gesichtsdatenbank aufzubauen ...

Will (bzw. muss) man sich diesem Ansinnen der anlass- und kontextlosen potenziellen Totalüberwachung und den damit verbundenen informationellen Grundrechtseingriffen auch nur in kleinen Ansätzen beugen, so bedarf es eines verfahrensrechtlichen Korrektivs. Bei der Videoüberwachung ist dieses Korrektiv die Melde- und Publikationspflicht nach dem Motto: »Beobachtet die Beobachter«.¹⁵

Ob die Verabschiedung des ungenügenden § 6b BDSG mehr Schaden als Nutzen bewirkt, wird die nahe Zukunft zeigen. Die gesellschaftliche Diskussion über Videoüberwachung in Anbetracht der Gefahren unserer Risikogesellschaft wie auch der Grad der technischen Entwicklung bei dieser Technik verdeutlichen uns, dass wir uns aktuell an einem wichtigen Scheidepunkt befinden. Der § 6b kann und darf nur ein Einstieg in eine umfassendere Regulierung der Videoüberwachung sein, die über die Rudimente des Kunsturhebergesetzes und des Bürgerlichen Gesetzbuches hinausgeht. Die Regelung muss zweifellos in einer zweiten Stufe der BDSG-Novellierung nachjustiert werden. Dabei sind sowohl materielle (Beschränkung auf »Sicherheit«) wie auch verfahrensrechtliche (Melde- und Publikationspflichten) Verbesserungen geboten.

13. Weichert DANA 2/2001, 7, 10.

14. Schnorr ZRP 2001, 292.

15. Vgl. Batt DANA 3/2001, 8 ff.

Rena Tangens und padeluun

Kameraverhalten

Kameraüberwachung schadet der Demokratie

Anfang der 80er Jahre hatte Datenschutz einen hohen Stellenwert im öffentlichen Bewusstsein: George Orwells negative Utopie »1984« gehörte zum allgemeinen Lesestoff und es gab breiten Widerstand gegen die Volkszählung vom Boykott bis hin zur Verfassungsklage. Das Urteil des Bundesverfassungsgerichtes (»Volkszählungsurteil«) von 1983 war wegweisend und eine der Grundlagen für ein anerkannt gutes Datenschutzgesetz in Deutschland. In der öffentlichen Wahrnehmung scheint das Bewusstsein für Datenschutz und Privatsphäre seither abgenommen zu haben. Tatsächlich aber registrieren Wirtschaftsstudien etwa 10% »Datenbewusste«, die aus Sorge vor missbräuchlicher Speicherung und Verwendung ihrer Daten die Nutzung bestimmter Technologien, Dienste und Angebote verweigern. Prognosen von elektronischen Diensteanbietern gehen davon aus, dass der Anteil datenbewusster Menschen innerhalb der nächsten Jahre auf 20% steigen wird. Dies sind vermutlich auch diejenigen, die sich der Selbstenttäußerung beim Nutzen öffentlicher Räume entziehen wollen: Sie wollen nicht auf Schritt und Tritt von Kameras beobachtet werden.

Kameraüberwachung schadet der Demokratie im gleichen Maße, wie dies mangelnder Datenschutz im Generellen tut. Die Zauberformel, die rückwärtsgesprochen »Gnummit Sebt s'bles elle noitam Rofni« lautet und auch in richtiger Richtung gesprochen immer noch sehr kompliziert »Informationelle Selbstbestimmung« lautet ist ein Schlüssel zum Verständnis. Auch zum Verständnis darüber, dass es eigentlich gar keiner Erklärungen bedarf.

Informationelle Selbstbestimmung

Das Thema »Datenschutz und informationelle Selbstbestimmung in der Demokratie« erhält immer wieder neue Bedeutsamkeit und Aktualität:

- Es werden von der Politik neue Maßnahmen ergriffen, neue Gesetze erlassen – insbesondere seit dem 11. September 2001 – die die informationelle Selbstbestimmung einschränken.
- Das Spannungsfeld zwischen Freiheit und Sicherheit wird neu ausgelotet.
- Die digitale Technik entwickelt sich weiter.
- Kameraüberwachung weitet sich aus.
- Viele Dienstleistungen werden digitalisiert.
- Individualisiertes Direktmarketing, Kundenkarten, bargeldloses Zahlen per Kreditkarte etc. sind auf dem Vormarsch.
- Es gibt eine starke Zunahme vorgeblicher »Gratis«-Angebote, die indirekt durch Preisgabe persönlicher Daten und das Betrachten von Werbung bezahlt werden (z.B. Freemailer).
- Es erfolgt eine detaillierte Auflistung und Speicherung vieler Vorgänge und Services, die vor einigen Jahren noch keine solche Datenspur verursachten (z.B. Telefon, Rabattmarken, Kundenkarten) oder die es noch gar nicht gab (z.B. Handy). All dies hat Einfluss auf das Leben jedes / jeder einzelnen – und auf das Zusammenleben in der Gemeinschaft.

Wo liegt das Problem?

Industrielle Vernetzung: Dampfmaschinen auf Rädern durchfahren das Land. Gerne wird das Eisenbahnzeitalter herangezogen, wenn es gilt, Kri-

tik an neuer Technik ins Lächerliche zu ziehen. Angst vor der zu hohen Geschwindigkeit sollen die Menschen gehabt haben. Es gab aber andere, realere Gefahren: Der sehr lange Bremsweg führte zu Sicherungsmaßnahmen und Gesetzen, die Unfälle vermeiden sollen. Zum Beispiel hat kraft des Gesetzes Schienenverkehr Vorrang vor anderem Verkehr. Ein ausgeklügeltes System aus Schranken, Halbschranken, Blinklicht und Signalisierungssystemen nebst Vorschriften verhindert Kollisionen mit den Schienenweg kreuzenden Pferdefuhrwerken und – heute – Autos.

Klar. Solche Unfälle können tödlich sein – oder tun zumindest sehr weh. Die Gefahr war also direkt erkennbar. Schwerer ist die Gefahr beim elektrischen Stromnetz zu vermitteln. Strom ist unsichtbar und Kindern muss sehr nachdrücklich gesagt werden, dass sie auf gar keinen Fall mit Gegenständen in der Steckdose herumkopeln dürfen.

Bei den jetzt modern gewordenen Datennetzen mit den Möglichkeiten der vollautomatischen Datenerhebung, Datenaustausch und Datenverarbeitung ist die Gefahr so unsichtbar, dass Sie sich als Leserin oder Leser dieser Zeilen gerade fragen, ob die obigen Vergleiche nicht allzu sehr an den Haaren herbei gezogen sind, um für bessere Informationsvermittlung zu plädieren. Nun, wenn Sie sich vor Augen halten, dass unmittelbare Lebensgefahr, wie sie die Kollision mit einer rasenden Dampfmaschine darstellt, drastisch genug ist, um sich schützen zu wollen, ist die Lebensgefahr durch Datenmissbrauch schleichend. Ursache und Wirkung treten so gut wie nie unmittelbar zusammen auf. Die Gefahr kann von Menschen also gar nicht so einfach erkannt werden. Deswegen müssen Fachleute hier den mahnenden Finger heben – und aufklärerisch wirken. Es handelt sich um eine schleichende Entwicklung,

deren Wirkungen erst viel später spürbar werden.

»Die Reaktionsfähigkeit komplexer fortgeschrittener Gesellschaften lässt sich in bestimmter Hinsicht mit denen von Fröschen vergleichen. Wirft man eine solche Amphibie experimentell in heißes Wasser, so wird der Frosch dieser unangenehmen Umgebung sofort zu entfliehen versuchen und mit einem Satz heraushüpfen. Setzt man das sensible Tier hingegen behutsam in ein mit Wasser gefülltes Gefäß und erhöht die Temperatur nur ganz allmählich in kleinen Schritten, so wird es die geringfügigen Veränderungen ertragen, sich jeweils an die Erwärmung gewöhnen und schließlich so lange verharren, bis es am Ende zu spät ist. Ein plötzlicher, starker Reiz löst bei Lebewesen als Kontrast der Umgebungsbedingungen, so lernt man daraus, eine starke aversive Reaktion wie Vermeidung durch Flucht oder Aggression aus; wird der Reiz dagegen nur Schritt für Schritt verstärkt, treten Anpassungs- und Gewöhnungseffekte ein, die sich auf längere Sicht ungünstig auswirken.

So ähnlich, ist zu befürchten, verhält es sich mit dem seitens der Obrigkeit zugemuteten Überwachungspegel in den hypermodernen Gesellschaften: Während Orwells Vision »1984« in der öffentlichen Kultur noch vor einer Generation nahezu einhellig als Schreckensbild empfunden und als warnende Dystopie verstanden wurde, ist die technische Infrastruktur zur ubiquitär-panoptischen¹ Ausleuchtung individuellen und kollektiven sozialen Lebens eingangs des 21. Jahrhunderts technisch weitgehend installiert und stößt nur noch sporadisch auf ernsthaften und/oder organisierten Widerstand, der sich im Zweifelsfall jedoch politisch leicht marginalisieren lässt oder in juristische Detailfragen von zugestandenem rechtlichen Einfriedungen abgedrängt wird.«²

Es stellt sich also die Frage: »Wie kann der Frosch über die langsame Erwärmung aufgeklärt werden?« oder »Wie kann die Erwärmung des Wassers gestoppt werden?«

Verletzung der informationellen Selbstbestimmung schadet der Demokratie

Informationelle Selbstbestimmung bedeutet: Jede und jeder hat das Recht, über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Informationelle Selbstbestimmung verhindert, dass Bürgerinnen und Bürger durch faktischen Zwang zu gläsernen und somit manipulierbaren Menschen werden. Eine Informationsverarbeitung, bei der die Bürgerinnen und Bürger nicht mehr wissen, an welcher Stelle welche Daten über sie gesammelt werden, beeinträchtigt nicht nur ihre individuellen Persönlichkeitsrechte, sondern ist auch mit dem demokratischen Rechtsstaat unvereinbar.

Ein Mensch, der ständig beobachtet, registriert, vermarktet und von speziell auf ihn abgestimmten Vorschlägen und Angeboten begleitet wird, verändert mit der Zeit sein Verhalten und richtet es nach den Erwartungen derer aus, die seine Daten auswerten. Individualisierte Manipulationsmöglichkeiten und faktischer Anpassungsdruck führen zu einer zunehmenden Fremdbestimmung.

Damit werden Grundprinzipien unserer Verfassung – die Menschenwürde und das Recht auf freie Entfaltung der Persönlichkeit – beschädigt. Wer sich solcherart beobachtet fühlt, nimmt möglicherweise andere von der Verfassung garantierte Rechte wie freie Meinungsäußerung und Versammlungsfreiheit nicht mehr in Anspruch. So zerstört der Verlust der informationellen Selbstbestimmung die Fähigkeit zur Kommunikation und zur Partizipation. Damit gehen

die Ideen, Meinungen und Talente dieser Menschen nicht mehr in die Allgemeinheit ein und so geht auch das Engagement für etwas, das über die eigenen Interessen hinausgeht, für die Gemeinschaft verloren.

Das bedeutet, dass es nicht mehr nur um individuelle Freiheiten geht, die jeder für sich selbst aushandeln könnte, sondern um nicht verhandelbare Grundrechte, die für das Gemeinwohl und den Fortbestand der Demokratie wichtig sind.

Diese Schlussfolgerungen hat das Bundesverfassungsgericht im sogenannten »Volkszählungsurteil« vom 15. Dezember 1983 ausdrücklich benannt:

»Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten frei-

1. ubiquitär: überall verbreitet, panoptisch: von überall einsehbar; panoptisches System: im Interesse einer zentralen Überwachung angewandte strahlenförmige Anordnung der Zellen mancher Strafanstalten

2. Nogala, Detlef: Der Frosch im heißen Wasser? in: Schulzki-Haddouti, Christiane (Hrsg.): Vom Ende der Anonymität. Die Globalisierung der Überwachung. Hannover: Heise Verlag, 2000, S. 139

heitlichen demokratischen Gemeinwesens ist.«³

Das ist nicht nur Theorie:

- Der Verlust der informationellen Selbstbestimmung beschädigt die persönliche Souveränität und schränkt die Handlungsmöglichkeiten ein.
- Der Verlust der informationellen Selbstbestimmung verringert die Bereitschaft zur Partizipation. Teilhabe der Bürgerinnen und Bürger an der Gestaltung der Gesellschaft aber ist essentielle Voraussetzung für eine lebendige Demokratie.
- Die Bereitschaft, ein öffentliches Amt zu übernehmen, nimmt – wie in den USA bereits zu beobachten – unter diesen Umständen erheblich ab. Denn wer ein politisches Amt oder auch eine aktive Position in einer Nichtregierungsorganisation übernimmt, muss damit rechnen, dass seine / ihre Vergangenheit und Lebensgewohnheiten von politischen Gegnern auseinandergepfückt werden und dabei Daten herangezogen werden, die durch das exzessive Datensammeln vieler unterschiedlicher Stellen entstehen: Einkaufsgewohnheiten durch bargeldloses Bezahlen und durch Kundenkarten, Telefonrechnungen mit Registrierung sämtlicher gewählter Nummern, Reisedaten durch Buchungen und Reservierungen, Bewegungsprofile der Funktelefone, Titel-Liste der ausgeliehenen Videos in der Videothek, Kommunikationsdaten (mit wem wurde wann und wie oft telefoniert oder eMail ausgetauscht), bevorzugte Webseiten im Internet, Krankenakten und Arzneikäufe etc. etc.

Informationelle Selbstbestimmung gerät zur Ware

Privatsphäre darf nicht als Ware betrachtet werden. Privatsphäre ist nicht individuell nach den Regeln des freien Marktes verhandelbar. Die Regulierungskräfte des Marktes funktionieren nur, wenn die Verhandlungspartner gleichberechtigt sind. Faire

Deals werden nur geschlossen, wenn so etwas wie »Waffengleichheit« herrscht. Waffengleichheit beim Verhandeln um die Privatsphäre zwischen Bürger/innen und Institutionen bzw. Firmen oder gar dem Staat aber ist in den meisten Fällen nicht gegeben:

- Es gibt keine ausreichende Information über langfristige Risiken, keine persönliche Kontrolle über Einhaltung der ausgehandelten Regeln.
- Es gibt keine Information über Alternativen.
- Den Milliarden-Werbeetats der Firmen stehen die minimalen Mittel der Verbraucherschützverbände und Bürgerrechtsorganisationen gegenüber.
- Bürgerinnen bzw. Verbraucherinnen haben oft keine andere Wahl als ein bestimmtes Angebot zu akzeptieren.
- Standardeinstellungen sind Politik. Wenn es normal ist, dass Kameras überall sind, dann kann ich mich so gut wie nicht mehr wehren.

Das ist schlicht zu viel Aufwand für Menschen, die das nicht à la Michael Kohlhaas zu ihrer Hauptlebensaufgabe machen wollen. Deshalb werden u.a. allgemein gültige Regeln gebraucht, die beide Seiten einhalten und deren Einhaltung eingefordert werden kann. Mit anderen Worten: Gesetze, die die »Waffengleichheit« fördern. Solche Gesetze wird es nur geben, wenn genügend Menschen sich dafür interessieren und sie fordern.

Informationelle Selbstbestimmung ist keine Ware, sondern ein Menschenrecht – Grundrechte sind nicht veräußerbar! Informationelle Selbstbestimmung ist kein Problem einer Interessengruppe – sondern geht alle an.

Der Verlust der informationellen Selbstbestimmung wird vielerorts als notwendige Begleiterscheinung des technischen Fortschritts, insbesondere der Digitalisierung und der Vernetzung, angesehen, an der man nichts ändern kann. Im Zweifelsfall ist der Terrorismus schuld. Beispielhaft ein Zitat:

»You have zero privacy anyway – get over it.« (sagt Scott McNealy,

Chef des Computerriesen Sun Microsystems, 1999)

Hier können wir eine Parallele zum Umweltschutz feststellen. Umweltverschmutzung wurde lange als unausweichliche Nebenwirkung der Industrialisierung akzeptiert. Dies hat sich geändert. Umweltschutz wird mittlerweile als Sicherung der Lebensgrundlagen auf diesem Planeten begriffen.

Für den Sustainability Fonds – ein Schweizer Fonds für langfristige Geldanlagen – beurteilen Analysten Firmen nach den Kriterien der Nachhaltigkeit. Dazu zählt u.a., wie eine Firma es mit dem Umweltschutz hält, ob sie risikoreiche Technologien einsetzt, wie die Arbeitsbedingungen sind, wie sie ihre Mitarbeiter/innen behandelt, wie sie mit ihren Kund/innen umgeht, wie sie mit ihrer Nachbarschaft, mit Initiativen und der sonstigen Öffentlichkeit kommuniziert. Zukünftig wird wohl auch die Achtung der Privatsphäre der Kund/innen und eine aktive Privacy Policy Rolle spielen bei den Kriterien, nach denen die Nachhaltigkeit eines Unternehmens beurteilt wird. Niemand fühlt sich richtig zuständig für das Thema, insbesondere im Kontext »Demokratie«.

»Informationelle Selbstbestimmung« wird auf »Datenschutz« verkürzt, die Verantwortung wird auf die Datenschutzbeauftragten abgeschoben – ähnlich wie bei den Frauenbeauftragten meint man, damit das Thema abgehakt zu haben. Tatsächlich handelt es sich jedoch um eine Querschnittsaufgabe, die an vielen Stellen berücksichtigt und aktiv angegangen werden muss.

Informationelle Selbstbestimmung ist wichtig für die Demokratie

Jede Demokratie lebt von der Handlungsfähigkeit ihrer Mitglieder, nicht nur bei politischen Entscheidungen, sondern auch im wirtschaftlichen, sozialen, kulturellen und sonstigen Bereichen. Um handlungsfähig zu sein bedarf es nicht nur der erforderlichen Kompetenzen, sondern zuallererst der Bereitschaft zu handeln. Diese ist allerdings nur dann vorhanden, wenn man sich von der eigenen Handlung

3. BVerfGE 65, 1

eine bestimmte Wirkung verspricht, über die man – zumindest bis zu einem gewissen Grade – die Kontrolle hat.

Die Erfahrung, dass infolge meiner Handlungen von mir nicht mehr zu kontrollierende Dinge geschehen – nämlich die Tatsache, dass Daten über mich gesammelt werden und in z.T. völlig willkürlichen Zusammenhang gebracht werden – kann mich nicht nur in meiner Handlungsfähigkeit (ich möchte z.B. etwas auf Raten kaufen, was mir aufgrund mehrerer Umzüge in der letzten Zeit nicht gestattet wird) einschränken, sondern wird auch meine Handlungsbereitschaft auf Dauer untergraben.

Darauf kann ich nun entweder reagieren – wie viele Interessierte dies ja bereits tun – und mich über Möglichkeiten des Schutzes vor Datenraub informieren oder ich werde resignieren – nach dem Motto »die da oben« – und Willkür auf Dauer akzeptieren statt eigene Kompetenz zu entwickeln.

Was ist zu tun?

Es muss ein Bewusstsein dafür geweckt werden, dass die informationelle Selbstbestimmung gefährdet sein kann, auch wenn keine Überwachung (Video-, Telefonüberwachung etc.) stattfindet, und auch wenn keine privaten Geheimnisse ans Licht gezerzt und veröffentlicht werden – einfach durch Sammlung, Speicherung, Kombination, Auswertung und Nutzung von vielen banalen Daten aus dem alltäglichen Leben – die jeweils für sich gesehen keineswegs »geheim« sind. Diese Daten können durch Speicherung, Akkumulation und Auswertung zu einem weitreichenden Persönlichkeitsprofil zusammengestellt werden. Anonyme Maschinerien, auf die die Menschen keinerlei Einfluss haben, von deren Existenz sie oftmals nicht einmal wissen, beurteilen sie aufgrund der vorhandenen Daten, ordnen sie nach Merkmalen und Verhaltensweisen in verschiedene Typisierungen ein und sorgen dafür, dass sie fortan entsprechend der Typisierung behandelt werden, also welche Angebote ihnen gemacht werden, welche Werbung ihnen zugeschickt wird, ob sie einen Job, eine Wohnung, eine Versicherung, einen Handyvertrag oder

einen Kredit bekommen. So kommt es zu erheblichen Einschränkungen der persönlichen Handlungsmöglichkeiten. Die freie Persönlichkeitsentfaltung muss gestärkt werden, Menschen gegen Manipulation gewappnet werden.

Menschen sind soziale und kommunikative Lebewesen: Sie nehmen ihre Umwelt wahr, orientieren sich daran, reagieren darauf und passen sich an. Wenn die Umwelt nun vorwiegend aus speziell auf mich abgestimmten Angeboten besteht, muss ich mich ständig dazu in Beziehung setzen. Wenn mich meine Umwelt ständig anonym beobachtet, muss ich mein Verhalten so anpassen, dass ich nicht mit dem Weltbild der Überwachenden kollidiere. Die Neigung, den Erwartungen zu entsprechen, ist groß. Die Manipulation, die so schleichend passiert, widerspricht dem Persönlichkeitsrecht, nämlich der Würde des Menschen und seinem Recht auf freie Entfaltung.

Informationelle Selbstbestimmung muss als Voraussetzung von Teilhabe an der Gesellschaft begreifbar gemacht werden, nicht als rücksichtsloser Individualismus.

Abgrenzung von der rein liberalistischen Interpretation von »Privacy« – als »das Recht, in Ruhe gelassen zu werden«. (>the right to be let alone« – dieses Zitat des Richters Thomas M. Cooley ist bekannt geworden durch den Artikel »The Right of Privacy« der us-amerikanischen Anwälte Samuel Warren und Louis Brandeis im Harvard Law Review von 1890 (sic!)).

Privatsphäre bedeutet z.B. nicht, im Auto mit 200 km/h durch die Stadt zu rasen, ohne dafür – anhand einer computerisierten Radarfalle und Erkennung des Kfz-Kennzeichens) belangt zu werden.

Privatsphäre darf nicht missverstanden werden als rücksichtsloser Individualismus des Einzelnen, sondern muss in Beziehung gesetzt werden zu den Rechten anderer und dem Zusammenleben und dem Engagement in der Gesellschaft. Auch das Volkszählungsurteil folgt dem Grundsatz »Soviel Freiheit wie möglich, soviel Bindung wie nötig.« Das heißt,

der Freiheit wird Vorrang eingeräumt, gleichzeitig sind Menschen aber auch Teil einer Gemeinschaft und müssen sich dazu in Beziehung setzen.

Informationelle Selbstbestimmung – Was bedeutet das?

»Das Bundesverfassungsgericht hat im Volkszählungsurteil vom 15.12.1983 den Begriff Recht auf informationelle Selbstbestimmung erstmals in dem Sinne verwendet, dass es sich bei dem Datenschutz um ein Grundrecht handelt. Das Gericht hat auf die Verwendung von Juristen-Deutsch verzichtet und im 1. und 2. Leitsatz dazu ausgeführt: Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf »informationelle Selbstbestimmung« sind nur im überwiegenden Allgemeininteresse zulässig. Gemäß dieser Entscheidung »wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst.« Demnach bildet das allgemeine Persönlichkeitsrecht in Zusammenhang mit der Menschenwürde die verfassungsrechtliche Grundlage für das Recht auf informationelle Selbstbestimmung. Die Grundaussage des Volkszählungsurteils zur informationellen Selbstbestimmung lässt sich mit dem Satz zusammenfassen: So viel Freiheit wie möglich und so viel Bindung wie nötig. Die Freiheit der Bürger wird dabei grundsätzlich vorangestellt; zugleich wird den Anforderungen der Gemeinschaft Rechnung getragen.«⁴

4. H. Bäumler, A. Breinlinger, H.-H. Schrader (Hrsg.): Datenschutz von A-Z. Neuwied: Luchterhand, 1999. Stichwort »Informationelle Selbstbestimmung« (I300).

Leon Hempel

Das elektronische Auge im Blick

Realistische Evaluation von Videoüberwachung im öffentlich zugänglichen Raum

Zusammenfassung

Die rasante Ausbreitung von Videoüberwachung im öffentlich zugänglichen Raum und auch die steigende Bereitschaft der öffentlichen Hand, in technische Sicherheitsmaßnahmen verstärkt zu investieren, macht eine Evaluation über Nutzen und Nachteil dieser Technik heute dringend erforderlich. Fraglich ist dabei nur, in welchem Rahmen eine Bewertung erfolgen sollte, damit hinreichend über Absichten und Wirkungen eines Einsatzes informiert werden kann.

In Deutschland liegen Evaluationen von Videoüberwachung bislang nur als Begleitmaßnahmen von Pilotprojekten vor, die über die Zielerreichung eines Einsatzes berichten. Sie werden meist von den Betreibern der Überwachungsanlagen durchgeführt, wobei der Fokus auf der statistischen Auswertung von Kriminalität liegt. Wissenschaftliche Evaluationen von Videoüberwachung im öffentlich zugänglichen Raum sind hingegen nur aus Großbritannien bekannt. Auch sie verfolgen den Anspruch, die Öffentlichkeit und die politischen Entscheidungsträger über die Effizienz der Videoüberwachung zu informieren, unterscheiden sich aber von Standardevaluationen durch ihre methodischen Ansätze und auch in den Ergebnissen. In Großbritannien haben wissenschaftliche Evaluationen zu einer Fülle inkonsistenter Ergebnisse über den Nutzen geführt. Dies hat nicht zuletzt dazu beigetragen, Evaluierungsansätze zu überdenken. Pawson und Tilley haben auf Grundlage ihrer Kritik der Evaluationsforschung einen Rahmen entwickelt, der die kontextuellen Bedingungen von sozialen Programmen im allgemeinen und Videoüberwachung im besonderen mit in die Bewertung aufnimmt. Ihr Ansatz einer »realistischen Evaluation« ermöglicht die Evaluation mit sozialwissenschaftlicher Theorie zu verbinden, woraus folgt, Videoüber-

wachung nicht mehr allein auf ihre intendierten Ziele und Wirkungen, sondern eben auch hinsichtlich ihrer politischen und sozialen Nebeneffekte zu befragen und auch als Zeichen des gesellschaftlichen Wandels wahrzunehmen.

Im folgenden Beitrag möchte ich auf die grundsätzliche methodische Problematik, aber auch auf die Notwendigkeit der Bewertung von Videoüberwachung hinweisen. Stehen die verschiedenen Evaluationsansätze zunächst im Vordergrund, werde ich abschließend auch einen knappen Ausblick auf die Anforderungen einer sozio-politische Bewertung der Technik geben.

Standardevaluationen in Deutschland

Videoüberwachung wird in der Regel als Instrument zur Kriminalitätsbekämpfung eingeführt. Einmal soll sie präventiv Taten verhindern und Kriminalitätsangst senken, zum anderen repressiv bei der Festnahme von Tätern helfen und so Kriminalität reduzieren. Folgerichtig konzentrieren sich Standardevaluationen auf die Auswertung von Kriminalitätsstatistiken, um die Wirksamkeit der Maßnahme unter Beweis zu stellen. Ihre Ergebnisse werden zur politischen Legitimation eines dauerhaften Einsatzes, aber auch zur Steigerung der öffentlichen Akzeptanz herangezogen. Dieser besondere Stellenwert fordert, sie kritisch zu hinterfragen.

Im Zuge diverser Pilotprojekte, wie in Leipzig, Halle und Regensburg, liegen erste Evaluationen polizeilicher Videoüberwachung in Deutschland vor. Insbesondere der Bericht des Regensburger Projektes ist aufschlussreich, als er die Bedeutung von Standardevaluationen unterstreicht. Er bildete »mitursächlich« die Entscheidungsgrundlage für die Änderung des bayerischen Polizeiaufgabengesetzes vom 01. September 2001, das jetzt

eine ständige Bildaufzeichnung durch offene Videoüberwachung an öffentlichen Plätzen und Strassen erlaubt. Der Bericht beruft sich auf einen festgestellten Rückgang der Straßenkriminalität um 13,7% innerhalb eines Jahres und kommt zum Schluss: »Die Videoüberwachung an Brennpunkten öffentlich zugänglicher Straßen und Plätzen ist eine sinnvolle Maßnahme, potentielle Straftäter abzuschrecken, nachhaltig das Sicherheitsgefühl der Bürger zu stärken und gegebenenfalls auch Tatverdächtige zu ermitteln.« Betont wird aber auch, dass sie kein »Allheilmittel«, sondern »eine zusätzliche technische Möglichkeit« darstellt, »die herkömmlichen polizeilichen Maßnahmen sinnvoll zu ergänzen« (Schweiger 2001: 5).

Zieht man zum Vergleich in Betracht, dass der Bund Deutscher Kriminalbeamter (BDK 2000) einen Rückgang der Straßenkriminalität um bis zu 80 % durch den Einsatz von Videoüberwachung für möglich hält, bleibt fraglich, inwiefern das Regensburger Ergebnis aussagekräftig ist, wie es die politischen Konsequenz suggeriert. Hinter den 13,7% verbergen sich ganze 25 Taten, wobei nicht nachvollziehbar ist, um was es sich für Delikte hierbei handelt. Standardevaluationen erfolgen auf Auftrag und hängen entsprechend ab von bestimmten Machtkonstellationen. Sie sind durch unterschiedliche Interessenlagen geleitet. Dies wird nicht zuletzt an Aussagen erkennbar, die sich gegenseitig mehr oder weniger deutlich einschränken. Der noch in jeder Evaluation auftauchende Hinweis etwa, dass Videoüberwachung ein ergänzendes Instrument innerhalb eines gesamten Maßnahmenkatalogs der polizeilichen Tätigkeit darstellt, dürfte mehr der beruflichen Praxis der Polizeibeamten geschuldet sein, und weniger dem politischen Willen, Videoüberwachung einführen zu wollen.

Aus wissenschaftlicher Perspektive bleiben Standardevaluationen von Videoüberwachung unbefriedigend. Die statistischen Analysen sind oft vage und entbehren meist jeder Selbstkritik. Bekanntlich ist aber schon das kriminelle Geschehen eines Ortes nicht mit den registrierten Straftaten in den Kriminalstatistiken in Übereinstimmung zu bringen. (vgl. Kerner 1993: 296) Eine ganze Reihe von Faktoren beeinflussen zudem Raten im Hinblick auf den Wirksamkeitsnachweis eines technischen Instruments. Abgesehen vom Dunkelbereich nicht registrierter Straftaten, gilt es die Differenz von gemeldeten und registrierten Straftaten in Erwägung zu ziehen, deren generelle Varianz sich durch den Einsatz von Überwachungstechnik verstärken dürfte. Auch spielt die Anwendung weiterer Sicherheitsmaßnahmen eine nicht unwesentliche Rolle (vgl. Coleman & Norris 2000: 153 ff). Die schottischen Kriminologen Ditton und Short (1995: 10-11) benennen fünf Probleme, die auch in den deutschen Standardevaluationen von Videoüberwachung meist keine Berücksichtigung finden:

- Die Phasen vor und nach der Einführung von Videoüberwachung sind bei der Beurteilung von Kriminalitätsraten häufig nicht lang genug. Saisonale Unterschiede werden nicht berücksichtigt.
- Verschiedene Kriminalitätstypen werden häufig zu einer Gesamtzahl zusammengefasst. Einen Anstieg in einigen Kriminalitätsformen kann als Fehlschlag wie auch als Erfolg beurteilt werden.
- Es werden zum Vergleich keine Kontrollanalyse in benachbarten Gebieten vorgenommen. Auch langfristige Kriminalitätstrends bleiben unberücksichtigt.
- Es gibt keine Diskussion über verschiedene Verdrängungseffekte.
- Die Präsentation von Prozentzahlen führt zu fehlerhaften Rückschlüssen in der Öffentlichkeit.

Umstritten bleiben Standardevaluationen letztlich auch, weil sie mit bestimmten Annahmen operieren. So wird durch die Beschränkung auf die Kriminalitätsstatistiken nicht nur ein Funktionieren der Technik vorausge-

setzt, sondern ebenso eine eindeutige Intention unterstellt, die den Nutzen allein im Bereich der Kriminalitätsbekämpfung ansiedelt. Unhinterfragt bleiben jede Art von Nebeneffekten. Für eine fundierte Evaluation indes gilt, dass im Gegensatz zu Befürwortern wie Kritikern an ein Funktionieren der Technik an und für sich zunächst nicht geglaubt wird.

Wissenschaftliche Evaluationen

Geht es um die wissenschaftliche Bewertung von Videoüberwachung, richtet sich der Blick nach Großbritannien. Dort liegen verschiedene, meist Innenstadträume betreffende Studien vor. Sie bieten eine verfeinerte Einschätzung von Closed Circuit Television (CCTV) im öffentlich zugänglichen Raum. Bilden die Grundlage erneut kriminalstatistische Auswertungen, so werden die Grenzen dieser Methode doch offengelegt, geht es etwa um die Verallgemeinerbarkeit der Befunde oder etwa um den konkreten Nachweis von Verdrängungseffekten.

Der Fall Airdrie

Die erste schottische Anlage zur Überwachung eines Stadtzentrums wurde 1992 in der Kleinstadt Airdrie installiert. Die Initiative, so lässt sich den Studien von Ditton und Short (1996, 1998, 1999) entnehmen, ging von einem Polizeibeamten aus, der sich um den ansteigenden Vandalismus im Innenstadtbereich sorgte. Die Lösung fand er in einem Jugendklub, dessen Mitglieder vom ortsansässigen Handel des Vandalismus bezichtigt worden waren. Ein Mädchen machte den Vorschlag, im Klub Kameras zu installieren, die den Verdacht abweisen sollten, worauf der Beamte diese Idee auf den Straßenraum übertrug.

Auf breiter Grundlage einer privatrechtlichen Partnerschaft wurden zwölf Kameras im November 1992 in Airdrie in Betrieb genommen. Die Initiative zeitigte zwei Erfolge. Während der Polizeibeamte zum Fachmann für die Etablierung weiterer Systeme avancierte, fiel die Kriminalitätsrate um 21 % oder 772 Taten durch den Einsatz der Kameras. Die Aus-

wertung für eine Laufzeit von jeweils 24 Monaten vor und nach der Installation erlaubte außerdem die signifikante Differenzierung des Gesamtbildes hinsichtlich einzelner Deliktformen, die sich zeitlich relativ konstant hielten und auch Erwartungen hinsichtlich langfristiger Trends noch übertrafen. »Crimes of dishonesty« (Hauseinbruch, diversen Formen von Diebstahl) verminderten sich um 48%. Zugleich stiegen »Crimes in public order« einschließlich Drogendelikte um 33 % an, was aber weniger ein Fehlschlagen von CCTV als vielmehr die Effizienz von videogestützter Überwachung dokumentierte. Durch vertiefende Untersuchung konnten auch nur leichte Verdrängungseffekte nachgewiesen werden (Ditton & Short 1998: 169), wodurch der Erfolg noch einmal bestätigt wurde.

Der Fall Glasgow

So sehr diese Befunde Videoüberwachung Effizienz bescheinigen, so bleibt doch umstritten, ob sie sich verallgemeinern lassen. In einer zweiten Studie haben Ditton & Short auf der gleichen methodischen Grundlage ein weiteres System in Glasgow untersucht. Die Initiative ging diesmal von einem Stadtentwicklungsbüro aus. Dieses verknüpfte mit der Überwachung die Erwartung, CCTV könnte einen positiven Effekt auf den schlechten Ruf der Stadt haben, potentielle Investoren anlocken, 1500 Arbeitsplätze schaffen und eine Viertelmillion Touristen anziehen (Ditton & Short 1999: 214-215). Doch ließ sich vom Zeitpunkt der Einführung im November 1994 kein Rückgang der Kriminalitätsrate durch die 32 Kameras nachweisen. Vielmehr stieg die Gesamtrate um 9% an. Neben der erneuten Feststellung, dass Videoüberwachung unterschiedliche Auswirkungen auf unterschiedliche Deliktformen hat, die aber keinen Erfolg bescheinigten, ließen sich hier Verdrängungseffekte erkennen.

Ist die Effizienz von Videoüberwachung somit in Frage gestellt, folgt aus der vergleichenden Gegenüberstellung beider Systeme, dass von einer einheitlichen Wirkung von Videoüberwachung nicht die Rede sein kann. Auch in ihren Übersichten bisheriger

Evaluationen haben Phillips (1999) und Coleman und Norris (2000) nochmals verdeutlichen können, dass bislang keinerlei konsistente Ergebnisse über den Einsatz des CCTV als Instrument zur Kriminalitätsbekämpfung zu gewinnen waren. Neben den Erfolgen gibt es Beispiele uneinheitlicher und auch negativer Effizienz. »We conclude«, heißt es bei Ditton & Short (1999: 217), »open-street CCTV can 'work' in limited ways, but it is not a universal panacea. It works in different ways in different situations and future evaluation might choose wisely to concentrate on 'how' rather than 'if'«.

Realistische Evaluation

Hinsichtlich des Einsatzes von Videoüberwachung scheinen verschiedene Kontexte zu verschiedenen Ergebnissen zu führen. Gilt es die Öffentlichkeit über die Effizienz und die Wirksamkeit einer bestimmten Maßnahme zu informieren und politischen Entscheidungsträgern Entscheidungs- und Planungshilfen zu liefern, bleibt die Uneinheitlichkeit von Ergebnissen ein unbefriedigender Zustand für jeden Evaluierungsansatz.

In ihrer grundsätzlichen Kritik an der bisherigen Evaluationsforschung haben Pawson und Tilley (1997) auf die Bedeutung der kontextuellen Bedingungen sozialer Programme hingewiesen. Indem sie einen Rahmen für eine »realistische Evaluation« entwickelt haben, begegneten sie auch der Problematik der Uneinheitlichkeit von Ergebnissen, die verallgemeinerbare Aussagen verhindert. Ihr Modell beruht nicht mehr auf der Konstruktion eines kausalen Zusammenhangs von Programm und Ergebnis, das die beteiligten immanenten Prozesse zugunsten der Frage, inwiefern ein Programm erfolgreich ist oder nicht, ausblendet, sondern auf einem generativen Rahmen. Eine Maßnahme bleibt in der vielschichtigen Realität eingebettet und bringt je nach Kontext verschiedene Wirkungen hervor.

Die Autoren unterscheiden hierfür drei Kategorien: 1. die Wirkungsweisen, die ein Programm in Gang setzen, 2. die Zusammenhänge, die zum Erzielen einer bestimmten Wirkung notwendig sind und 3. die Ergebnisse,

die von einer Wirkungsweise in einem bestimmten Zusammenhang hervorgerufen werden. Anhand einer Evaluation von CCTV auf Parkplätzen, die Tilley im Auftrag des British Home Office 1992 durchgeführt hat (Tilley: 1993), haben die Autoren für jeden Aspekt Typologien erstellt. Ich wähle einige Beispiele der beiden ersten Kategorien zur Illustrierung:

Wirkungsweisen von CCTV

- Auf frischer Tat ertappt: Verhinderung von Kriminalität
- Im Blick der Kamera: Abschreckung potentieller Täter
- Erinnerungstütze: Gefahrenhinweis für potentielle Opfer
- (...)

Kontexte von CCTV

- Tote Winkel: Schutz besonderer Deliktformen
- Alternativen: Täter suchen sich andere Ziele
- Ressourcen: polizeilicher Personalmangel
- (...)

Indem vielschichtige Bedingungen in die Betrachtung mit aufgenommen werden, ermöglicht dieser Rahmen neue Fragestellungen hinsichtlich der Effizienz von Videoüberwachung. Coleman und Norris (2000, 169) kommentieren zurecht: »Realistic evaluation refocuses attention on the processes that produce the particular outcomes rather than just on the outcomes themselves.« Die Kontextualisierung verlagert den Evaluationsmaßstab von der bloßen Orientierung auf den Erfolgsgrad bezüglich des intendierten Ziels zu Fragen der konkreten Anwendung einer Maßnahme. In forschungspraktischer Hinsicht folgt daraus, sich neben der Auswertung von Kriminalitätsstatistiken auch für andere Methoden zu öffnen, damit die Kontexte sinnvoll in den Bewertungsprozess integriert werden können. Theoretisch hat die Einbindung der Kontexte zur Konsequenz, dass im Zuge einer Evaluation auch soziale Modelle hinterfragt werden können und auch sollten. Bereits Ditton und Short haben in ihren Untersuchungen für den Nachweis von Verdrängungseffekten auf Täterbefragungen zurückgegriffen. Realistische Evalua-

tion geht darüber hinaus. Sie öffnet, indem sie auf die inneren Prozesse einer Anwendung und deren Kontexte hinweist, etwa auf die Arbeitsorganisation der polizeilichen Sicherheitsarbeit, die Perspektive für eine sozio-politische Bewertung von Videoüberwachung.

Sozio-politische Bewertung von Videoüberwachung

Die Anwendung der Videoüberwachung impliziert zahlreiche Prozesse von Akteuren innerhalb eines sozio-technischen Systems. Bleiben diese für gewöhnlich im Verborgenen, verlangt die Analyse auf der Basis »realistischer Evaluation« Interesse am Detail. So bedarf es der Beschreibung von Einzelsystemen einschließlich der physischen und sozialen Beschaffenheit des überwachten Raumes. Stadtgeographische Fragen werden hierdurch relevant, wie sie etwa in der These anklingen, Videoüberwachung könnte künftig zur fünften Säulen städtischer Infrastruktur werden (Graham 1998: 108). Auch die räumliche Konfigurierung der Technik, die praktische Anwendung inklusiv paralleler, gekoppelter und automatisierter Nutzungen einzelner technischer Systemkomponenten muss berücksichtigt werden, was ein technisches Verständnis voraussetzt. Ebenso gilt es die personelle Organisation der Überwachung und auch die Einbettung in die Gefahrenabwehr und den rechtlichen Ermächtigungsrahmen mit einzubeziehen. Die Komplexität der Ebenen zieht einen entsprechend erheblichen Methodenaufwand nach sich, deren zentraler Baustein aber die ethnographische Beobachtung der Beobachtung innerhalb und außerhalb der Überwachungszentralen sein dürfte. Im Wechselverhältnis von Beobachtern, Technik und Beobachteten erschließen sich die komplexen Wirkungsweisen von Videoüberwachung.

Die Beobachtung der Beobachtung

Von Mai 1995 bis April 1996 haben Norris und Armstrong (1999) in drei

verschiedenen Raumkonfigurationen die soziale Dynamik von Kontrollzentren untersucht. Das Ergebnis der Studie unterstreicht unter anderem, dass es keine sachlich neutrale Beobachtung gibt, wie es häufig nahegelegt wird. Die kontextuelle Bedingtheit des öffentlich zugänglichen Raumes, der durch immer weitere technische Verfeinerung zu begegnen versucht wird, korreliert mit der subjektiven Auswertung der Bilderflut in den Kontrollräumen. Neben Entscheidungsprozessen der Beobachtung ließen sich Kodifizierungen und damit die Konstruktion bestimmter Verdachtsmomente wie auch ganzer Verdachtsgruppen beobachten. Dabei stellte sich heraus, dass Videoüberwachung auch zu einem institutionalisierten Instrument sozialer Diskriminierung werden kann:

»The sum total of these individual discretionary judgements produces, as we have shown, a highly differentiated pattern of surveillance leading to a massively disproportionate targeting of young males particularly, if they are black or visible identifiable as having sub-cultural affiliations. As the differentiation is not based on objective behavioural and individualised criteria, but merely on being categorised as part of a particular social group, such practices are discriminatory" (Norris & Armstrong 1999: 150).

Diese Befunde fordern weitere Befragung des Phänomens der Videoüberwachung heraus. Längst ist man in der Diskussion darauf aufmerksam geworden, dass die Intentionen sich nicht allein auf Kriminalprävention beschränken. Vielmehr verbinden sie sich mit der Herstellung einer besonderen Atmosphäre, indem störende soziale Gruppen ausgegrenzt werden. Videoüberwachung steigerte dann sozialräumliche Segregation. Sie wird deshalb vielfach mit dem Wandel des öffentlichen Raums in Verbindung gebracht, in dessen Folge Orte der Unterscheidung zu Orten der Gleichförmigkeit umgestaltet werden, die in erster Linie der Konsumption und nicht der Begegnung und des Austauschs dienen (Bannister et al 1998, Reeve 1998). Auch aus kriminologischer Sicht stellt sich die Frage, ob der

Einsatz von Videoüberwachung nicht Ausdruck eines grundsätzlichen gesellschaftlichen Wandels ist, der »Verhaltensweisen der Kälte« unterstützt. Zurückgegriffen wird auf ein primäres Instrument der Kriminalprävention, das Kriminalität schon immer als »normal« einstuft und insofern nicht soziale Ursachen, sondern allein das Delikt bekämpft (vgl. Coleman & Norris 2000, 147). Darüber hinaus kann Videoüberwachung auch als Symbol der Reflexivität unserer informatisierten Gesellschaft diskutiert werden. Mittels der Hypothek auf den Ernstfall holt sie das Künftige immer schon in das Jetzt hinein. Sie zeigt den politischen Willen der Gesellschaft an, sich um die Sicherheitsbelange der Menschen zu kümmern, dabei erzeugt die gewählte Strategie aber womöglich erst die Angst vor Kriminalität.

Schlussbemerkung

Angesichts der rasanten Ausbreitung und der zunehmenden Automatisierung sind fundierte Evaluationen von Sicherheitstechniken dringend geboten. Der angezeigte Weg einer »realistischen Evaluation« weist dabei die Videoüberwachung aufgrund der komplexen kontextuellen Bedingungen des Einsatzes als einen multidisziplinären Forschungsgegenstand aus. Letztlich stellt der Ansatz die Forschung aber auch vor eine Schwierigkeit. Auf der eine Seite eröffnet die Abkehr von der technikorientierten hin zu einer kontextorientierten Evaluation sozialer Programme die Aussicht auf weitere soziale und politische Zusammenhänge integrierende Studien, deren Ergebnisse dann auch noch einmal den dringenden Bedarf einer Regulierung unterstreichen. Andererseits impliziert die Kontextabhängigkeit aber auch, dass allgemeine Handlungsempfehlungen zur Regelung eines Einsatzes nur noch bedingt aus Ergebnissen einzelner Fallstudie abgeleitet werden können. Verlangt ist deshalb ein vergleichender Ansatz im Sinne einer Variation urbaner Kontexte von Videoüberwachung, und ein normativer Rahmen, damit Entscheidungshilfen formuliert werden können. Ohne einen Ansatz, der die inneren Prozesse und Kontexte in die Untersuchung mit einbezieht, werden

sich weder das Nutzungsspektrum nach Sinnfälligkeiten differenzieren, noch die Gefahren und die Kosten für einen Einsatz von Videoüberwachung im öffentlich zugänglichen Raum einschätzen lassen.

Literatur

- Bannister, J., Fyfe, N. and Kearns, A. (1998), 'Closed Circuit Television and the City', in C. Norris, J. Moran and G. Armstrong (eds), *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate.
- Bund Deutscher Kriminalbeamter (2000), 'Kriminalbeamte fordern Videoüberwachung', PM vom 14.04.2000, Birkenwerder: BDK.
- Coleman, C. and Norris, C. (2000) 'CCTV and Crime Prevention: Questions for Criminology' Chapter six of C. Coleman and C. Norris, *Introducing Criminology*, Willan Publishing.
- Ditton, J. and Short, E. (1995), 'Does CCTV Affect Crime?' *CCTV Today* 2: 10-12.
- Ditton, J. and Short, E. (1996), 'Does Closed Circuit Television Prevent Crime?' An Evaluation of the Use of CCTV Surveillance Cameras in Airdrie Town Centre», The Scottish Office Central Unit.
- Ditton, J. and Short, E. (1998), 'Evaluating Scotland's First Town Centre CCTV Scheme.' in C. Norris, J. Moran and G. Armstrong (eds), *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate.
- Ditton J. and Short, E. (1999), 'Yes it does, no it doesn't: Comparing the Effects of Open-Street CCTV in two adjacent Scottish Town Centres' in Painter, K. and Tilley, N. (eds) *Crime Prevention Studies*, Vol 10 pp 201-223. Special edition entitled 'Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention'.
- Graham, S. (1998), 'Towards the Fifth Utility? On the Extension and Normalisation of Public CCTV', in C. Norris, J. Moran and G. Armstrong (eds), *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate.
- Kerner, H.-J.: 'Kriminalstatistik', in: Kaiser et al. (1993), 'Kleines Kriminologisches Wörterbuch', Heidelberg: C.F. Müller.
- Norris, C. and Armstrong, G. (1999), *The Maximum Surveillance Society: The Rise of CCTV*, Berg Oxford.
- Pawson, R. and Tilley, N. (1997), *Realistic Evaluation*, London: Sage.
- Phillips, C. (1999): »A review of CCTV Evaluations: Crime Reduction Effects and Attitudes Towards it Use« in Painter, K. and Tilley, N. (eds) *Crime Prevention Studies*, Vol 10 pp 123-156. Special edition entitled 'Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention'.
- Schweiger, J. (2001), 'Videoüberwachung in Regensburg', PM 430, Regensburg: Polizeidirektion Regensburg, Pressestelle.
- Tilley, N. (1993), 'Understanding Car Parks, Crime and CCTV: Evaluation Lessons From Safer Cities', *Crime Prevention Unit Series Paper 42*. London: Home Office.
- Tilley, N. (1998), 'Evaluating the Effectiveness of CCTV Schemes' in C. Norris, J. Moran and G. Armstrong (eds), *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate.

Hardy Frehe

Freiheit und ihre Verstümmelung im »Synopticon«?

Zur sozialphilosophischen Dimension der Überwachungstechnik

Ich möchte in diesem Aufsatz die sozialphilosophischen Aspekte einer interdisziplinären Studie zur Videoüberwachung vorstellen. Die Studie untersucht die zunehmende Durchdringung der Gesellschaft mit Kontrolltechniken anhand der Videoüberwachung öffentlicher Plätze (CCTV). Dabei ist die Studie dem Thema entsprechend interdisziplinär angelegt und versucht, den Gegenstand in Kooperation mit der Rechtswissenschaft und den entsprechenden technischen Disziplinen zu erschließen.

Sozialphilosophische Thematik

Anlass zur Studie gibt die relativ hohe Akzeptanz der Videoüberwachung in der Bevölkerung. In Frage steht, worin diese begründet liegt. Des weiteren fordert auch die Artikulation des Unbehagens an dieser Form der Überwachung die philosophische Arbeit am Begriff heraus. In diesem Zusammenhang sollen die Begründungs- und Deutungsstrategien kritisch hinterfragt werden. Dies in Entgegensetzung sowohl zum funktionalistischen Diskurs als auch zu dem, der um das Phantasma der Sicherheit kreist. Im Sicherheitsdiskurs avanciert Sicherheit zum neuen Supergrundrecht, wodurch »beliebige Grundrechtseinschränkungen« legitimiert werden können (vgl. Bendrath 1998). Der Bürger wird primär als potentiell Sicherheitsrisiko angesehen und die Unschuldsvermutung wird suspendiert. Überwachung wird »tendenziell allgegenwärtig und an jeder Ecke einforderbar«: »Vor den flexiblen Straßenkameras gibt es überhaupt kein Entkommen mehr.« (Blum 1999: 42). Ein »gesichtsloser Blick« entsteht, »der den Gesellschaftskörper zu seinem Wahrnehmungsfeld macht: Tausende von Augen, die überall postiert sind; bewegliche und ständig wach-

same Aufmerksamkeiten« (Foucault 1976: 275). Dabei wird die Totalisierung der Kontrolle nicht zuletzt durch die den hohen Personalkosten und der Datenflut begegnende Automatisierung möglich. Die Kontrolle durchdringt alle Bereiche (man denke nur an die aufgezeichneten und ausgewerteten Datenschatten [Internet, Handy etc.]). Die Auswirkungen lassen sich anhand des mit CCTV unternommenen Schrittes betrachten. Thematisch wird dabei der latente Anpassungsdruck durch die Installationen, das Aufkündigen des Vertrauens in den neuinstrumentierten Räumen sowie die Gefahr der Verselbständigung der technischen Überwachungsinfrastruktur. Das Aufkommen von CCTV ist – aufgrund des Verdrängungseffekts – als Bestandteil der Reinigungsstrategien der »neuen panoptischen« Stadt zu begreifen. Die Opfer der gesellschaftlichen Polarisierung werden nach dem Konzept der »sauberen Stadt« (Zero-Tolerance-Strategie) nicht mehr in der Innenstadt geduldet. Sie werden entfernt: »Wie Giftfässer, die man ins Meer wirft – in der Hoffnung, das Problem auf immer loszusein« (Neitzke 1999: 13). Die Stadtgesellschaft zerfällt in immer kleinere, sozial homogene Gemeinschaften (vgl. Rada 1999: 38) und unterschiedlich überwachte Bereiche. Die »gebaute Umwelt« übernimmt immer mehr »Polizeifunktionen« und wird »von den Techniken des »elektronischen Schlachtfeldes« der Polizeitruppen überwacht und gesichert« (Werber 1999: 433).

Folgende Fragen sollen in der Studie verfolgt werden: Welche Auswirkungen ergeben sich für unser Selbst- und Weltverhältnis? Was heißt es, sich in einem Raum der völligen Sichtbarkeit und Kontrolle, einem »sozialen Raum ohne Schatten« (Wunderlich 1999: 354) zu bewegen? Ändert sich

nicht das Selbstbild der Menschen signifikant, wenn es durch aufgenommene Bilder erweitert wird, die sich seiner Kontrolle entziehen? Wenn es also (virtuell) zu verfügbarem Material wird? Vollzieht sich eine »obszöne Hyperinklusion« (Stäheli 2000a: 66), wo in Big-Brother-Szenarien das »good subject als möglichst perfektes Experiment-Subjekt« (Stäheli 2000a: 69) produziert wird, bzw. die Big-Brother-Show eine universelle Lebensstruktur sichtbar macht: »Ich existiere nur insofern, als ich dauernd beobachtet werde« (Žižek 2000: 152)? Die Auswirkungen auf die Subjektivierung sollen mit Blick auf die neuen Formen der gesellschaftlichen Identitätsproduktion – »deren Akzent auf Nicht-Festlegung, auf Manövrierfähigkeit und auf der Fähigkeit, neue Erfahrungen und Gelegenheiten einfach aus Vergnügen wahrzunehmen« liegt (Bauman 1997: 130) – nachgezeichnet werden.

Eine mögliche Kritikstrategie kann sich auf den subjektivitätstheoretischen Strukturbegriff der Exzentrizität des Selbst, auf die leere Mitte des Selbst beziehen. Die Mitte des Selbst ist leer, da wir uns niemals in der Präsenz erreichen, sondern uns in »ursprünglicher Verspätung« (Derrida) nur in ununterbrochenen prädikativen Differenznahmen suchen können. Besonderung und damit auch Selbstentzug ist nötig,

»weil wir uns niemals anders »gegeben« sind als im Vollzug oder in der Performativität von Handlungen und Sprechweisen, die, sobald sie sich in äußerer oder sinnlicher Gestalt verpuppen, uns auch verfehlen« (Gamm 2001: 46).

Das Unverfügbare der Subjektivität, die sich gleichwohl besondern muss, aber nicht darin aufgeht, entgeht notwendig den Kameras.

Sozialphilosophisch stellt sich die Frage, ob CCTV nicht negativ in die Grundlagen unseres Zusammenlebens eingreift, in dem sie identifikatorisch den normativen, obzwar extimen (i.S. von Nichtverortbarkeit) Kern des Sozialen besetzt. Das Soziale, das tragende Gewebe des Zusammenlebens der Menschen, dieses als vorgängiges Medium begreifbare »Zwischen« lässt sich normativ ausgehend vom Bezug auf die Alterität verstehen. Sozialität muss also nicht auf dem synthetischen Begriff der Gesellschaft gegründet werden. So betrachtet Lévinas das Reale nicht nur ausgehend von der historischen Objektivität, sondern auch von dem »Geheimnis, das die Kontinuität [...] unterbricht« (Lévinas 1986: 61). Dieses Geheimnis der sich in der Verantwortung für den Anderen als Antlitz konstituierende Subjektivität, macht die Pluralität der Gesellschaft möglich. Antlitz zielt auf die nicht einholbare Differenz, die alle bildhaften Vorstellungen, die als solche immer begrenzt sind, überschreitet und das Geheimnis begründet. Dabei lässt sich das Antlitz mit Bauman als Fiktion ausweisen, insofern der Andere niemals als reine unbestimmte Andersheit begegnet, sondern es immer das Antlitz eines bestimmten Anderen ist, das uns begegnet. Aber er verweist mit Lévinas ebenso darauf, dass der Andere nicht in der Bestimmtheit aufgeht. Bauman betrachtet den sozialen Raum als eine »komplexe Interaktion dreier ineinander verwobener, jedoch unterschiedlicher Prozesse und ihrer jeweiligen Produkte« (Bauman 1995b: 217). Er unterscheidet ästhetische, kognitive und moralische Raumbildungsprozesse. CCTV ist den kognitiven, auf Eindeutigkeit drängenden Raumbildungsprozessen zuzuordnen. Die künstlichen Räume stellen die Stadtbewohner vor Identitätsprobleme und zeigen sich als abträglich für die Moralität:

»The faceless monotony and clinical purity of the artificially construed space deprived them of the opportunity for meaning-negotiating [...] We may add that human responsibility [...] would find the perfectly designed space to be an infertile if not downright poisonous

soil. [...] Only such people could face up to the fact of their responsibility who would have mastered the difficult art of acting under conditions of ambivalence and uncertainty, born of difference and variety« (Bauman 1998: 46).

Die technisch neu instrumentierten Räume treiben den Monotonie und Reinheit befördernden Prozess voran.

Dies wirft die Frage nach der Technik in ihrer modernen Struktur auf. Ein Verständnis von Technik als das Medium der Selbst- und Welterschließung, als das Vorgängige, in dem wir uns bewegen, welches sowohl Möglichkeitsräume eröffnet als auch Begrenzung durch die bereitgestellten Unterscheidungen mit sich führt, leitet diese Studie an. Es ist zu konfrontieren mit einer Deutung von Technik (CCTV) als Mittel für einen vorgegebenen Zweck (z.B. Verbrechensprävention). Technik als Medium verweist dabei »auf den Horizont, von dem her wir die Welt erfinden oder auch das Bild von uns selbst immer nachdrücklicher technisch überschreiben« (Gamm 2000: 285). Dabei fällt Technik als Manifestation der leeren Mitte des Selbst, »die sich nicht im Medium des (geistigen) Begriffs reflektiert, in identitätslogische Reformulierungen« (Gamm 2000: 307) zurück. Unter dem Regime der Identitätslogik zeigt sich für Foucault die Spielart der panoptischen Macht, »in der jeder seine eigene Individualität als Stand zugewiesen erhält, in der er auf die ihn charakterisierenden Eigenschaften, Maße, Abstände und »Noten« festgelegt wird, die aus ihm einen »Fall« machen« (Foucault 1976: 247). CCTV erschließt nun den öffentlich zugänglichen Raum den identifikatorischen Praktiken.

Die Frage nach Kontrolle, Kriminalität und der übergreifenden gesellschaftlichen Figuration, in der wir uns befinden, wird im folgenden anhand der Zeitdiagnose von Zygmunt Bauman nachgegangen. Die zeitdiagnostische Einbettung des Prozesses der zunehmenden Implementierung von Kontrolltechniken dient dem Ziel einer umfassenden Deutung. Erklärt werden soll, warum in der »Kontrollgesellschaft«, »die nicht mehr durch Internierung funktioniert« (Deleuze

1993: 250) und in der sich ein Kontrollmechanismus durchsetzt, »der in jedem Moment die Position eines Elements in einem offenen Milieu angibt« (Deleuze 1993: 261), das Wuchern der Videokameras nicht nur hingenommen, sondern geradezu begrüßt wird.

Is there life after the Panopticon?

CCTV scheint sich auf der Linie des von Foucault unter Rekurs auf Bentham nachgezeichneten Panoptismus deuten zu lassen. Für Foucault ist das Panoptikum das architektonische Modell der modernen »Disziplinarmacht«, die vom Beginn des 19. Jh. an die »normalen« Individuen als Soldaten und Arbeiter mittels Gesetzgebung und Reglementierung produzierte. Die Fabriken der Ordnung wurden gerechtfertigt durch das Glück der wiedergeborenen Ordnung. Bentham »glaubte, dass das Nebenprodukt der panoptischen Fabrik der Ordnung das Glück der Insassen sein würde: »Nenne sie Soldaten, nenne sie Mönche, nenne sie Maschinen; sind sie nur glücklich, kümmert es mich nicht.« (Bauman 1997: 174).

Gegenwartsdiagnostisch lässt sich nach der Angemessenheit des Denkformulars Panoptikum fragen, weil die panoptische Macht durch Verführung ergänzt wird. Die Strategien der Repression richten sich in der Konsumgesellschaft besonders gegen die nicht durch Verführung (mittels der Marktmechanismen) integrierte Klasse. In dieser Gesellschaft boomt die Gefängnisindustrie, die Ausgaben für die Überwachung steigen und das Gefühl der Unsicherheit verbreitet sich gleichzeitig allgemein. Wobei ein Nebeneffekt dieser gesellschaftlichen Figuration in der steigenden Kluft zwischen den Wohlhabenden und den gesellschaftlich Deklassierten zu sehen ist. Dabei unterliegen die Randgruppen trotz der als Modernisierung begriffenen Deregulation immer stärkeren Kontrollen, was die Kosten von Fürsorge zur Überwachung verschiebt. Die verlockenden Impulse werden in der Konsumgesellschaft an alle in gleicher Weise gesendet, aber sie können nur höchst unterschiedlich umgesetzt werden. Insofern ist die

forcierte Überwachung und die zunehmende Kriminalität als »das ureigene, logisch [...] legitime Produkt der Konsumgesellschaft« (Bauman 1999: 75) und nicht als Funktionsstörung zu begreifen. Die radikale Freiheit des Marktes geht mit dem Abbau des Wohlfahrtsstaates und der Tendenz, Armut zu kriminalisieren, einher. Sozialleistungen sollen nur die »wirklich Bedürftigen« erhalten, was mit der Stigmatisierung der Sozialhilfeempfänger als unfähig und sorglos sowie der verstärkten Überprüfung dieser Gruppe verbunden ist.

Bauman stellt das Schicksal der panoptischen Macht unter Bezug auf Mark Posters Rede vom »Superpanoptikum« dar. Poster, der »the electronic database as an updated cyberspatial version of the Panopticon« (Bauman 1998: 50) beschreibt, sieht im »Superpanoptikum« ein Panoptikum mit der Erweiterung: »the surveilled, supplying the data for storage, are prime – and willing – factors in the surveillance« (Bauman 1998: 50). Dabei sind die Ähnlichkeiten zum Panoptikum nur oberflächlicher Art, denn

»the Panopticon's main purpose was to instill discipline and to impose a uniform pattern on the behaviour of its inmates; the Panopticon was first and foremost a weapon against difference, choice and variety« (Bauman 1998: 50).

Es wurden bestimmte Lebensformen produziert: »The Panopticon ensnared its inmates as producers and/ or soldiers, of whom routine and monotonous conduct was expected and demanded« (Bauman 1998: 50).

Das Superpanoptikum zielt dagegen auf das Identifizieren der potenten Konsumenten, die zwischen den marktförmigen Differenzen frei wählen können:

»the data-base puts on record the reliable and trustworthy consumers – [...] the database's main function is to make sure that no intruder can enter it under false pretences and without proper credentials« (Bauman 1998: 51).

Die neue Freiheit wird gerade durch Überwachung, Erfassung und Feststellung möglich: »The more information about you the database contains,

the more freely you can move.« (Bauman 1998: 51). Dieses gilt aber nur für die durch den Konsum Verführbaren, während weiterhin und zwar um so durchdringender die Repression gegen die impotenten Mitspieler greift.

In einem weiteren Aspekt wird die Veränderung des Machtmechanismus mit Bezug auf die neuen Lebensformen bei Thomas Mathiesen diskutiert. Mathiesen beschreibt den Übergang vom Panoptikum – »where the few watch the many« und »surveillance replaced the spectacle« – zu dem »Synopticon«, »the development of new techniques of power, consisting [...] in the many (as many as never before in history) watching the few« (Bauman 1998: 51). Diese Transformation zeichnet Mathiesen zunächst für die Massenmedien und den »interactive one-way medium« Internet nach. Das globale Synopticon führt nun zu einem Distanzen vergleichgültigenden Raum, während das in seiner Anwendung zwar universale Panoptikum jeweils lokal gebunden war. Es immobilisierte die Subjekte, während wir in der Postmoderne, in der jede endgültige Festlegung, jede irreduzible Differenzierung und jeder Sicherheit gebende Hafen diskreditiert ist, unterwegs sind, ohne je physisch reisen zu müssen. Die »targets« des Synopticons werden nun in Zuschauer transformiert. Dabei werden gerade ihre Beobachtungen in einem bisher unbekannten Maße beobachtbar, wovon die in einer Gesellschaft von Zuschauern versammelten Individuen unberührt bleiben, da es nicht die individuelle Wahlfreiheit beschneidet.

Mit dem Konzept des »Synopticon« lässt sich der Übergang zur Überwachungsgesellschaft fassen. In der Tat sind es private Unternehmen, die Daten sammeln und verwerten sowie private »Sicherheitsdienste« die Shopping Malls mit Überwachungskameras und schwarzen Sheriffs kontrollieren. Somit dezentriert sich die Überwachung in einer vernetzten Welt, in der der Staat zwar die Reproduktion der systemischen Ordnung den politisch nicht rechenschaftspflichtigen Kräften des Marktes überließ, aber aufgrund des Gewaltmonopols in eine spezielle Funktion, der

Konzentration auf die Ausübung des hoheitlichen Zwanges, gedrängt wird. Auf ihm lastet im Bereich der Sicherheit der Druck, mit Überwachung dem postmodernen Unbehagen, welches durch eine »Freiheit, die auf der Suche nach Lustgewinn zuwenig individuelle Sicherheit toleriert« (Bauman 1999: 11) entsteht, zu begegnen. Dabei zeichnet sich in »Sicherheitspartnerschaften« das Miteinbeziehen der Kameras der Privatwirtschaft ab. Dennoch lässt sich im Staat die einzige Instanz ausmachen, die das Recht auf informationelle Selbstbestimmung durchsetzen kann.

Verstümmelte Freiheit

Neben einer Kritik, die sich auf die identifikatorisch depotenzierte, Sozialität fundierende Alterität oder die durch die Installationen sich auf Konformität gedrängt sehende Subjektivität bezieht, kann eine andere Strategie ihren Ausgang von der »individualisierten Welt« nehmen. Diese versteht sich über die individuelle Wahlfreiheit – zu der wir verurteilt sind.

Die Freiheit der Konsumenten ist als eine verstümmelte, defizitäre Form von Freiheit zu dechiffrieren. Sie steht der zivilgesellschaftlichen Gestaltung des sozialen Lebens entgegen und tendiert zu einer vergleichgültigenden Beziehung zum Anderen. Freiheit ist als soziale, stratifizierende Größe zu fassen, denn die individuelle Wahlfreiheit nimmt zwar alle in die gleiche »Verantwortung«, aber die Mittel zur Realisierung der jeweiligen Wahl sind höchst unterschiedlich verteilt. Da sich diese Freiheit nicht allein durch individuelle Anstrengungen realisieren lässt, wäre die (alte) Einsicht, dass die »die Freiheit der Freien [...] die Freiheit aller« (Bauman 1999: 364) erfordert, aufzunehmen. Auch sind die als Konsumenten gesellschaftlich produzierten Individuen, die sich sicher und heimisch nur in »einbruchssicheren Häusern in grünen Vororten, befestigten Büros in polizeilich überwachten Geschäftsvierteln und sicherheitselektronisch hochgerüsteten Autos« (Bauman 1999: 55) fühlen, von dem Unsicherheitsgefühl betroffen.

In einer dies berücksichtigenden Politik gälte es, sich auf Freiheit, Ver-

schiedenheit und Solidarität verpflichtet zu sehen, wobei Freiheit und Verschiedenheit, wenngleich in einer defizitären Form, von der gegenwärtigen Konstellation unterstützt werden. Dabei ist die gemeinschaftsselige Missbrauchsmöglichkeit, die in einer Differenzen planierenden Forderung nach Solidarität liegt, zu beachten. Dieser Gefahr ist durch die Institutionierung radikal-demokratischer Strukturen zu begegnen.

Postmoderne Politik

Die Frage nach Gestaltungsmöglichkeiten, nach der Artikulation des bürgerrechtlich orientierten Unbehagens an der Videoüberwachung lässt sich anhand der Theorie der radikalen Demokratie verfolgen. Diese Theorie ist dadurch charakterisiert, dass sie die unentbehrliche Rolle der symbolischen Einheitsrepräsentation des diskursiven Systems – im Bewusstsein der Unmöglichkeit und auch der Gefahr einer endgültigen Schließung über eine Repräsentation – in Rechnung stellt. Ferner verabschiedet sie das Konzept der antagonismusfreien Gesellschaft zugunsten der als radikal geschichtlich zu begreifenden, sich selbst in ihren Repräsentationen performativ erzeugenden Zivilgesellschaft, die sich auf keine abgesicherten Gewissheiten berufen kann. Die Zivilgesellschaft ist auf temporäre Schließung durch Füllung des leeren Signifikanten angewiesen. Dabei ist eine Allgemeinheit anzustreben, die aber im Sinne eines wahren, sättigenden Begriffs unmöglich ist. Die Schließung ist als Kampf zu begreifen, der sich nicht auf letzte Wahrheiten berufen kann und Intoleranz »zum Zweck einer politischen, Uneinigkeit schaffenden Leidenschaft« (Zizek 1998: 13f) verlangt. Der »Kampf um die eigene Stimme, die als die Stimme eines rechtmäßigen Partners gehört und anerkannt werden soll« (Zizek 1998: 31), muss doch – entgegen der Vorstellung des gleichberechtigten, konsensfrömmelnden Partners – die Repräsentation des Ganzen beanspruchen. Der Bezug auf das Ganze – wie er sich in der Rede von der Inneren Sicherheit herstellt – ist durch den Versuch einer Besetzung des leeren Signifikanten vermittelt. Auf dem Feld der Video-

überwachung bieten sich die Begriffe der **Inneren Sicherheit** und der **Kontrollgesellschaft** als Themata für die diskursive Re-Artikulation an. Die mit CCTV verbundene Exklusion und das den sozialen Raum okkupierende Misstrauen werfen die Frage auf, ob wir wirklich eine Überwachungsgesellschaft, flankiert durch einen immer tiefer in das soziale Leben durch Überwachungsmaßnahmen eingreifenden Staat, wollen? Stellen sich die Grundlagen des normativ gehaltvollen Sozialen als dadurch gefährdet heraus? Es lässt sich fragen, »ob es ein Grundrecht auf Anonymität gibt und in welchen Bereichen es gewahrt sein muss« (Rötzer 2000: 166)? Dies steht den Überwachungsinstallationen, die nach Datenschutzrecht erlaubt sind, gegenüber, wobei die durch die neuen technischen Errungenschaften eingeräumte, erschreckend weitgehende Möglichkeit kontrolliert zu werden, aufgenommen werden müsste. Nur stellt sich da die Frage: Wie soll dies Grundrecht durchgesetzt werden? Werden nicht bürgerrechtlich zu begrüßende Entscheidungen wie das Volkszählungsurteil in der Praxis unterlaufen? Wird die als Korrektiv fungierende Öffentlichkeit nicht immer weiter durch Kontrollmedien strukturiert? Wie ist es mit dem Argument, dass durch CCTV auch eine neue Form der Aufklärung eröffnet wird? Wobei dies ja als Chance zu begreifen wäre! Hier verweisen Norris und Armstrong darauf, dass im TV nur ausgewählte Bilder, die den gängigen Vorstellungen von 'richtiger Polizeiarbeit' entsprechen, dem Publikum präsentiert werden:

»Die Überwachung von Demonstranten, die Vertreibung 'lästiger' Jugendlicher durch die Polizei oder die Fernhaltung von Kindern aus Einkaufszentren durch Wachleute gehen nicht über die Fernsehbildschirme. Dennoch gehören sie zur täglichen Praxis der Videoüberwachung« (Norris/Armstrong 1998: 36).

Ebenso rar sind Bilder von Polizeiübergriffen.

Eine andere sich in der Praxis subvertiert findende »Chance« stellt das berühmte Volkszählungsurteil von 1983 dar, das die Bedeutung der

Nichtregistrierung für Freiheit und Wahrnehmung von Partizipationschancen herausstellt, denn im Blick auf die Verfassungswirklichkeit dürften die auf dieses Urteil folgenden Kodifizierungen ja ebenso bekannt sein (vgl. bspw. Narr 1998 und die »Vorwärtsverrechtlichung«). So stellt sich angesichts der Probleme, das komplexe Verhältnis von Macht, Recht und Politik in ein ausbalanciertes Verhältnis zu bringen, die Frage, ob das Verhältnis von Freiheit und Sicherheit (Kontrolle) nicht als Widerstreit (Lyotard) gefasst werden muss? Und zwar dies in Kritik von Bestrebungen, diesen Widerstreit durch Ausweisung von Sicherheit als grundlegenden Wert zu invisibilisieren.

Mit radikal-demokratischen Theorien lässt sich die Auseinandersetzung als Kampf um den leeren Signifikanten, um die Schließung des unbestimmten, dabei aber die normativen Potentiale der Unbestimmtheit (i.S. der Unbestimmtheit des Selbst, der offen zu haltenden Mitte der symbolischen Repräsentation, des extimen Kerns des Sozialen) nicht ausschöpfenden Begriffs der Inneren Sicherheit begreifen. Aber ist es wirklich so schlimm auf dem Feld der Sicherheit bestellt? Dem Ruf, dass den inzwischen bewährten bundesrepublikanischen demokratischen Institutionen doch zu vertrauen sei, lässt sich durch verschiedene Betrachtungen entgegen treten. So brachte immerhin das als Vorbild ausgelobte, demokratische Amerika einen McCarthy hervor und die politischen Kontrollmechanismen scheinen ebenso eine auf einen politischen Akt zielende Opposition von vornherein zu unterdrücken. Die Beförderung der Konformität durch die Überwachungsinfrastruktur scheint ein weitaus größerer Effekt zu sein als die Erfolge bei der Prävention, wobei die Untersuchung unterschiedliche Resultate zeigten (vgl. Beste und Hempel in diesem Heft).

Natürlich können in diesem Diskurs keine konkreten Maßnahmen wie die Einschränkung des Schwenkkreises einer bestimmten Kamera (vgl. bspw. Sokol 2001: 68f.) vorgeschlagen werden. Es geht eher um die Frage, wie wir uns verstehen wollen. Wie soll die Gesellschaft verfasst sein? Dabei geht es um die Artikulation des Unbe-

hagens oder um eine Politik der Entparadoxierung, die Paradoxien aufdeckt und im Kampf um den leeren Signifikanten versucht, diesen anders zu besetzen (vgl. Stäheli 2000b). Mögliches Ziel wäre die Etablierung eines Horizontes, der den Grundlagen des Zusammenlebens einer sich als offen verstehenden Gesellschaft, die das Soziale in der Alterität fundiert sieht, gerecht wird.

Literatur

- Bauman, Z. (1995a): »Ansichten der Postmoderne«; Argument, Hamburg.
- Bauman, Z. (1995b): »Postmoderne Ethik«; Hamburger Edition.
- Bauman, Z. (1997): »Flaneure, Spieler und Touristen; Essays zu postmodernen Lebensformen«; Hamburger Edition.
- Bauman, Z. (1998): »Space Wars: a Career Report« in: »Globalization; The Human Consequences«; Polity Press, Cambridge, S. 27-54.
- Bauman, Z. (1999): »Vom Unbehagen in der Postmoderne«; Hamburger Edition.
- Bendrath, R. (1998): »Über die Umwertung des Staates und das Grundrecht auf Sicherheit; Von Freiheit stirbt mit Sicherheit zu Keine Freiheit ohne Sicherheit?« in: »Telepolis« (<http://www.telepolis.de/deutsch/inhalt/co/3246/1.html>)
- Blum, E. (1999): »Zeichen von Barbarei: die neue panoptische Stadt« in: »Centrum: Jahrbuch Architektur und Stadt«; Birkhäuser, Basel, S. 40-45.
- Deleuze, G. (1993): »Unter-Handlungen 1972 – 1990«; Suhrkamp, Frankfurt/Main.
- Foucault, M. (1976): »Überwachen und Strafen. Die Geburt der Gefängnisse«; Suhrkamp, Frankfurt/Main.
- Gamm, G. (2000): »Nicht Nichts«; Suhrkamp, Frankfurt/Main.
- Gamm, G. (2001): »Aus der Mitte denken«; Zeitschrift für kritische Theorie, 12/2001, S. 29-50.
- Lévinas, E. (1986): »Ethik und Unendliches«; Graz, Edition Passagen.
- Narr, W.-D. (1998): »Wir Bürger als Sicherheitsrisiko«; Bürgerrechte & Polizei/CILIP 60 (2/98), S. 52-59.
- Neitzke, P. (1999): »Andauernder Zustand mit ungewissen Ausgang«, in: »Centrum« a.a.O., S. 9-15.
- Norris, C./Armstrong, G. (1998): »Smile, you're on camera. Flächendeckende Videoüberwachung in Großbritannien«, in: »Bürgerrechte & Polizei/CILIP 61« (3/1998), S. 30-40.
- Rada, U. (1999): »Die Grenzen von Arkadien« in: »Centrum« a.a.O., S. 34-39.
- Rötzer, F. (2000): »Vom Ende der Anonymität« in: »Vom Ende der Anonymität; Die Globalisierung der Überwachung«, Schulzki-Haddouti, Christiane (Hg.), H. Heise Verlag, Hannover, S. 157-168.
- Sokol, B. (2001): »Fünftehnter Datenschutzbericht der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen; für die Zeit vom 1. Januar 1999 bis zum 31. Dezember 2000«; <http://www.nordrhein-westfalen.datenschutz.de/>
- Stäheli, U. (2000a): »Big Brother: das Experiment »Authentizität« – Zur Interdiskursivität von Versuchsanordnungen«; in: »Big Brother. Beobachtungen«, Balke, F. et. al. (Hg.); transcript Verlag, Bielefeld, S. 55-77.
- Stäheli, U. (2000b): »Sinnzusammenbrüche – Eine dekonstruktive Lektüre von Niklas Luhmanns Systemtheorie«, Velbrück Wissenschaft, Weilerswist.
- Werber, N. (1999): »Die Zukunft der Weltgesellschaft« in: »Kommunikation, Medien, Macht«, Maresch R. und N. Weber (Hg.), Suhrkamp, Frankfurt/Main, S. 414-444.
- Wunderlich, S. (1999): »Vom digitalen Panopticum zur elektrischen Heterotopie; Foucaults Topographien der Macht« in »Kommunikation, Medien, Macht«, a.a.O., S. 342 – 367.
- Zizek, S. (1998): »Ein Plädoyer für die Intoleranz«; Passagen-Verlag, Wien.
- Zizek, S. (2000): »Die Kamera liebt dich. Unser Leben als Seifenoper« in: »Big Brother. Beobachtungen«, a.a.O., S. 151-155.

Steve Mann

Intelligent Bathroom Fixtures and Systems

Aquionics Research at EXISTech Corporation

Introduction

This paper describes new approaches to the design of automatic sensor operated bathroom fixtures, systems for controlling bathroom fixtures, and methods of bathroom fixture design, control, and management, as well as the control and management of hygiene and water resources. Through the use of new computer vision technologies, and image processing, a safe, clean, and efficient facility can be provided, while reducing maintenance and operating costs.

First impressions are lasting ones and when a person visits a company's public bathroom, a perception of the entire company is immediately formed. Thus many businesses are reali-

zing the need to make sure the impression is a positive one.

Fully automated bathroom fixtures will function without wasting unnecessary water and energy which otherwise results with the use of conventional manually operated fixtures. Touchless automatic sensor operated bathroom fixtures have become very popular, and are beginning to replace older manually operated fixtures.

Additionally, these new fixtures offer a high degree of hygiene by creating an atmosphere where the user completely avoids any direct physical contact with the unit. As a result, the risks of spreading of infectious diseases are greatly reduced.

The new fixtures are quick and easy to install and require minimal maintenance.

Networked plumbing systems also help facility managers monitor the operation of various bathrooms in a facility or at remote facilities. Control boxes controlling several showers, faucets, urinals, or water closets are now being used in some of the large bathroom complexes.

Terminology

A »bathroom« refers to an environment that contains bathing or sanitary fixtures. Therefore, in this paper, the term »bathroom« includes, for example, a toilet room, or a room that has a toilet and sink, even if no bath

tub is present in this room. A bathroom may be a room intended for individual users, or it may be a communal bathroom for use by more than one person at the same time. For example, a bathroom may be a room that contains a plurality of urinals, toilets, sinks, showers, or the like, for use by one or more persons. The term bath is taken to include various forms of baths, including a showerbath, steam bath, sauna bath, or swimming bath. Thus a room containing only one or more showers will still be considered to be a bathroom even if there is no bath tub or other form of basin in this room.

Similarly, a mass decontamination facility, a washdown facility, a mass delousing center, a cleansing station, or the like, is considered to be a bathroom.

Likewise, an environment containing a whirlpool, jacuzzi, swimming pool, or the like, will be considered to be a bathroom even if the fixture is not located within the boundaries of an explicitly defined room.

For example, the environment around an outdoor swimming bath will still be considered to be a bathroom, and to thus fall within the scope of this paper.

Smart Bathrooms with Video Based Motion Detection

The sensor systems used in EXISTech Corporation's research prototype bathroom facilities comprise standard video cameras. Because of mass production, a single camera costs much less than one of the specialized sensors commonly used to automatically flush toilets and urinals. Moreover, further costs savings are introduced by the fact that a single video camera can monitor a number of fixtures. For example, one video camera can monitor a whole row of urinals, to flush only the urinals having been used. Intelligent computer vision systems monitor traffic flow patterns, so that a weaker flush is used when others are standing in line to use the facilities, whereas a stronger flush is provided after the last user of a group of users has finished.

Thus intelligent video based sensor technology will reduce initial installation costs as well as operating costs, when compared to other sensor technologies.

It is desired that a sensor system either passively observe the bath environment or if it is an active vision system, that the active element of its vision system appear invisible to the user of the bathroom. Ideally even the passive element of the system is also concealed from users, to prevent vandalism or experimentation with the sensors, or to prevent the user from reverse engineering the sensors to learn how they work.

For example, the sensors are often built into or behind materials where the sensors respond to light in a manner having lesser sensitivity to ordinary human biological vision. In this way, bathroom users cannot see the sensors but the sensors can see the bathroom users. A simple example is the use of infrared cameras, which can be concealed behind surfaces that are only transparent in the infrared.

A shiny vitreous material that a user can not see through may at the same time gather some light to at least one camera or other optical imaging system.

Camera based sensors can provide a much more intricate and sophisticated form of control, because they can detect user behaviour, usage patterns, traffic flow patterns, and other attributes not evident in traditional bathroom presence or occupancy sensors.

However, since sensors often become the target of vandalism or reverse-engineering by hackers trying to understand how they work, concealment is often desirable.

Many bathroom surfaces are made of shiny glasslike materials such as ceramic. Thus viewing windows can be easily built into or concealed in bathroom fixtures, walls, or other surfaces. Such viewing windows typically include some or all of the following:

- sapphire windows, ceramics, and vitronic devices;
- sapphire (alumina) infrared viewing windows;
- optical ceramics;
- glass, fiberglass;

- vitreous china.

Such viewing windows will have a normal appearance to bathroom users.

In one embodiment, the sensors are concealed by a synchronized electrochromic viewport which is preferably not synchronized, or easily synchronizable by bathroom users attempting to reverse engineer the bathroom control system.

Ordinarily the viewport will therefore appear more transmissive to the video sensors than to biological human vision of bathroom users.

One of EXISTech Corporation's intelligent bathroom prototypes was recently built at 80 Spadina Ave, in Toronto, in July of 2001.¹

EXISTech's other intelligent bathrooms typically use various kinds of image sensors, some within fixtures, some being part of actuators for fixtures, some not in fixtures, and various possible connections and arrangements.

Special optics preferably block visible light and pass infrared light, so that the sensor is sensitive to the infrared. In this way, the sensor can be an active sensor, or can be part of an active sensor system in which infrared light is used to illuminate subject matter in the bathroom. Typically the optics consist of a dark smoked glass tile cemented to the wall of the bathroom, together with other smoked glass tiles. Such tiles have an appearance of ordinary black bathroom tiles, but afford the sensors with a view of a detection zone in the bathroom.

In other cases, the optics is a camera lens, which also provides a watertight seal in a cavity filling material such as an optical epoxy, so that there is no air gap in the camera between the lens and an image sensor. In this way the camera is sealed and completely water tight. Preferably the epoxy encapsulates the sensor as well as some processing circuits such as portions of the image capture devices.

Different kinds of optical elements are being used in EXISTech Corporation's experimental bathrooms. For example ceiling domes that provide the sensor with a wide field of view

1. See for example, http://wearcam.org/tpw_decon_summary.htm for sample images.

are being used for controlling a large number of bathroom fixtures with just one sensor. Many of the lowest cost cameras have wide angle lenses. A camera with a fisheye lens, such that when placed on the ceiling of a shower room, can monitor the entire shower room, and therefore a single sensor can be used to automatic several showers.

Users will enjoy a nice hot shower, without having to adjust the temperature, or even touch anything at all. Users simply step into the viewing area, or detection zone, and the shower turns on. Instantly, out comes water at the perfect temperature! When a user steps away to lather up with soap, the water turns off. When the user steps toward the spray head for a rinse, the water turns on again.

Process control systems ensure that water is circulated in the pipes at the right temperature, even when none of the showers are actually running. With face recognition software, users can receive their own preferred shower settings. Additionally, multiple spray heads at each station can spray a user with water in such a way that very little is wasted. A beam pattern of spray can adapt to the position and orientation of the user's body.

Pictures from a video capture device are directed to a processor which provides a signal to a controller. The controller activates one or more solenoid valve actuators. A shower room containing a dozen shower spray heads, each controlled by its own actuator comprised of a solenoid activated valve, may therefore be controlled by a single sensor on the ceiling of the shower room. Such a single

sensor is out of the way of vandalism, soap scum buildup, or other problems that would arise if a dozen sensors were distributed throughout the shower room, one for each shower head.

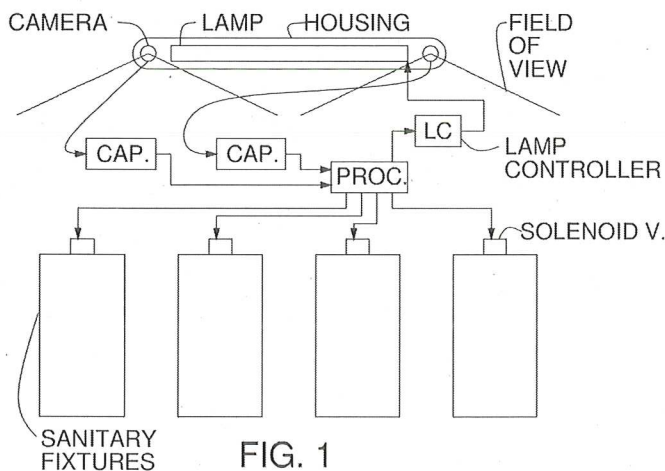
Moreover, maintenance and installation are simplified by having one image sensor controlling various shower spray heads. Additionally, the one image sensor may provide other features such as automatically warning building staff if a person has slipped and fallen, or automatically recognizing faces of users, and providing each user with water tempered to the preference of each individual user. The video based motion detection sensor will also act as a deterrent to crime and vandalism in the shower room.

A client/server model is implemented for all of the sensors in the smart bathroom for the creation of a global network of smart bathrooms. Each sensor may be implemented through Java applets. This permits any level of sophistication desired. While many installations are quite simple (e.g. little interprocess communication), the degree of interprocess and interfixture communication can be controlled remotely over the Internet. This is useful for monitoring usage patterns for generating statistics and for identifying areas of congestion in the restroom environment. By identifying areas of possible congestion, these problems can often be resolved with software. Systems can be reprogrammed to respond to users in slightly different ways, and therefore user behaviour can be modified slightly. Through slight modifications in user behaviour, efficiency and

restroom throughput can be increased. For example, the system might detect that, in a row of hand faucets, the furthest one is used excessively during certain times of day. It might be determined that a homeless person is using it for hair washing purposes, especially if it is somewhat hidden

from view. The system can detect this pattern of deviant use, and correct it by adjusting the timing on that particular fixture so that it will time out sooner than the others. This would effectively move that user to another faucet. Thus slight changes in system parameters can be used to effect slight changes in user behaviour.

Software, such as Java applets, allow restroom fixtures to communicate with each other, and to communicate with remote sites. Whether the building owner wants to delight users with responsive, predictive fixtures, or please users by keeping the restroom crime-free, the owner can be sure that everyone will be happier, and profits will increase. If crime ever does become a problem, sensors can transmit crime statistics back to a central law enforcement facility. Using Vitri-View™ ceramics for the optics can ensure outstanding image quality, and will provide excellent greyscale rendition and tonal fidelity, even in poor light. If crime is a problem, Cerami-View™ tiles can be replaced with SafetyGlass™ tiles (from EXISTech Corporation's public safety products division), which are known for their color rendition. Proper white balancing of the sensors to compensate for the greenish color cast of fluorescent lights or other bathroom fixtures will ensure forensic quality of the images for use in courtroom proceedings. As with all video-based machine vision technology, accurate color reproduction in the presence of mixed lighting (as when natural daylight entering through windows mixes with fluorescent lights) may be addressed with ATW (Auto Tracking White) sensors. Hair colour, eye colour, and even the colour of clothing are important identifiers of those who might, whether through vandalism or recklessness, reduce profits and the satisfaction of other users. Rapid apprehension of suspects is important to maintaining a crime-free airport, shopping mall, arena, or other establishment. Drug use will fall, and everyone will be happier, except those with something to hide, such as terrorists, thieves, or those engaged in other forms of criminal activity.



Additionally, the intelligent bathroom fixtures and systems will help enhance the privacy of users. Privacy enhancing fixtures and bathroom control systems ensure that normal users need not be disturbed by police foot patrols into the restroom areas, or by security guards entering simply to make inspections. Thus the aquionics bathroom control system of the invention will maintain the cleanliness, safety, security, and privacy of the occupants in a smart building. Aquionics refers to this kind of electronic control of water in plumbing systems.

Smart Bathroom Fixtures

Figure 1 depicts a smart light fixture consisting of a long fluorescent light fixture having two video sensors, one at each end. The light fixture, as shown in the figure, is mounted above a row of urinals. The sensors each have a clear view a detection zone where bathroom users might be standing in front of any one of the four urinals.

Because the lamp is generally hot, we find that the heat drives out any small amount of moisture present, or at least lowers the relative humidity since relative humidity decreases with increasing temperature inside the fixture.

Therefore the optics tends not to fog up due to bathroom moisture, even when placed in shower rooms.

The intelligent light fixture provides the advantage that the two cameras will be spaced an exactly known distance apart, and have an exactly known relative orientation. In this way, the epipolar geometry is known or determined in advance of installation. Thus the light fixture provides a conveniently calibrated stereo rig.

A typical lamp such as a fluorescent light has a convenient length that allows the two cameras to have a good baseline distance between them, so that they are nicely separated, yet the distance and orientation between them remain fixed by the intelligent light fixture.

Additionally, since the light from the light fixture is known in relation to the sensors, the stereo rig is also photocalibrated, in the sense that the light source distribution and orientation,

etc., are known with respect to the sensors.

The light fixture also contains infrared LEDs, so that it can communicate wirelessly with the actuators in the plumbing fixtures located below the light fixture.

In the figure, four urinals are shown, with a user standing at the urinal second from the right. When the user departs, as determined by the video sensors, the intelligent light fixture wirelessly sends a signal to the actuator of the urinal second from the right, to flush that urinal.

Additional functions of the intelligent light fixture can

be provided, such as to reduce crime, or to detect abnormal activity. An additional function may also be simply to automate the function of the light fixture itself, or to automate the function of other

light fixtures in the facility. Each intelligent light fixture communicates wirelessly with other intelligent light fixtures and, based on a map of where people are located in the bathroom, the light fixture outputs are gradually raised and lowered so that a lightspace is present around the persons in the bathroom, but light is not wasted. This system also avoids the abrupt start and stop of lights that might startle the bathroom user. Instead the lights gradually rise and fall in output, to track the users, so that users are not even aware they are being tracked. In a large bathroom facility such as a locker room complex, the benefit in light savings from video based tracking is provided together with intelligent control of many fixtures throughout the facility. The bathroom ventilation systems can also be incorporated into this system to provide for an intelligent energy-efficient facility.

The intelligent bathroom control system includes smart fixtures, smart

lighting, and other sensors that all communicate with one another to create a user-friendly environment.

Additional features include user safety and security, by way of watching the user to make sure that the user is attended to when encountering danger through tripping and falling, such as when slipping on a soapy shower room floor. Additional benefits to the occupants of such a building include reduced crime, reduced danger, and improved safety, security, and efficiency.

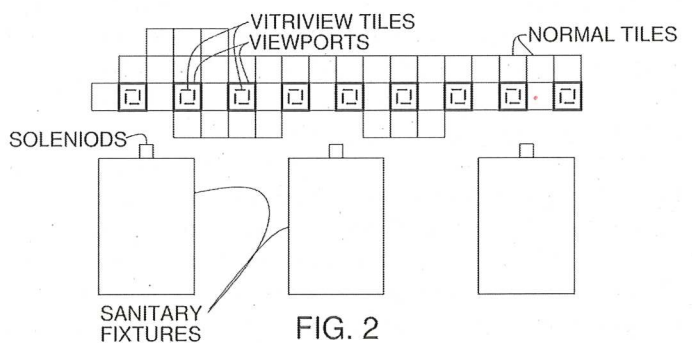


FIG. 2

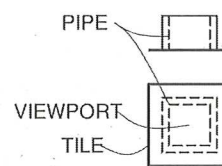


FIG. 2A

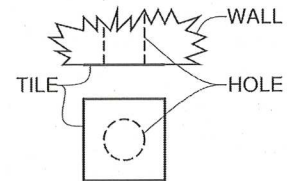
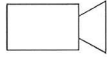


FIG. 2B

SmarTile™ Intelligent Bathroom Tile

Figure 2 shows the use of a SmarTile™ tile in an intelligent bathroom. SmarTiles™ manufactured by EXISTech Corporation, are available in black, chrome, gold, and copper, and add a nice accent to a tiled wall, such as a bathroom wall. The aesthetics of an otherwise stark wall of solid white tile is much improved with, for example, one or two rows of SmarTile black tiles.

In the installation show, there is behind-the-wall access. At the time of construction, a row of CeramiView™ tiles is run around the outside of the bathroom. The tiles comprise optics and viewport. Normal tiles such as plain white bathroom tiles look nice together with the CeramiView tiles.



Prior to installation of any tiles, it is decided at what height a row of SmartTile will be installed. Alternatively, especially if the viewtiles are to be mixed with ordinary white bathroom tile, two rows of SmartTile can be run for a better aesthetic, even if only one row of the tiles is going to be used for monitoring the bathroom environment. A double row creates a sense of visual balance.

In a typical installation, for example, over a row of urinals, there may be one row of SmartTile that runs just above where the urinals will be installed. This is the active row where the sensors are contained. A second row of SmartTile a couple of tiles further up, is often placed simply for aesthetics (e.g. none of these tiles need be used for viewing users of the urinals).

Once it has been decided where to place the view tiles, viewing holes are drilled in the bathroom wall. It is preferable that the view tiles then be cemented to the wall before cementing the other tiles to the wall. Preferably, before cementing the viewtiles to the wall, the wall, especially where the holes have been drilled, is cleaned and painted black.

After the viewtiles are cemented to the wall, regular tile (from another vendor, or from EXISTech Corp.) is installed around the SmartTile viewtiles.

With SmartTile, the sensors are completely hidden from view. Moreover, the users will not know which tiles have sensors behind them. Vandalism, whether arising from malicious hate of a better future, or simply arising from curiosity, costs us all. Through complete concealment of all sensory apparatus, vandalism is eliminated, resulting in increased savings, and increased profits. Moreover, in shower room applications, soap and shampoo that often splashes onto the wall and runs down the wall, will not get clogged into exposed lenses. Sensor products from other vendors

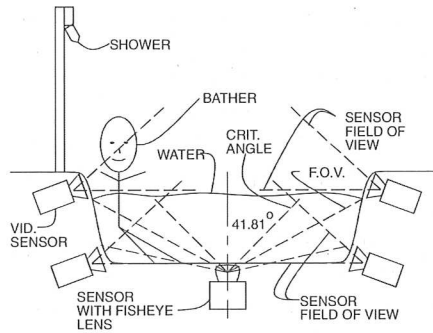


FIG. 3

quickly clog with soap residue, due to the inset lenses. Again, soapy lenses produce blurry images. A sharp clear view of bathroom users will keep them happy by delivering the utmost in fixture responsiveness and user-satisfaction.

High quality pictures assist facility managers in monitoring restroom usage patterns, to help reduce or eliminate deviant behaviour such as excessively long showering, shaving in the shower room, vagrancy, the washing of clothes in the shower room. Using the appropriate software, with artificial intelligence, management can be sure to maximize user satisfaction by making certain one inconsiderate user does not decrease the user-satisfaction of other users.

Additionally, a dense lattice of image sensors in the bathroom environment can have a large range of secondary uses. Web-based client/server software can ensure maximum efficiency, optimal traffic flow, and increased user-satisfaction. Users will appreciate the efforts taken to make their experience pleasant.

Moreover, dummy tiles can be installed, or viewtiles can be installed and never used, so that users will never know whether or not they are being watched by the intelligent building. The use of SmartTile simply because of its outstanding appearance and durability, thus provides additional safety and security. Simply installing SmartTile, even without any sensors whatsoever, will put an end to petty locker room pilfering, vandalism, or graffiti in bathrooms.

Drowning Prevention: Cameras Save Seconds and Lives

Figure 3 shows EXISTech's smart bath tub. Bath tubs and shower enclosures are often made of acrylic, or of polycarbonate. EXISTech tubs are made of smoked polycarbonate, or smoked acrylic, so that the bathtub itself forms the sensor's optics. Such a tub will have a black appearance to a user of the tub, but image sensors concealed under the tub will be able to see the user of the tub. Additional image sensors may also be concealed behind the dark transparent bath tub material in such a way that they provide a field of view of the bather above and below the waterline during a typical bath.

The intelligent bath tub has no knobs, or other adjustments, and is therefore much easier to use. The user simply undresses and sits in the tub, and then the tub fills with water automatically by way of activation of a solenoid valve actuator. Sensors also monitor the amount of water in the tub, and as the tub gets close to full, the water flow is gradually reduced. A sophisticated control system is possible without much cost, since the sensors and processors and controllers are already present.

Software running on the image processor and controller determines if the user is clothed (e.g. when a user is cleaning the tub) and only fills the tub when the user is not clothed (indicating that the user wishes to have a bath).

Additionally, if the system sees that the user is standing naked in the tub enclosure, the shower is turned on automatically. The distinction between shower and bath is made possible because the camera sensors allow the computer to distinguish between when a bather is sitting or standing.

Thus the intelligent bath tub serves users of the tub by way of control of various actuators in response to user activity.

Moreover, if the bather's head goes underwater, the system will also automatically drain the tub, to prevent drowning. Thus the intelligent bathroom can save lives.

The explanation of this tub has assumed that there is only one user, but the invention can also be applied

to multi user baths such as whirlpools, jacuzzis, steam rooms, and other bathing environments. For example, a bath can begin to fill when a user sits in the tub, and then jets can massage the user's body. If another user enters the tub, other jets can be activated for that other user. A pattern of jets can operate for optimal user satisfaction, given the distribution of users in the bath.

In a sauna bath, heat flow can be directed in response to the occupants of the sauna, so that the majority of users experience the best sauna bath that the bathroom environment can

by using other urine smuggled into the test center. With the Securinal™, however, the subject can enjoy complete privacy while urinating into a drug analysis urinal that also keeps a video record of the urine delivery process. In this way the subject can be completely alone while urinating, and this will serve useful especially for subjects suffering from shy bladder syndrome. Privacy is the right to be left alone, and thus Securinal greatly protects the privacy of individuals undergoing drug testing.

Smart Showers

Figure 4 shows a six station sensor operated column shower. Optics is comprised of a single sheet of smoked polycarbonate that was heated and bent around the outside circumference of the round column, and then inserted inside, after six viewing holes were drilled. Some further pictures of the sensor operated column shower in actual usage (men's shower room) are shown in

http://www.wearcam.org/dusting/tpw/bradley_column_shower.htm

A typical installation of this invention uses optics with approximately 15% transmissivity, so that the degree of light coming back from light that first passes into the viewing window and back out is 2.25%, which falls nicely below the 4% level of light reflected from typical such material. This allows color cameras to be used in as the motion sensors. When the column is used as a regular shower in a typical locker room setting, it can also double as a mass decontamination facility in times of emergency, thus having full color video feeds assists remote decon officers in determining, for example, if a powder on a patient's body is grey powder such as anthrax, or some other color of powder. In a typical installation, one such column is placed in the hexagonal men's shower room of a mass decontamination facility as described in Canadian Patent 02303611, whereas another is placed in the women's shower room. Since there are six cameras in each shower and six cameras in the central triage room described in Canadian Patent 02303611, there are a total of 18 cameras, which

can be displayed on two television sets as a 3 by 3 mosaic of images (a 9-up image on each TV). This allows two TV sets to be used, one for the men's side and the other for the women's side. A square lattice of images ensures the same aspect ratio of any one image, so that the images efficiently use the TV screen real estate at the decon officer's station.

An adhesive sealant makes the inside of the column water tight. Six video cameras are installed in the column with a 45 degree mirror on each one. Every second camera is pointing up from underneath, while the other three point down from above. A PC104 computer embodies video capture devices in the column to control the six separate solenoid valve actuators.

Appropriate software detects the presence of users, and turns on the appropriate showerheads where flesh is detected. In this way no water is wasted.

Conclusion

By using video based sensors, the intelligent bathroom provides a safe, hygienic, and user friendly environment that responds automatically to the needs of the user. Concomitant functions, such as security, drowning prevention, and other safety features are possible with the intelligent bathroom. It is assumed that the benefits of automation of fixtures will cause sensors to be installed in virtually all bathrooms of the future. It is also expected that the most economical sensors will be video cameras, which now only cost \$10 in mass production, whereas other sensors such as specialized infrared position sensing devices now used in electronic plumbing systems cost much more because they are specialized devices. Similarly radar and sonar systems commonly used for occupancy detection (for automatic door openers, lighting control, etc.) cost much more. Therefore once these cameras are installed in most bathrooms, new uses, such as automation of lighting, automatic bathroom door openers, automatic call for help in case of slip and fall injury, and automated drowning prevention will emerge.

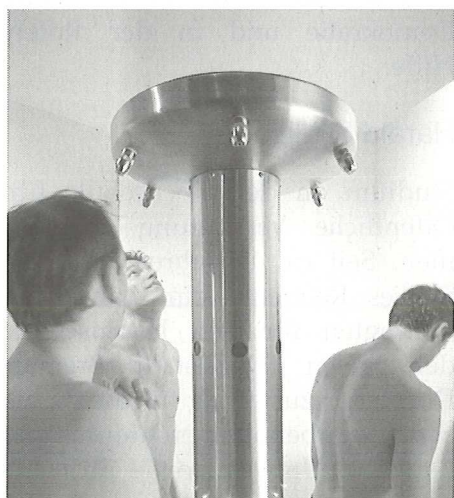


Fig. 4

provide, through intelligent control of air jets, heaters, and ventilation systems. Additionally, the system can detect the onset of drowning, hyperthermia, or slip and fall injuries, and respond appropriately by ejection of water, shutdown of the sauna or steam room heaters, and automated remote call for help.

The partially transparent material of the plumbing fixture of the invention is not limited to baths, but also includes other fixtures such as urinals and water closets. For example, a Securinal™ privacy-protecting drug testing urinal is made of smoked glass, and contains camera sensors to provide the automatic flush functionality, with a secondary concomitant function of protecting privacy. Privacy is a problem with drug testing because it is often necessary for persons to urinate in the presence of a supervisory staff member who ensures that the subject of the drug test does not cheat

Die Beteiligten am Schwerpunkt

Hubert Beste

Privatdozent für Soziologie am Fachbereich Gesellschaftswissenschaften der Universität Frankfurt/M. und wissenschaftlicher Angestellter am Institut für interdisziplinäre Konflikt- und Gewaltforschung (IKG) der Universität Bielefeld.

Peter Bittner

Studium der Informatik mit Nebenfach Wirtschaftswissenschaften an der Universität Kaiserslautern. Von 1996-2001 wissenschaftlicher Mitarbeiter an der TU Darmstadt im Zentrum für Interdisziplinäre Technikforschung. Seit Oktober 2001 wissenschaftlicher Mitarbeiter an der Humboldt-Universität zu Berlin in der Lehr- und Forschungseinheit »Informatik in Bildung und Gesellschaft«. Derzeit stellvertretender Vorsitzender des FIFF.

Wolfgang Föste

Dr. Wolfgang Föste ist Redakteur des kommunalpolitischen Online-Magazins Webwecker Bielefeld (www.webwecker-bielefeld.de).

Hardy Frehe

Studium der Philosophie und Elektrotechnik an der TU Darmstadt. Arbeitet zur Zeit an einer Promotion im Bereich Philosophie und an einer vom Zentrum für Interdisziplinäre Technikforschung (ZIT) Darmstadt geförderten Studie zur Videoüberwachung öffentlicher Plätze.

Leon Hempel

Leon Hempel studierte Neuere Deutsche Philologie, Vergleichende Literaturwissenschaft und Politikwissenschaft in Berlin. Seit 1999 ist er am Zentrum Technik und Gesellschaft (ZTG) der TU Berlin als Wissenschaftlicher Mitarbeiter beschäftigt. Von 1999-2001 arbeitete er im EU-Projekt *TeleCity-Vision*, das Wirkungszusammenhänge von Informationstechnologien und Stadtentwicklung untersuchte. Seit September 2001 ist er im vom ZTG koordinierten EU-Forschungsprojekt *Urbaneye* (<http://www.urbaneye.net>) zur Videoüberwachung im öffentlich zugänglichen Raum tätig.

Steve Mann

Steve Mann is considered by many to be the inventor of WearComp (wearable computer) and WearCam (eyetap camera and reality mediator). He is currently a faculty member at University of Toronto, Department of Electrical and Computer Engineering. He has recently published 2 new books (<http://wearcam.org/books.htm>) and a 35mm feature length motion picture film (<http://wearcam.org/cyberman.htm>) describes the apparatus of his invention.

Helmut Pollähne

Jahrgang '59, Dr. iur., wiss. Assistent am Institut für Kriminalpolitik der Universität Bremen, arbeitet derzeit an einer Habilitation zum Thema »Razzia zwischen Polizeirecht und Strafverfahrensrecht«; weitere Schwerpunkte: politisches Strafrecht, Kriminolo-

gie und Kriminalpolitik, Strafvollzug und Forensische Psychiatrie; seit dem erfolgreichen Widerstand gegen die Volkszählung 1983 in Bielefeld politisch aktiv in Sachen Datenschutz, Überwachung, BürgerInnenrechte; u.a. Mitglied im Komitee für Grundrechte und Demokratie und in der Roten Hilfe.

Harald Stelljes

Studium an der Hochschule für Öffentliche Verwaltung in Bremen. Seit ca. 10 Jahren ist Herr Stelljes Referent beim Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen. Dort ist er zuständig für die Bereiche Arbeitnehmerdatenschutz, Bau und Umwelt sowie Straßenverkehr.

Julia Stoll

ist Diplom-Informatikerin und z.Zt. Promotionsstudentin an der TU Darmstadt. In Teilzeit arbeitet sie bei der Firma SuSE in Nürnberg. Zudem ist sie Mitglied im Vorstand des FIFF, da sie nicht nur im produktiven Sinn mitgestalten möchte, sondern ihr auch die soziale Komponente ihres Handelns wichtig ist.

Rena Tangens & padeluun

sind Künstlerin und Künstler und leben in Bielefeld. Gründeten 1984 das Galerie- und Kunstprojekt »Art d'Ameublement«. Brachten 1987 das erste Modem auf die documenta (d8) und die Häcksen in den Chaos Computer Club. Seit 1987 Kurator und Kuratorin der monatlichen Kultur- und Techno-

logie-Veranstaltungsreihe 'PUBLIC DOMAIN' und Mitbegründer der BIONIC-MailBox und des FoeBuD e.V. in Bielefeld. Aufbau der Bürgernetze Z-NETZ und /CL sowie Zamir Transnational Network in Ex-Jugoslawien. 1990-1996 Softwaregestaltung für das MailBox-Programm ZERBERUS. 1993 Veröffentlichung des deutschen Handbuchs zum Verschlüsselungsprogramm PGP (Pretty Good Privacy). Forschung zum Thema Androzentrismus im Netz. Seit 2000 Organisatorin und Mitglied der Jury der deutschen Big Brother Awards.

Eric Töpfer

ist Diplom-Politologe und arbeitet zur Zeit als wissenschaftlicher Mit-

arbeiter am Zentrum Technik und Gesellschaft (ZTG) der Technischen Universität Berlin in dem von der Europäischen Kommission finanzierten Forschungsprojekt *Urbaneye: On the Threshold to Urban Panopticon?*

Thilo Weichert

Dr. Thilo Weichert, 46 Jahre alt, Jurist und Politologe. Er ist Vorsitzender der Deutschen Vereinigung für Datenschutz (DVD) und stellv. Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

Jens Woinowski

Informatik-Studium an der TU Darmstadt, danach dort wissenschaftlicher Mitarbeiter und Pro-

motion zum Dr. rer.nat. in Theoretischer Informatik. Seit Oktober 2001 Senior Software Ingenieur bei sd&m AG, software design & management, München.

Rolf P. Würtz

Studium der Mathematik an der Universität Heidelberg. Danach Mitarbeiter am MPI für Hirnforschung in Frankfurt, am Institut für Neuroinformatik (INI) der Ruhr-Universität Bochum, und an der Fakultät für Informatik der Universität Groningen. Promotion 1994 über automatische Gesichtserkennung. Seit 1997 leitender wissenschaftlicher Mitarbeiter und Dozent am INI mit Forschungsprojekten in Computersehen und Robotik.

Wir trauern um

Ingrid Engelke

gestorben am 20. Februar 2002

Mit großer Erschütterung haben wir von ihrem plötzlichen Tod erfahren. Ingrid betreute von 1999 bis 2000 in Medemstade die FIFF-Geschäftsstelle und bleibt uns mit ihrer optimistischen und lebensfrohen Art in Erinnerung. Wir haben in ihr eine Freundin und Kollegin verloren.

Der Vorstand des FIFF

*Uns gehört nur die Stunde. Und eine
Stunde, wenn sie glücklich ist, ist viel.
Nicht das Maß der Zeit entscheidet, wohl
aber das Maß des Glücks.*

Theodor Fontane

Peter Bittner

Sicher ist sicher ...

Zum sogenannten Terrorismusbekämpfungsgesetz

»Der Sinn von Politik ist Freiheit«
(Hannah Arendt)

Der hier unter einem Motto Hannah Arendts zusammengestellte Beitrag basiert¹ auf der Stellungnahme »Schilys Terrorismusbekämpfungsgesetz: Der falsche Weg.« von Bürgerrechtsorganisationen zur Anhörung des Innenausschusses des Deutschen Bundestages am 30. November 2001 zum Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz). Die gesamte Stellungnahme ist erschienen innerhalb der Bundestagsdrucksache 14/7386. Sie ist unter <http://www.cilip.de/terror/> zugänglich im HTML-Format bzw. als PDF-Version zum Download. Das FIFF gehört zu den unterstützenden Organisationen dieser Stellungnahme, die die bürgerrechtsbewegte Kritik am sogenannten Terrorismusbekämpfungsgesetz bisher am besten bündelt. Wegen des »unerhörten« Tempos im Gesetzgebungsverfahren, mußte diese Stellungnahme innerhalb weniger Tage zusammengetragen werden – das sollten die Leserinnen und Leser wissen.

Staatliche Überwachung und gesetzgeberische Kontinuität

Das Gesetz zur Bekämpfung des internationalen Terrorismus² (ein Artikelgesetz, das viele andere Gesetze

ändert) passierte am 14.12.2001 den Bundestag und kurz darauf am 20.12.2001 den Bundesrat. Dabei war die im Gesetzgebungsverfahren an den Tag gelegte Hektik wirklich nicht nachvollziehbar. In seiner Stellungnahme³ (Brief vom 27.11.2001) für die öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 30.11.2001 drückt dies der Bundesvorsitzende der Humanistischen Union Dr. Till Müller-Heidelberg sehr passend aus:

»Angesichts der Tatsache, daß keine einzige der im Gesetzesentwurf vorgeschlagenen Maßnahmen den Anschlag vom 11. September 2001 in den USA verhindert hätte und darüber hinaus (mit Ausnahme der vorgeschlagenen Änderungen des Luftverkehrsgesetzes) fast keine Maßnahme im Gesetzesentwurf mit Terrorismusbekämpfung etwas zu tun hat, ist dieser Zeitdruck nicht nur unangemessen, sondern auch völlig überflüssig.«

Im aktuellen Sicherheitspaket drücken sich eher Tendenzen der Innen- und Rechtspolitik aus, die die gesamten 90er Jahre prägten. Diese Tendenzen lassen sich am besten an den Begriffen Sicherheits- oder Krisenbekämpfungsstaat festmachen und zeitigen in der Summe schwerwiegende Eingriffe in rechtsstaatliche Grundsätze⁴. Beispielhaft lässt sich dies an den verdachtsunabhängigen Abhör- und Datenübermittlungskompetenzen des Bundesnachrichtendienstes nachvollziehen. Die durch das Verbrechensbe-

kämpfungsgesetz 1994 eingeführte Befugnis wurde nach dem entsprechenden Urteil des Bundesverfassungsgerichts vom 14.07.1999 durch die rot-grüne Regierung Anfang 2001 teilweise neu gefasst. Zu dieser Neufassung hatten DVD (Deutsche Vereinigung für Datenschutz e.V.) und RAV (Republikanischer Anwälten- und Anwälteverein) in einer gemeinsamen Presseerklärung ausgeführt, dass sich das Artikel-10-Gesetz »verschlimmbessert« hätte. Bündnis 90/ Die Grünen hätten den Kampf gegen die Vergeheimdienstlichung der inneren Sicherheit aufgegeben im Tausch gegen einige datenschutzrechtliche Verbesserungen. Das G10-Gesetz weist dieselbe Richtung auf wie das »Schily-Sicherheitspaket«: geheimdienstliche und polizeiliche Strukturen werden geschaffen und auf den jeweiligen Bestand moderner Technologien gebracht, nicht unbedingt um aktuell bei inneren und äußeren Konflikten zu intervenieren, sondern um »auf Vorrat« Verfahren und Ermächtigungen bereitzuhalten, die nach Gutdünken der Apparate der Inneren Sicherheit eingesetzt werden können [1.1].

Damit korrespondiert eine mittlerweile fast 15-jährige Tradition von Gesetzesaktivismus und symbolischer Politik im Bereich des Strafrechts und des Polizeirechts. Nach dem Wegfall der Blockkonfrontation und dem Ende des Kalten Krieges wurde jede sich bietende Gelegenheit genutzt, um innere und äußere Bedrohungen wie organisierte Kriminalität, Einheitskriminalität, Betäubungsmittelkriminalität, Rechtsradikalismus, Hooligans oder Sexualstraftaten zum Anlass zu nehmen, um Gesetzesänderungen mit teilweise weitreichenden Folgen durchzusetzen. Nur zwei Beispiele: Das DNA-Feststellungsgesetz wurde unter dem Eindruck von schwersten

1. Der Autor dankt für die Möglichkeit der Nutzung der Quellen aus der gemeinsamen Stellungnahme der Bürgerrechtsorganisationen. Insbesondere geht der Dank an Wolfgang Kaleck (Republikanischer Anwälten- und Anwälteverein), von dem das Kapitel 1 der Stellungnahme stammt, an Dieter Hummel (Vereinigung Demokratische Juristinnen und Juristen) für die SÜG-Analyse in Kapitel 3 und an Wolf-Dieter Narr (Komitee für Grundrechte und Demokratie) für sein Resümee (Kapitel 9 der Stellungnahme). Einzelzitate werden i.d.R. nicht ausgewiesen, Bezugnahme erfolgt nur auf die Kapitel innerhalb der Stellungnahme. Die zugehörigen Kapitel/Abschnitte sind in eckigen Klammern [] zur leichteren Orientierung in der Originalquelle an den jeweils passenden Stellen vermerkt.

2. Kurz: Terrorismusbekämpfungsgesetz

3. ebenfalls abgedruckt in der schon erwähnten BT-Drucksache 14/7386.

4. Hierzu gehören ein Schuldstrafrecht und klar ausgewiesene Strafzwecke, enge strafprozessuale Eingriffsvoraussetzungen, klare polizeirechtliche Ermächtigungsgrundlagen und eine der Rechtsweggarantie des Grundgesetzes gerecht werdende gerichtliche Kontrolle.

Sexualstraftaten geschaffen, mittlerweile muss sich jeder Strafverteidiger fast alltäglich mit Anordnungen von DNA-Feststellungen wegen Körperverletzungen oder politischer Delikte wie Landfriedensbruch auseinandersetzen. Die drastischen Maßnahmen, die gegen Hooligans im Passgesetz beschlossen wurden, nämlich Passbeschränkungen und Meldeauflagen, wurden im Sommer 2001 erstmals im größeren Umfang gegen Globalisierungskritiker im Vorfeld der Treffen in Salzburg und Genua eingesetzt [1.1].

Selbst wenn bei Einführung bestimmter gesetzlicher Maßnahmen eine breite Anwendung der Gesetze nicht durchsetzbar ist, sind die technischen und organisatorischen Strukturen zunächst geschaffen und können dann entweder in der Verwaltungspraxis oder durch weitere Gesetzesänderungen auf eine Vielzahl von ursprünglich nicht erfassten Fällen ausgeweitet werden. Dies alles ist seit Jahren bekannt und wird von Berufsverbänden sowie kritischen Kommentatoren immer wieder beanstandet [1.1].

Übertroffen wird diese Entwicklung durch die »Schily-Sicherheitspakete« vom Herbst 2001. Unter dem Titel Terrorismusbekämpfung wurden zahlreiche Gesetze geändert, die mit Terrorismusbekämpfung von vornherein nichts zu tun haben und die vor allem in ihrer Anwendung von vornherein nicht auf »Terrorismusbekämpfung« beschränkt sind [1.1].

Fehlende Geeignetheit und fehlende Verhältnismäßigkeit

Absurderweise hat sich in der Öffentlichkeit die Diskussion nach dem 11.9.2001 teilweise so entwickelt, dass nicht der Staat und die Befürworter eines repressiven Vorgehens die geplanten Maßnahmen akribisch begründen und dann gemessen an dem Verhältnismäßigkeitsprinzip (Geeignetheit der Maßnahme zur Terrorismusbekämpfung, Erforderlichkeit und Verhältnismäßigkeit in Bezug auf die Grundrechte) rechtfertigen müssen. Vielmehr werden die Kritiker solcher Gesetzgebungsvorhaben immer wieder dazu aufgefordert,

doch eigene Vorschläge zu machen, denn, so lautet das Totschlagargument, »man müsse doch schließlich angesichts dieser Bedrohung etwas tun« [1.2].

Dieser Einwand geht grundlegend an der Sache vorbei. Der Staat ist stets nachweis- und begründungspflichtig für Grundrechtseingriffe und dieser Nachweis- und Begründungspflicht ist das Bundesinnenministerium bis heute nicht nachgekommen. In der Begründung (hier nach S. 84 des Gesetzentwurfes) heißt es, das Gesetz beinhalte:

»die für eine entschlossene, aber auch wirkungsvolle Bekämpfung des internationalen Terrorismus dringend erforderlichen Maßnahmen. Hierzu bedarf es der Anpassung zahlreicher Sicherheitsgesetze, wie des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des Bundesgrenzschutzgesetzes, des Bundeskriminalamtgesetzes, aber auch des Ausländergesetzes und anderer ausländerrechtlicher Vorschriften. Der Schwerpunkt der Gesetzesänderungen liegt darin, den Sicherheitsbehörden wie dem Bundesamt für Verfassungsschutz, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, dem Bundesgrenzschutz und dem Bundeskriminalamt die nötigen gesetzlichen Befugnisse zu geben.«

Bereits am 17.10.2001 hat das Bundesjustizministerium hat in einer Stellungnahme (Seite 3) darauf hingewiesen, dass es im Hinblick auf den Titel »Terrorismusbekämpfungsgesetz« angeraten sei, »den Gesetzentwurf auch tatsächlich auf Maßnahmen zur Bekämpfung des Terrorismus zu beschränken«. Der Bundesbeauftragte für den Datenschutz hat in seiner Stellungnahme vom 23.10.2001 beispielhaft unter Ziffer 5 zu den (vorgesehenen) Änderungen im Paß- und Personalausweisgesetz bemerkt,

»daß es sich in den beiden Gesetzen um Änderungen handelt, die nur schwerlich in einen Zusammenhang mit der mit diesem Gesetzentwurf beabsichtigten Bekämpfung des internationalen Terrorismus zu

bringen sind. Es handelt sich um Sicherheitsbestrebungen im Bereich der deutschen Ausweisdokumente, die ohne konkrete Darlegung der geplanten Maßnahmen lediglich die Tür für das technisch Mögliche öffnen. Es sind daher keine Gründe zu erkennen, die gegen eine Behandlung dieser Fragen in einem eigenen Gesetzesverfahren ohne den jetzt erkennbaren Zeit- und Beratungsdruck sprechen würden.«

In einer gemeinsamen Erklärung vom 26.10.2001 verkündeten die Datenschutzbeauftragten des Bundes und der Länder im Rahmen ihrer 62. Datenschutz-Konferenz (Münster):

»Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist.«

Im Spiegel vom 05.11.2001 war sogar vom Bund Deutscher Kriminalbeamter (BDK) mit Blick auf das »Schily-Sicherheitspaket« zu lesen: »(...) Wir brauchen eine kritische Fachdiskussion und keine politische Kraftmeierei«.

Die Zweifel an der Erforderlichkeit, der Verhältnismäßigkeit und der Geeignetheit der vorgeschlagenen Maßnahmen wurden bisher nicht ausgeräumt. Besonders schwer wiegt – und dies macht das Terrorismusbekämpfungsgesetz so gefährlich –, dass viele der Maßnahmen auch im engeren Sinne unverhältnismäßig sind, also der Ertrag den angerichteten Schaden für die Grundrechte vieler tausender Menschen und den sozialen demokratischen Rechtsstaat als Ganzes nicht aufwiegen kann [1.2].

Ins Detail ...

kann ich an dieser Stelle nicht gehen, da es sich bei diesem »Gesetzesmachwerk« (nachzulesen im Bundesgesetzblatt Jahrgang 2002 Teil I Nr. 3, ausgegeben zu Bonn am 11.01.2002) um ein Artikelgesetz handelt und dieses in zahlreiche Vorschriften bzw. Gesetze eingreift⁵.

Hier möchte ich beispielhaft näher auf die Änderungen eingehen⁶, die

das Sicherheitsüberprüfungsgesetz (SÜG) betreffen, ein Bereich der viele ArbeitnehmerInnen betreffen wird und in dem sich relativ schnell Wirkungen des Gesetzes zeitigen werden. Aktuell formiert sich der gewerkschaftliche Widerstand gegen diese Gesetzesänderung.

Die Auswahl soll nicht dokumentieren, dass die anderen Änderungen nicht bedeutsamer wären (z.B. Vermischung von Geheimdiensten und Polizei, viel restriktiveres Ausländer- und Asylrecht, Eingriffe in das Recht auf informationelle Selbstbestimmung).

Ausweitung der Sicherheitsüberprüfungen

Die bisherige rechtliche Situation

[3.1] Das bisherige Gesetz dient nach der Begründung des seinerzeitigen Gesetzentwurfs alleine dem Geheimnisschutz. Schützenswerte Geheimnisse sollten vor der Offenbarung geschützt werden. Demnach war nach der bisherigen Gesetzeslage die Sicherheitsüberprüfung nach § 1 SÜG konsequenterweise grundsätzlich beschränkt auf Beschäftigte des öffentlichen Dienstes, die im Rahmen ihrer Tätigkeit Zugang zu sicherheitsrelevanten Daten hatten. Nach § 24 SÜG unterlagen weiter Beschäftigte, die bei nicht-öffentlichen Einrichtungen tätig wurden, nur dann der Sicherheitsüberprüfung, soweit sie dort zu sicherheitsempfindlichen Tätigkeiten

durch die zuständige Stelle ermächtigt waren.

Damit bleibt festzuhalten, dass nach bisherigem Recht nur ein sehr eingegrenzter Teil von Beschäftigten des öffentlichen Dienstes einer Sicherheitsüberprüfung unterzogen werden konnte.

Gesetzeslage nach der Änderung

[3.2] Die Bundesregierung beabsichtigte, mit der Gesetzesänderung den Personenkreis, der sicherheitsüberprüft werden kann, über den bisherigen Bereich hinaus zu öffnen und auf Beschäftigte bei Privatunternehmen zu erstrecken. Einfallstor sind die neuen Absätze 4 und 5 des § 1 des SÜG:

»(4) Eine sicherheitsempfindliche Tätigkeit übt auch aus, wer an einer sicherheitsempfindlichen Stelle innerhalb einer lebens- oder verteidigungswichtigen Einrichtung oder wer innerhalb einer besonders sicherheitsempfindlichen Stelle des Geschäftsbereiches des Bundesministeriums der Verteidigung (»Militärischer Sicherheitsbereich«) beschäftigt ist oder werden soll (vorbeugender personeller Sabotageschutz).

(5) Lebenswichtig sind solche Einrichtungen, 1. deren Beeinträchtigung auf Grund der ihnen anhaftenden betrieblichen Eigengefahr die Gesundheit oder das Leben großer Teile der Bevölkerung erheblich gefährden kann oder 2. die für das Funktionieren des Gemeinwesens unverzichtbar sind und deren Beeinträchtigung erhebliche Unruhe in großen Teilen der Bevölkerung und somit Gefahren für die öffentliche Sicherheit oder Ordnung entstehen lassen würde.

Verteidigungswichtig sind außerhalb des Geschäftsbereiches des Bundesministeriums der Verteidi-

gung solche Einrichtungen, die der Herstellung oder Erhaltung der Verteidigungsbereitschaft dienen und deren Beeinträchtigung auf Grund 1. fehlender kurzfristiger Ersetzbarkeit die Funktionsfähigkeit, insbesondere die Ausrüstung, Führung und Unterstützung der Bundeswehr und verbündeter Streitkräfte sowie der Zivilen Verteidigung, oder 2. der ihnen anhaftenden betrieblichen Eigengefahr die Gesundheit oder das Leben großer Teile der Bevölkerung erheblich gefährden kann.

Sicherheitsempfindliche Stelle ist die kleinste selbstständig handelnde Organisationseinheit innerhalb einer lebens- oder verteidigungswichtigen Einrichtung, die vor unberechtigtem Zugang geschützt ist und von der im Falle der Beeinträchtigung eine erhebliche Gefahr für die in Satz 1 und 2 genannten Schutzgüter ausgeht.«

Welche Wirtschaftsbereiche unter § 1 Abs. 4 und 5 SÜG fallen, wird nach § 34 SÜG durch eine Rechtsverordnung der Bundesregierung festgelegt. Nach der Begründung des Änderungsgesetzes sollen darunter Einrichtungen verstanden werden, die für

»die Versorgung der Bevölkerung (z.B. Energie, Wasser, pharmazeutische Firmen, Krankenhäuser, Banken) dienen oder die für das Funktionieren des Gemeinwesens (z.B. Telekommunikation, Bahn, Post, Rundfunk- und Fernsehanstalten) notwendig sind.«

Entscheidend für die Sicherheitsempfindlichkeit einer Stelle ist lediglich, dass im hypothetischen Sabotagefall Ausfälle mit Folgen für die nach dem Gesetz geschützten Güter drohen. »Unverzichtbar« sind in diesem Zusammenhang Einrichtungen, deren Ausfall in Krisenzeiten erhebliche Unruhe in großen Teilen der Bevölkerung und somit eine Bedrohung der öffentlichen Ordnung entstehen lassen würden.

Das Gesetz verschleierte damit in seinem Wortlaut, wie niedrig die Schwelle zur Sicherheitsrelevanz gelegt werden kann. Der Personenkreis, der sich zukünftig möglicherweise einer Sicherheitsüberprüfung

5. Es geht um Änderungen des Bundesverfassungsschutzgesetzes (Art. 1), des MAD-Gesetzes (Art. 2), des BND-Gesetzes (Art. 3), des Artikel 10-Gesetzes (Art. 4), des Sicherheitsüberprüfungsgesetzes (Art. 5), des Bundesgrenzschutzgesetzes (Art. 6), des Passgesetzes (Art. 7), des Gesetzes über Personalausweise (Art. 8), des Vereinsgesetzes (Art. 9), des Bundeskriminalamtgesetzes (Art. 10), des Ausländergesetzes (Art. 11), des Asylverfahrensgesetzes (Art. 12), des Gesetzes über das Ausländerzentralregister (Art. 13), der Verordnung zur Durchführung des Ausländergesetzes (Art. 14), der Ausländerdateienverordnung (Art. 15), der AZRG-Durchführungsverordnung (Art. 16), des Bundeszentralregistergesetzes (Art. 17), des Zehnten Buches Sozialgesetzbuch (Art. 18), des Luftverkehrsgesetzes (Art. 19), Luftverkehrszuverlässigkeitsüberprüfungsverordnung (Art. 19a) sowie des Energiesicherungsgesetzes 1975, der Elektrizitätslastverteilungsverordnung und der Gaslastverteilungsverordnung (Art. 20).

6. An dieser Stelle habe ich Dieter Hummel (Vereinigung Demokratische Juristinnen und Juristen) zu danken, der die Änderungen am SÜG in Kapitel 3 der gemeinsamen Stellungnahme so tiefgehend analysiert hat. Ich übernehme hier seine Ausführungen, habe aber für diesen Beitrag redaktionelle Kürzungen vorgenommen und die Ausführungen mit Bezug auf den realisierten Gesetzestext aktualisiert.

unterziehen muss, wird ausgeweitet auf z.B. Journalisten bei Funk und Fernsehen, Krankenschwestern, Chemiker bei Pharmaunternehmen, Monteure bei der Telekom, Arbeiter bei der Post bis womöglich auf die Arbeiter bei Kleinfirmen, die im Auftrag von Elektrizitätsfirmen oder Wasserbetrieben tätig sind. Zuständig für diese Sicherheitsüberprüfung gem. § 25 Abs. 2 SÜG (neu) soll dasjenige Bundesministerium sein, dessen Zuständigkeit durch die Bundesregierung bestimmt wird.

Für den hier in Frage stehenden Personenkreis soll es bei der »Einfachen Sicherheitsüberprüfung« nach § 8 Abs. 1 Nr. 3 SÜG bleiben. Für eine solche Sicherheitsüberprüfung hat der Beschäftigte dann zunächst eine Sicherheitserklärung nach § 13 SÜG abzugeben. In dieser Sicherheitserklärung hat er eine Vielzahl von persönlichen Angaben zu machen, u.a. Angaben zu den bisherigen Wohnsitzen, Ausbildungs- und Beschäftigungsstellen, über Zwangsvollstreckungen und finanzielle Verpflichtungen, Beziehungen zu verfassungsfeindlichen Organisationen, Beziehungen zu und in Staaten, die als Sicherheitsrisiko eingestuft sind. Es können bedingt auch die Lebenspartner einbezogen werden. Im Verfahren kann als mitwirkende Stelle auch das Bundesamt für Verfassungsschutz Einblick in die Personalakte erlangen. Bestehen Zweifel an der Zuverlässigkeit der Person, dann ist das Arsenal der intensiveren Überprüfungen weitläufig. Es beginnt mit Abfragen bei den Verfassungsschutzbehörden der Länder, an das BKA, die Nachrichtendienste des Bundes bis hin zu der Einholung von Auskünften bei der Staatsanwaltschaft oder Gerichten.

Hierbei hat das Sicherheitsinteresse nach § 14 Abs. 3 SÜG Vorrang vor anderen Belangen, also auch den Belangen des Beschäftigten. Das Ergebnis der Überprüfung ist dem Betroffenen mitzuteilen. Ihm ist vor einer abschließenden Entscheidung Gelegenheit zur Äußerung zu geben. Allerdings ist die Anhörung so durchzuführen, dass »der Quellenschutz gewährleistet« ist. Das bedeutet, dass man sich gegen anonyme Anschuldigungen kaum wehren kann. Nach § 11

SÜG steht den jeweiligen Behörden das Recht zu, alle erforderlichen Daten zu erheben.

Was das SÜG bedenklich macht ...

[3.3] Das SÜG dient nicht mehr – wie bisher – dem Geheimnisschutz, sondern wird auf den »vorbeugenden personellen Sabotageschutz«, so der Gesetzestext selbst, erweitert. Damit handelt es sich jedoch um Regelungen hinsichtlich der allgemeinen Gefahrenabwehr. Demnach liegen die Kompetenzen für diesen Bereich nach der verfassungsmäßigen Ordnung der Bundesrepublik nicht beim Bund, sondern bei den Ländern zustehen.

Die vorliegenden Regelungen sind zu unbestimmt und damit verfassungsrechtlich bedenklich. § 34 SÜG (neu) enthält die Ermächtigung an die Bundesregierung, mittels einer Rechtsverordnung diejenigen Bereiche festzulegen, die unter § 1 Abs. 4 und 5 SÜG (neu) fallen sollen. Nach Art. 80 Abs. 1 GG sind in dem Gesetz, das die Ermächtigung zum Erlass einer Rechtsverordnung enthält, Inhalt, Zweck und Ausmaß der erteilten Ermächtigung zu bestimmen. Nach der Wesentlichkeitstheorie des Bundesverfassungsgerichts hat das Gesetz, je intensiver in die Grundrechte eingegriffen wird, umso bestimmter zu sein. Diesen Anforderungen wird das Gesetz zur Änderung der Sicherheitsüberprüfung nicht gerecht. Die Begriffe »lebens- oder verteidigungswichtige Einrichtungen«, »erhebliche Gefährdung für die Gesundheit oder das Leben von großen Teilen der Bevölkerung« zu »befürchten« oder »Funktionieren des Gemeinwesens« sind viel zu unbestimmt. Es sind keine abgrenzenden Kriterien möglich. Warum sollen nicht auch der öffentliche Nahverkehr einer Großstadt oder nicht auch die Printmedien darunter fallen?

Die Maßnahme steht in keinem Zusammenhang mit den terroristischen Angriffen. Nach den Vorschriften ist die flächendeckende Überprüfung aller Beschäftigten nach den bisher für die Sicherheitsüberprüfung geltenden Vorschriften geplant. Irgendwelche Einschränkungen auf bestimmte Personengruppen sind

nicht vorgesehen. Jeder ist verdächtig und soll in den großen Datenspeicher der Sicherheitsbehörden. Achtung! Das Bundesamt für Verfassungsschutz darf Sicherheitsüberprüfungsdaten auch zu anderen nachrichtendienstlichen Zwecken verwenden.

Angesichts der Menge der geplanten Überprüfungen – in den angesprochenen Einrichtungen und Bereichen ist ein großer Teil der arbeitenden Bevölkerung beschäftigt, hinzu kommen deren Ehepartner oder Lebensgefährten – entsteht hier eine Datensammlung über einen großen Teil der Bevölkerung der Bundesrepublik, der über das regelmäßige Wiederholen der Sicherheitsüberprüfungen immer aktuell gehalten wird. Die Betroffenen selbst sind verpflichtet, etwaige Veränderungen mitzuteilen.

Nicht zu vergessen ist, dass auch die Arbeitgeber Informationen über ihre Beschäftigten erlangen, die sie unter arbeitsrechtlichen Aspekten nicht erfahren dürften. Hier ist insbesondere auf die Auskunft hinsichtlich jeder Art von Strafverfahren, auf finanzielle Verhältnisse oder Lebensverhältnisse (mit wem wohne ich in welcher rechtlichen Art zusammen) hinzuweisen. Das Trennungsgebot des § 25 Abs. 2 SÜG dürfte gerade dann, wenn vielleicht dieselben Sachbearbeiter der in Klein- und Mittelbetrieben vielleicht sogar der Inhaber der Firma selbst für die Personalverwaltung und die Sicherheitsüberprüfung gleichermaßen zuständig ist, ins Leere gehen. Von niemandem kann verlangt werden, dass er erlangtes Wissen in konkreten Situation nicht automatisch mit berücksichtigt.

Für eine durch das Gesetz nicht begrenzte Anzahl von Arbeitnehmern wird durch diese Gesetzesänderung nunmehr nicht mehr alleine durch den Arbeitgeber und unter anderen Aspekten als bisher über ihre beruflichen Möglichkeiten entschieden. Staatliche Stellen nehmen Einfluss auf die Möglichkeit, in privaten Wirtschaftsbereichen eine Beschäftigung zu finden. Diese Einflussnahme ist aufgrund des normierten Quellenschutzes nicht wirklich überprüfbar und setzt den Beschäftigten einer willkürlichen Behandlung aus. Rechtsschutz gegen die Ergebnisse von

Sicherheitsüberprüfungen ist praktisch nicht zu erlangen. Wie will sich ein Beschäftigter im Fall der Kündigung aus »sicherheitspolitischen« Überlegungen denn wehren, wenn er im Kündigungsschutzverfahren nicht einmal die tatsächlichen Grundlagen der Entscheidung angreifen kann, da sie ihm nicht offengelegt werden müssen? Die nachrichtendienstliche Zwangsbewirtschaftung von Arbeitsplätzen lässt zudem erwarten, dass Ausländerinnen und Ausländer, die unter Umständen weniger flächendeckend auf ihre sicherheitspolitische Zuverlässigkeit hin überprüft werden können, auch die Sicherheitsüberprüfung nicht bestehen können. Mit dieser Verdrängung aus bisher zugänglichen Beschäftigungsbereichen setzt sich das Gesetz potentiell auch in Widerspruch zum Europäischen Gemeinschaftsrecht.

Heiße Nadeln nähen gesetzlich allemal kontraproduktiv

Wolf-Dieter Narr faßt in seiner rechtsstaatlichen Summe (siehe Kapitel 9 der gemeinsamen Stellungnahme) die Kritik prägnant zusammen:

»Dem antiterroristischen Gesetzespotpourri (...) fehlt zum einen die zureichende Begründung (1.); ob es darum antiterroristisch irgend nützt ist überaus fraglich (2.); es ist dagegen eindeutig und klar rechtsstaatswidrig, wird der Rechtsstaat von seinem Fundament und Hauptbezug: den Grund- und Menschenrechten her – mitsamt den Artikeln 1 und 20 GG – verstanden (3.). Das Gesetzespaket beeinträchtigt die ohnehin prekär schwache parlamentarische Kontrolle, es hebt die so notwendige inneradministrative Kontrolle weiter aus (4.); es schaltet die Bürgerinnen und Bürger der Bundesrepublik Deutschland antiterroristisch gleich und degradiert Ausländerinnen und Ausländer zu willkürlich zu traktierenden Sicherheitsobjekten (5.); Polizei und Geheimdienste werden noch näher aneinander gerückt, der Datenschutz wird in Sachen inne-

rer Sicherheit und nicht nur innerer Sicherheit nahezu aufgegeben, entgegen dem verfassungsorganisationsföderalistischen Wesenselement und ohne erkennliche Notwendigkeit wird die Gestalt einer Bundespolizei in Form des BGS nahezu fertig gezimmert (6.). Am schlimmsten jedoch sind die (...) »Grundtöne«, die alle geplanten gesetzlichen Änderungen durchdringen und vereinheitlichen.«

Das Gesetzespaket

- » • fördert zum ersten die Ausländerfeindlichkeit, die ihrerseits zum erneuten Anlass werden mag, die ausländischen Mitbürgerinnen und Mitbürger im Zeichen des »Bündnisses für Toleranz« zu diskriminieren; die Effekte auf die deutschen Staatsbürgerinnen und Staatsbürger im ausgedehnten Lauschangriff, in neuen Formen der Residenzpflicht, der Einschränkungen der Freizügigkeit u.a.m. sind heute schon sichtbar;
- zum zweiten stellt das Gesetzespaket in der Fülle seiner diversen, hier jedoch einheitlich wirkenden Regelungen und den damit begründeten potentiellen Maßnahmen zentrale Grund- und Menschenrechte in einer Weise in Frage, dass von einem gesetzeswillkürlich erzeugten Grundrechtenotstand gesprochen werden muss. Zu diesen in zerzausten und durchlöchernten Grund- und Menschenrechte gehören – die prinzipiell gleichermaßen für Ausländerinnen und Ausländer gelten –: das Grundrecht auf Integrität (Art. 2 GG), hier besonders das vom Bundesverfassungsgericht 1983 daraus hergeleitete Grundrecht auf »informationelle Selbstbestimmung«; das Grundrecht auf Meinungsfreiheit (Art. 5 GG), das Grundrecht auf Integrität der Wohnung (Art. 13 GG), sogar das 1993 überaus begrenzte Grundrecht auf politisches Asylrecht (Art. 16a GG) und nicht zuletzt das Grundrecht auf menschliche Würde, das allen anderen Grundrechten zugrunde liegt. Art. 1 Satz 1 GG: »Die Würde des Menschen ist unantastbar.« Dort, wo Ausländerinnen und Ausländer zu Sicherheitsobjekten werden, wo ihre Person keine Rolle mehr spielt, wird dieses Grundrecht verletzt;

- zum dritten schadet das Gesetzespaket dem Grundgesetz und der durch dasselbe begründeten Bundesrepublik als lebendiger Demokratie. Nicht Schutz und Sicherheit der Demokratie und ihrer Bürger/-innen stehen an erster Stelle, sondern die gesetzlich produzierte Fiktion einer apparativ und auf Kosten der Grund- und Menschenrechte produzierten »perfekten« Antiterrorismus.«

F...I...f...F...e.v.

F...I...f...F...Überall

FlfF-Vorstand

- Prof. Dr. Reinhard Keil-Slawik (Vorsitzender) Paderborn
- Peter Bittner (stellv. Vorsitzender) Berlin
- Dagmar Boedicker München
- Prof. Dr. Leonie Dreschler-Fischer Hamburg
- Eva Hornecker Bremen
- Werner Hülsmann Mörgen-Eppishausen
- Klaus Köhler München
- Prof. Dr. Dietrich Meyer-Ebrecht Aachen
- Michael Müller Schwaigern
- Prof. Dr. Gabriel Schade Leipzig
- Prof. Dr. Britta Schinzel Freiburg i. Br.
- Julia Stoll Darmstadt
- Ralf E. Streibl Bremen
- Prof. Dr. Joseph Weizenbaum Berlin

Beirat

Michael Ahlmann (Bremen); Prof. Dr. Wolfgang Coy (Berlin); Prof. Dr. Wolfgang Däubler (Bremen); Prof. Dr. Christiane Floyd (Hamburg); Prof. Dr. Klaus Fuchs-Kittowski (Berlin); Prof. Dr. Thomas Herrmann (Dortmund); Prof. Dr. Wolfgang Hesse (Marburg); Prof. Dr. Michael Grütz (Konstanz); Ulrich Klotz (Frankfurt); Prof. Dr. Hans-Jörg Kreowski (Bremen); Prof. Dr. Herbert Kubicek (Bremen); Prof. Dr. Hans-Peter Löhr (Berlin); Dipl.-Ing. Werner Mühlmann (Oppurg); Prof. Dr. Frieder Nake (Bremen); Prof. Dr. Rolf Oberliesen (Bremen); Dr. Hermann Rampacher (Bonn); Prof. Dr. Arno Rolf (Hamburg); Prof. Dr. Alexander Roßnagel (Kassel); Prof. Dr. Gerhard Sagerer (Bielefeld); Prof. Dr. Dirk Siefkes (Berlin); Dr. Marie-Theres Tinnefeld (München); Dr. Gerhard Wohland (Wankheim)

Tagung

Überwachung überall? Steht die Privatsphäre vor einer grundsätzlichen Neubewertung?

von Freitag, 26.7. um 15.00 Uhr bis Sonntag, 28.7.02 um 13.00 Uhr in der Akademie für Politische Bildung Tutzing, Buchensee 1, 82323 Tutzing

Veranstalter: Akademie für Politische Bildung Tutzing (<http://www.apb-tutzing.de/>) in Zusammenarbeit mit der Fachhochschule München (<http://www.informatik.fh-muenchen.de>)

Anmeldung bitte direkt bei der Politischen Akademie Tutzing

FIFF-Kommunikation

Regionalgruppe Berlin

Aktionen zum Terrorismusbekämpfungsgesetz

Am 05.12.2001 hielten Wolfgang Kaleck (RAV) und Peter Bittner (FIFF) auf Einladung von attac-Berlin einen zweiteiligen Vortrag zum Thema: Europa rüstet auf nach Innen: Die Wirklichkeit von Sicherheitspaketen und Überwachungstechnologien. Die gut besuchte Veranstaltung fand im Hauptgebäude der TU Berlin statt.

Diese Veranstaltung ist im Kontext der Bürgerrechtsbewegung zu sehen, die sich in Berlin formiert hat, um mit der vereinten Kraft von über 20 Vereinen/Gruppen etwas gegen Schilys Sicherheitspakete zu unternehmen. Es gab diverse Presseerklärungen und sektorale wie umfassende Analysen des Gesetzesmachwerkes. An einigen der kritischen Stellungnahmen war das FIFF beteiligt bzw. hat sie unterstützt. Die Aktivitäten dieses Zusammenschlusses sind unter <http://www.cilip.de/terror/> gut dokumentiert. Man trifft sich auch nach der Verabschiedung des Gesetzes weiter – und zwar jeden ersten Montag im Monat im Haus der Demokratie und Menschenrechte, um sich insbesondere gegenseitig über die Auswirkungen der Gesetzesänderungen zu informieren und aktuelle Entwicklungen im Bereich Bürgerrechte und Innere Sicherheit zu diskutieren.

Wiederaufbau der Bildung in Afghanistan

Vom 10.12. bis 14.12. fand an der TU Berlin (FR 3533) unter der organisatorischen Federführung von Dr. Nazir Peroz (ZIIK, TU Berlin) unter dem Motto »Die Welt wächst zusammen: Gemeinwohl – Gerechtigkeit – Solidarität« eine Kultur- und Dialogwoche mit zahlreichen Vorträgen und einer abschließenden Diskussionsrunde zum Thema »Wiederaufbau der Bildung in Afghanistan« statt. Nähere Informationen zur Veranstaltung findet man unter: <http://bas.cs.tu-berlin.de/Globalisierung.html>. Das FIFF gehörte zu den Unterstützern der Veranstaltung. Einer der Vortragsbeiträge kam von unserem Vorstandsmitglied Joseph Weizenbaum. Er sprach zum Thema: »Moderne Zeit, moderne Technik, moderner Krieg«.

Aus dieser Veranstaltung hat sich eine Arbeitsgruppe Informations- und Kommunikationstechnologie zum Wiederaufbau Afghanistans (AITA) entwickelt, auch hier ist das FIFF beteiligt und unterstützt die Arbeiten. Diese Arbeitsgruppe ist derzeit extrem aktiv!

Wiederbelebung der Regionalgruppentreffen

Sicherlich passiert ob der großen Anzahl von FIFF-Mitgliedern noch sehr viel mehr. Auch bestehen sicher Chancen, sich zu speziellen Themen wie z.B. »(Video-)Überwachung«, »Information Warfare« oder auch »Geistiges Eigentum« intensiver auszutauschen. Wer Lust hat, sich im FIFF-Kreise zu treffen, der möge sich doch bitte bei Peter Bittner (bittner@informatik.hu-berlin.de) melden. Ein erstes Treffen könnte z.B. in der zweiten April-Woche stattfinden.

Überregionale Arbeitskreise des FIFF

AK »RUIN« (Rüstung und Informatik)

Ingo Ruhmann
Rittershausstraße 11
53113 Bonn
ingo.ruhmann@acm.org

AK »Videoüberwachung und Bürgerrechte«

Peter Bittner
Humboldt-Universität
Institut für Informatik
Unter den Linden 6
10099 Berlin
Bittner@informatik.hu-berlin.de

FIFF im Netz

Das ganze FIFF

<http://www.fiff.de>

Mailing-Liste

Beiträge an:
fiff-l@fiff.de
An- und Abbestellungen an:
fiff-l-request@fiff.de

Regionalgruppen

Bremen:
<http://fiff.informatik.uni-bremen.de>
Konstanz:
<http://www.puk.de/fiff-kn>
München:
<http://hyperg.uni-paderborn.de/fiff/regional/muenchen>

Achtung!

Fast alle FIFF Bücher sind stark im Preis reduziert! Einige sind nur noch als Restauflage erhältlich.

Jetzt zugreifen!



Ute Bernhardt, Ingo Ruhmann (Hrsg.): Ein sauberer Tod: Informatik und Krieg.

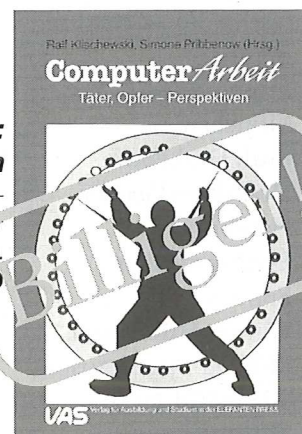
Informations- und Kommunikationstechnik – seit ihren Anfängen politisch geformt • Computer auf dem Schlachtfeld • Dual-Use: zivil geforscht – militärisch genutzt? • »Wehrtechnik und Landesverteidigung« – Zur Forschung in der Bundesrepublik • Weiter so oder umsteuern? • u.v.a.

320 Seiten, Marburg 1991, 5,- EURO

Ralf Klischewski, Simone Pribbenow (Hrsg.): ComputerArbeit. Täter, Opfer – Perspektiven

Das demokratische Potential der Neuen Fabrik • Maschinelle Intelligenz – Industrielle Arbeit • Arbeitnehmer und Betriebsräte zur Informatik im Betrieb.

190 Seiten, Berlin 1989, 1,50 EURO



Ute Bernhardt, Ingo Ruhmann (Hrsg.): Computer, Macht und Gegenwehr – InformatikerInnen für eine andere Informatik

Protected Mode • Computersicherheit: militärisch oder zivil • Computer und Umwelt • Technologiepolitik und Technikfolgenforschung • Partizipative Entwicklung von Systemen •

EU: Grundrechte als Handelshemmnisse? • u.v.a.

216 Seiten, Bonn 1991, 1,50 EURO

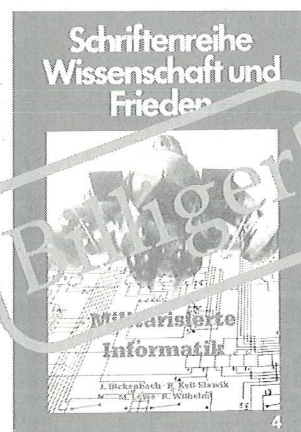


Jutta Schaaf (Hrsg.):

Die Würde des Menschen ist unverNETZbar.

Netznoten Frankfurt • Automatisierung des Zahlungsverkehrs • Rüstungshaushalt und Informationstechnik • Verfassungsverträglichkeit als Kriterium der Technikbewertung • Ethik und Technik • Theorie der Informatik • u.v.a.

300 Seiten, Bonn 1990, 1,50 EURO



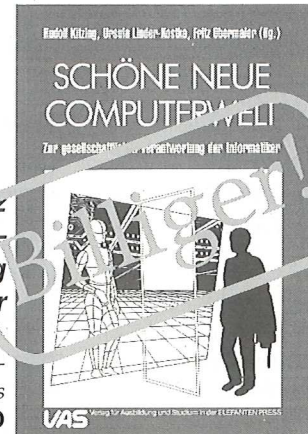
J. Bickenbach et. al. (Hrsg.): Militarisierte Informatik

Erschienen in der Schriftenreihe Wissenschaft und Frieden, Nr. 4, 1985. Dieses Buch war vergriffen, doch sind einige Restexemplare aufgetaucht, die jetzt über das FIFF-Büro zum Preis von 2,- EURO erhältlich sind.

Bibliothek

Rudolf Kitzing, Ursula Linder-Kostka, Fritz Obermaier (Hrsg.): Schöne neue Computerwelt – Zur gesellschaftlichen Verantwortung der Informatiker

Beherrschbarkeit von Systemen, ihre Verletzlichkeit und die Verantwortung von Informatikern · Neue Wege in der Informatik · Psychosoziale Folgen des Computereinsatzes
256 Seiten, Berlin 1988, 1,50 EURO

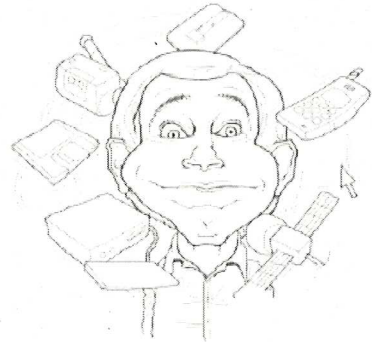


Heiko Dörr (Hrsg.): Herausforderungen an die Informatik? – Science in a Rapidly Changing Environment

Wissenschaft und Ethik · Computergestützte und Elektronische Kriegsführung · Curricula und Forschungs- & Entwicklungs-Ansätze in der Informatik – den Anforderungen des 21. Jahrhunderts gerecht werden · Computertechnologie – ein angemessenes Mittel gegen die Armut der 3. Welt? · (Kredit-)Kartenzahlung im Licht von Daten- und Verbraucherschutz · Vernetzung von Friedensgruppen · Texte in englisch und deutsch
126 Seiten, Bonn 1992, 1,50 EURO

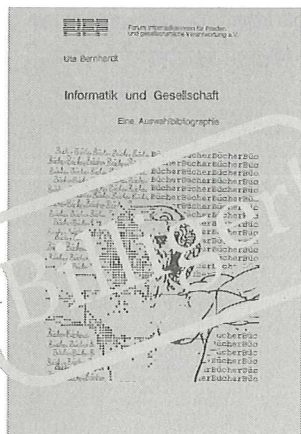
Peter Bittner, Jens Woinowski (Hrsg.): Mensch – Informatisierung – Gesellschaft

Kritische Informatik, Band 1, Beiträge zur 14. Jahrestagung des FfF 1998 in Darmstadt unter dem Motto: „Mensch sein in einer informatisierten Gesellschaft“, 188 Seiten, Münster: Lit-Verlag, 1999, Preis: 39,90 DM



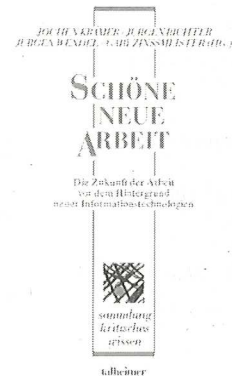
Ute Bernhardt: Informatik und Gesellschaft. Eine Auswahlbibliographie

Ein thematisch gegliederter Einstieg in die Literatur zu Informatik und Gesellschaft
26 Seiten, Bonn 1990, 1,- EURO



Jochen Krämer et. al. (Hrsg.): »Schöne Neue Arbeit«

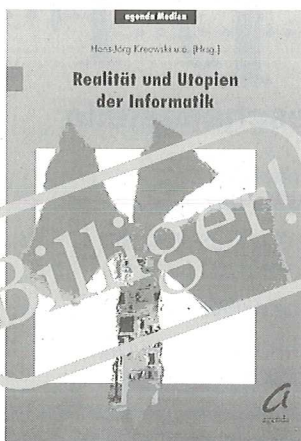
Die Zukunft der Arbeit vor dem Hintergrund neuer Informationstechnologien. Der Tagungsband zur 12. Jahrestagung des FfF in Tübingen 1996
Talheimer, 1997, 44,- DM



Hans-Jörg Kreowski et al.: Realität und Utopien der Informatik

Aus dem Vorwort: »Realität und Utopien der Informatik werden im vorliegenden Sammelband aus unterschiedlichen Sichten dargestellt, um die aktuelle Diskussion im Spannungsverhältnis von Informatik und Gesellschaft zu unterstützen und voranzubringen. Zusammengestellt sind ausgewählte Beiträge der 10. Jahrestagung des »Forums Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung« (FfF), die vom 7. bis 9. Oktober 1994 in Bremen unter dem Motto »1984 plus 10 – Realität und Utopien der Informatik« stattfand.«

Münster: agenda Verlag, 1995, 5,- EURO



Alle Bücher sind erhältlich über: FfF-Geschäftsstelle, Goetheplatz 4, 28203 Bremen

Adressen

Aachen

Prof. Dr. Dietrich Meyer-Ebrecht
Lehrstuhl für Meßtechnik und
Bildverarbeitung
RWTH Aachen
52056 Aachen
Tel.: (0241) 80 78 60
Fax: (0241) 88 88 200
Mail@LfM.RWTH-Aachen.De

Berlin

Peter Bittner
Humboldt-Universität
Institut für Informatik
Unter den Linden 6
10099 Berlin
Bittner@informatik.hu-berlin.de

Irina Piens
Schlesische Str. 29
10997 Berlin
piens@prz.tu-berlin.de

Bonn

Ingo Ruhmann
Rittershausstrasse 11
53113 Bonn
ingo@ruhmann.ki.shuttle.de

Braunschweig

TU Braunschweig
Fachschaft Informatik
ASTA-Fach
Katharinenstraße 1
38106 Braunschweig

Bielefeld

c/o Angewandte Informatik
Technische Fakultät
Universität Bielefeld
Postfach 100 131
33502 Bielefeld
fiff-bi@TechFak.Uni-Bielefeld.DE

Bremen

Prof. Dr. Hans-Jörg Kreowski
Uni Bremen
FB Informatik/Mathematik
Postfach 330 440
28334 Bremen
Tel.: (0421) 218-2956
fiff@informatik.uni-bremen.de

Darmstadt

Julia Stoll
Heinheimer Str. 29-31
64289 Darmstadt
Tel.: (06151) 71 21 81
julias@acm.org

Erlangen/Fürth/Nürnberg

Klaus Thielking-Riechert
Am Dummettsweiher 9
91056 Erlangen
k.thielking@link-n.cl.sub.de

Freiburg

Uwe Jendricke
Bernhardstrasse 1B
79098 Freiburg
Tel. & Fax: 0761/25665
jendricke@telematik.iig.uni-freiburg.de

Frankfurt

Ingo Fischer
Dahlmannstraße 31
60385 Frankfurt am Main

Hamburg

Simone Pribbenow
Hein-Köllisch-Platz 5
20359 Hamburg
Tel.: (040) 54715-366
pribbeno@informatik.uni-hamburg.de

Hannover

Bernhard Pfizner
Rosenbergstraße 14a
30163 Hannover

Heilbronn

Michael Müller
FH Heilbronn, FB
Max-Planck-Straße 39
74081 Heilbronn
Tel.: (07131) 50 43 64
michael.mueller@fh-heilbronn.de

Jena

Prof. Dr. Eberhard Zehendner
Institut für Informatik
Friedrich-Schiller-Universität
07740 Jena
Tel.: (03641) 946385
Fax: (03641) 946372
zehendner@acm.org

Kaiserslautern

Frank Leidermann
Institut für Technol. und Arbeit
Universität Kaiserslautern
Gottlieb-Daimler-Str.
67663 Kaiserslautern
Tel. 0631/205-3742
fleider@sozwi.uni-kl.de

Karlsruhe

Prof. Dr. Thomas Freytag
Weltzienstr. 35
76135 Karlsruhe
Tel.: (0721) 815416 (p)
fiff@thomas-freytag.de

Kiel

Hans-Otto Kühl
Alte Kieler Landstraße 118
24768 Rendsburg
Tel.: (04331) 201-2187

Koblenz

Dr. Michael Möhring
Uni Koblenz-Landau
FB Informatik
Rheinau 3-4
56075 Koblenz
Tel.: (0261) 9119477
Fax: (0261) 37524
moeh@infko.uni-koblenz.de

Köln

Manfred Keul
Landsbergstraße 16
50678 Köln
Tel.: (0221) 317911
100031.12@compuserv.com

Konstanz

Ulrich Moser
Roseneckweg 2
T8244 Gottmadingen
Tel.: (07731) 74261 (p)
+41-79-3112051 (d)
info@fiff-kn.kujm.de
http://fiff-kn.kujm.de/

Lahn-Dill

Fiff-Regionalgruppe Lahn-Dill
c/o Markus Thielmann
Fritz-Philippi-Straße 7
35767 Breitscheid
Tel.: (02777) 1271
mt@donut.de

München

Bernd Rendenbach
Leerbichlallee 19
82031 Grünwald
Tel.: (089) 6410547

Münster

Werner Ahrens
Franz-Dispestr. 36
48231 Warendorf

Oldenburg

Universität Oldenburg
Fachschaft Informatik
Ammerländer Heerstraße
26129 Oldenburg
Fachschaft.Informatik@informatik.uni-oldenburg.de

Paderborn

Harald Selke
Heinz Nixdorf Institut
U-GH Paderborn
Fürstenallee 11
33102 Paderborn
Tel.: (05251) 606518
hase@uni-paderborn.de

Stuttgart

Kurt Jaeger
Schozacher Straße 40
70437 Stuttgart
Tel.: (0711) 8701309
(0711) 90074-23
Fax: (0711) 7289041
pi@lf.net

Tübingen

Jochen Krämer
Sand 13
72076 Tübingen
Tel.: (07071) 29-5957
fiff@informatik.uni-tuebingen.de

Ulm

Universität Ulm
Fachschaft Informatik
Bernhard C. Witt
Oberer Eselsberg
89081 Ulm
wittbe@pcpool1.informatik.uni-ulm.de

F...I...f...F...

Geschäftsstelle

Fiff e.V.
Goetheplatz 4
D-28203 Bremen
Tel.: (0421) 33 65 92 55
Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Mittwochs 13 bis 16 Uhr,
Freitags 10 bis 13 Uhr
Sparda Bank Hannover eG
Kontoverbindung: 927929
BLZ 250 905 00

Was will das FlfF?

Im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FlfF) e.V. haben sich InformatikerInnen zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen ihres Fachgebiets verantwortlich fühlen und entsprechende Arbeit leisten wollen:

- Kritik üben, denn wir haben das Know-how dazu
- uns für eine Abrüstung der Informatik engagieren
- uns am Diskurs über Technik und Wissenschaft beteiligen
- die Öffentlichkeit warnen, wenn wir Entwicklungen in unserem Fachgebiet für schädlich halten
- möglichen Gefahren eigene Vorstellungen entgegensetzen
- die Informations- und Kommunikationstechnik nicht gegen, sondern für den Menschen gestalten
- uns für eine zivile und gerechte Welt einsetzen; eine Welt, in der die Grundrechte aller Menschen gewahrt werden, eine Welt, die menschenwürdig ist
- last not least nicht alles machen, was machbar ist

Geplante

Themen- schwerpunkte

für die FlfF-Kommunikation

2/2002 »Globalisierung«

zuständig: Dagmar Boedicker

3/2002 »Geschlechter- verhältnisse in der Informations- gesellschaft«

zuständig: Britta Schinzel

Die FlfF-Kommunikation bittet um Beiträge!

Die FIFF-Kommunikation lebt von der aktiven Mitarbeit ihrer LeserInnen! Interessante Artikel sowie Fotos und Zeichnungen zur Illustration (mit Quellengaben) sind immer herzlich willkommen. Die Bearbeitung wird erleichtert, wenn Beiträge elektronisch und zusätzlich auf Papier der Redaktion zugehen. Die Redaktion behält sich Kürzungen und Titelländerungen vor.

Impressum

Die FlfF-Kommunikation ist das Mitteilungsblatt des »Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.« (FlfF). Die Beiträge sollen die Diskussion unter Fachleuten

anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder. Nachdruck genehmigung wird nach Rücksprache mit der Redaktion in der Regel gerne erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Heftpreis: 5 EUR. Der Bezugspreis für die FlfF-Kommunikation ist für FlfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FlfF-Kommunikation für 20 EUR/Jahr (inkl. Versand) abonnieren.

Erscheinungsweise: einmal vierteljährlich

Erscheinungsort: Bremen

Auflage: 2000

Herausgeber: Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FlfF)

Verlagsadresse: FlfF-Geschäftsstelle, Goetheplatz 4, D-28203 Bremen, Tel. (0421) 33 65 92 55

ISSN: 0938-3476

Druck: Meiners Druck Bremen

Layout: Markus Hoff-Holtmanns

Titelbild: Getarnte Videokameras in Finnland, fotografiert von Julia Stoll, siehe Seite 2

Redaktionsadresse: FlfF-Kommunikation, Goetheplatz 4, D-28203 Bremen, Tel. (0421) 33 65 92 55, Fax (0421) 33 65 92 56
E-Mail: redaktion@fiff.de

FlfF-Überall: In dieser Rubrik der FlfF-Kommunikation ist jederzeit Platz für Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an: hubert@mtsf.de

Lesen, Schluß-PFIF: Beiträge für diese Rubriken bitte per Post an Claus Stark (Heilbronn) oder per E-Mail an: stark@secorvo.de

Redaktionsschluß für die Ausgabe 2/2002: 15. 04. 2002

Redaktions-Team

FlfF-Kommunikation 1/2002:

Peter Bittner, Hardy Frehe, Markus Hoff-Holtmanns (verantwortlich), Julia Stoll & Jens Woinowski

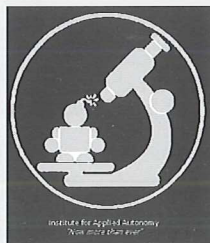
Hinweis: Postvertriebsstücke wie die FlfF-Kommunikation werden von der Post auch auf Antrag nicht nachgesandt; daher bitten wir alle Mitglieder und Abonnenten, dem FlfF-Büro jede **Adreßänderung** rechtzeitig bekanntzugeben!

Schluß-P E...I...f...F...

iSEE

New York für Heimlichtuer

Die Zahl der Überwachungskameras in New York wird auf rund 2400 geschätzt. Wer trotzdem ungesehen von A nach B will, kann sich auf einen Straßenkarten-Service der ganz besonderen Art verlassen.



iSee-Symbol: Mensch auf dem Mikroskopierteiler

Man darf nicht lauffaul sein, wenn man etwas zu verheimlichen hat. Fast zweieinhalbtausend Kameras beobachten das New Yorker Straßenleben, schwenken über Plätzen, starren in Einfahrten, innen, außen, überall. Gerade nach der WTC-Katastrophe geben diese Kameras vielen Menschen ein Gefühl der Sicherheit; es gibt gar den Ruf nach noch mehr Überwachung im Alltag.

Und es gibt Menschen und Interessengruppen, denen vor all dem graut. Für die sich die Wertmaßstäbe auch nach dem 11. September nicht grundlegend geändert haben: Sie opponieren weiter mit viel Phantasie gegen das, was sie als zunehmenden Eingriff in ihre Privatsphäre empfinden.

So ist das, was die Bewegten des »Institutes für angewandte Autonomie« zu verbergen haben, in aller erster Linie einmal »nur« die eigene Person. Und die mag sich wünschen, von Punkt A zu Punkt B zu gelangen, ohne dass sie von irgendeinem »Voyeur« beobachtet wird: Denn genau das ist einer der Vorwürfe. Immer mehr Bilder würden an TV-Stationen verkauft, wenn Schlimmes oder Peinliches passiere; immer häufiger würden Sicherheitsleute dabei ertappt, wie sie mit Beobachtungskameras auf Brüste und Hinterteile von Passantinnen zoomten.



Leichter Umweg inklusive: Wer nicht beobachtet werden will, braucht Zeit und gutes Schuhwerk

Wer so etwas nicht will, der ist bei »iSee« richtig.

Die Website ist ein Stadtplanservice der ganz besonderen Art. Man gibt seinen Ausgangspunkt ein, den Zielpunkt und - schwupp: Die Datenbank empfiehlt einen Weg mit der niedrigstmöglichen Kameradichte.

Kann das ernst gemeint sein? Die Meinungen gehen auseinander.

Immerhin aber gelingt es iSee und dem »Institut for Applied Autonomy«, das Thema des Schutzes vor der wachsenden Zudringlichkeit von Überwachungstechnik im privaten und öffentlichen Raum wieder in die Medien zu bringen. Vor Monaten versuchten sich die »Surveillance Camera Players« in einem ähnlich humorvollen Ansatz politischen Protestes.

Und hatten die Sympathien auf ihrer Seite - was im Falle von iSee längst noch nicht geklärt ist: Der Service ist erst seit wenigen Wochen online, doch schon mehrten sich die Stimmen, die darauf verweisen, dass dies doch ein toller Dienst für Kriminelle und Terroristen sei.

Doch Sicherheitsexperten glauben nicht, dass iSee von sonderlichem Nutzen für solche Zielgruppen sei. Sie vermuten die Zielgruppe, die sich direkt von iSee angesprochen fühlen könnte, ganz woanders: Ehemänner, auf dem Weg von A nach C.