

Kapitel 1 – Ein verbreitetes, aber diffuses Unbehagen

»Ich habe nichts zu verbergen!« Als in den 1990er-Jahren in immer mehr Geschäften und auf immer mehr öffentlichen Plätzen Videokameras installiert wurden, war dieser Satz oft zu hören. Repräsentative Meinungsumfragen in Deutschland ermittelten eine Zustimmung von 90 Prozent und mehr für die Videoüberwachung im öffentlichen Raum.¹ Warum auch sollte sich jemand daran stören, der sich nichts zuschulden kommen lässt? Nur eine Minderheit wandte ein, die Videoüberwachung sei nicht verhältnismäßig, weil sie auch ganz unschuldige Bürger in den Blick nähme. Außerdem erzeuge sie einen Konformitätsdruck: Wer weiß, dass er beobachtet wird, verhält sich möglicherweise so, dass er erst gar nicht die Aufmerksamkeit der Wachleute erregt. Ja, die Videoüberwachung sei ein weiterer Schritt in Richtung einer Überwachungsgesellschaft. Diese klassischen Argumente des Datenschutzes stießen kaum auf Interesse oder gar Zustimmung.

Mittlerweile ist Videoüberwachung in Deutschland alltäglich. Aber die breite Öffentlichkeit ist deutlich misstrauischer geworden. Das Vorhaben der Regierung, alle Telefon- und Internetverbindungen für ein halbes Jahr zu speichern und bei Bedarf den Sicherheitsbehörden zur Verfügung zu stellen – die sogenannte »Vorratsdatenspeicherung« – führte zu der größten Sammelklage in der Geschichte der Bundesrepublik. Im März 2010 urteilte das Verfassungsgericht, die Speicherung sei mit dem Fernmeldegeheimnis zwar »nicht schlechthin unvereinbar«, aber in der geplanten Form verfassungswidrig. Es sei nicht klar genug geregelt, wer und in welchen Fällen auf die Daten zugreifen kann. Nun wird die Sammlung der Verbindungsdaten in anderer, abgespeckter Form kommen.

Sind wir auf dem Weg in eine Überwachungsgesellschaft? Sowohl die deutsche Regierung als auch die Europäische Union investieren gegenwärtig

1) Jan Wehrheim (2000): CCTV – ein fast ignoriertes Überwachungsdrama breitet sich aus, In: Forum Wissenschaft, Nr. 2 34 – 40, hier Seite 37. Im Netz zu finden unter www.safer-city.de/2000/cctv.html.

viel Geld in die Entwicklung neuer Überwachungstechnik. Im Herbst 2009 wurde publik, dass im Rahmen des EU-Sicherheitsforschungsprogramms Überwachungsanlagen entwickelt werden, die alle verfügbaren Informationen über ein städtisches Gebiet sammeln und auswerten, darunter Daten der Verkehrsüberwachung, des öffentlichen Nahverkehrs, aus dem Internet und der Videokameras. Mit dieser Technik namens Indect sollen Sicherheitsbehörden Anschläge verhindern. Um Kriminalität und Terrorismus zu bekämpfen, erhalten Polizei und Nachrichtendienste immer weiter gehende Befugnisse. Aber Überwachung ist kein Staatsmonopol: Beinahe wöchentlich wird ein neuer Fall bekannt, bei dem personenbezogene Daten weitergegeben, gestohlen oder verkauft, immer aber ohne das Wissen und gegen den Willen der Betroffenen genutzt werden. Unternehmer verlangen beim Vorstellungsgespräch Blutproben. Krankenkassen verkaufen die Daten ihrer Kunden.

Das ist der politische Hintergrund, vor dem über »Sicherheit«, »Überwachung« und »Datenschutz« debattiert wird. Die Parteien betonen allesamt, wie sehr ihnen der Schutz der Privatsphäre der Bürger am Herzen liegt, während gleichzeitig technisch-organisatorische Infrastrukturen geschaffen werden, die eine umfassende Überwachung aller Lebensbereiche in den Bereich des Möglichen rücken. Zwischen Versprechungen auf »Sicherheit« und auf »Privatheit« hin- und her gerissen, mutet das Verhalten der Volksvertreter geradezu schizophran an. So fördert das Bundesforschungsministerium unter der Christdemokratin Annette Schavan die Entwicklung von »Terahertz-Scannern«. Diese Geräte schicken Strahlung mit extrem kurzer Wellenlänge aus, mit der Personen und Gegenstände sozusagen abgetastet und nichtmetallische Gegenstände entdeckt werden, etwa Keramikkesser, die von den herkömmlichen Metalldetektoren nicht erkannt werden. Die Scanner, unter anderem gedacht für den Einsatz an Flughäfen, erzeugen dazu ein Bild des nackten Körpers. Als die Presse im Winter 2008 diese Anlagen deshalb »Nackt-Scanner« taufte und ihren Lesern in Aussicht stellte, bald würde das Sicherheitspersonal ihnen schamlos unter die Kleidung schauen, beeilte sich der damalige Innenminister Wolfgang Schäuble – immerhin ein Partei- und Kabinettskollege von Annette Schavan – auf einer Pressekonferenz zu versichern, ein solcher »Unfug« sei mit ihm nicht zu machen: »Ich will nicht, dass die Bundespolizei in das Licht kommt, sie seien heimliche Spanner.«

Zu einer ähnlich grotesken Situation kam es, als die FDP ein Jahr später von der Oppositions- zur Regierungspartei wurde. Zu den vielen Beschwerdeführern gegen die Vorratsdatenspeicherung hatte nämlich auch Sabine Leutheusser-Schnarrenberger gehört – nur war sie damals noch nicht Bundesjustizministerin. Im Winter 2009 war sie es und kündigte an, sie werde zur Verhandlung vor dem Bundesverfassungsgericht erscheinen. »Ich werde mich

nicht zur Sache einlassen, will aber mit meiner Anwesenheit deutlich machen, dass ich zu meiner Rechtsposition stehe, und die Bedeutung unterstreichen, die ich diesem Thema beimesse.«

In der bundesdeutschen Geschichte war es immer eine Minderheit, die sich von der Überwachung durch Staat und Polizei bedroht sah oder wenigstens gestört fühlte. Das verbreitete Desinteresse hatte auch damit zu tun, dass sich die Eingriffe in Bürgerrechte und die Überwachungsmaßnahmen immer gegen andere zu richten schienen: gegen die Kriminellen, die Terroristen oder die Russen-Mafia. Haben wir wirklich nichts zu verbergen? Überwachung rückt immer näher an die Bevölkerung heran, sie wird flächendeckend: Ein Gerät, das die Durchsuchten nackt bis auf die Haut darstellt. Eine Software, die buchstäblich alle Information auswertet, um »verdächtiges Verhalten« zu erkennen. Die Dokumentation jedes Telefonats und jeder E-Mail der ganzen Bevölkerung. Kein Wunder, dass es immer mehr Menschen schwerfällt zu glauben, das alles habe nichts mit ihnen zu tun.

Der Datenschatten – unentrinnbar und mehrdeutig

Überwachung ist nichts Neues. Feudalherren trieben von den Bauern den Zehnten ein und achteten scharf darauf, dass sie nicht zu wenig bekamen. In Schulen und Universitäten wird regelmäßig überprüft, ob die Schüler und Studierenden ihren Lernstoff intus haben. In Dörfern sorgt der Klatsch über die Nachbarn für eine lückenlose Überwachung, die das Bundeskriminalamt neidisch machen muss. Politische Polizei und Nachrichtendienste verfolgen Terroristen und solche, die es einmal werden könnten.

Es ließen sich leicht weitere Beispiele finden, für die der Begriff »Überwachung« auf die eine oder andere Art zutrifft. Wo Menschen Beziehungen mit anderen Menschen eingehen, wo sie Macht über andere erlangen, wird beobachtet, überprüft, kontrolliert, kurz: überwacht. Der Begriff überschneidet sich mit dem der »sozialen Kontrolle« und ist wie sie allgegenwärtig. Im Alltagsgebrauch meint das Wort eigentlich nur eine besonders starke, tiefgreifende Kontrolle, der auch nicht entgeht, was der Kontrollierte lieber verbergen würde. Deshalb ist jede Gesellschaft eine »Überwachungsgesellschaft«. In dem modischen, etwas unglücklichen Begriff drückt sich allerdings eine wirkliche historische Entwicklung aus. Die »Informatisierung« führt dazu, dass immer mehr Wissen in Form von Daten vorhanden ist. Überwachung ist nichts historisch Neues. Die technischen Möglichkeiten zu überwachen wachsen aber in einem ungeahnten Ausmaß.

Daten zirkulieren. Aus ihrem Entstehungskontext herausgenommen, werden sie problematisch: Was wir unserem Arzt erzählen, muss unser Chef

oder unser Ehemann nicht wissen; was wir der Freundin verraten, geht die Polizei nichts an. Aber der Datenschatten ist, einmal vorhanden, im Prinzip für alle verfügbar. Zwischen ihm und den zahlreichen Interessenten stehen oft nur rechtliche Regelungen (die nicht durchgesetzt werden) und technische Maßnahmen (die zu umgehen nur eine Frage des Aufwands ist). Die Auswertung des Datenschattens kann zunehmend automatisiert, von Maschinen durchgeführt werden. Dadurch wird Überwachung einfacher – und auch immer billiger. Der Datenschatten senkt in vielen Fällen die »Kontrollkosten« – der Aufwand, der nötig ist, um festzustellen, ob eine Erwartung erfüllt wurde oder nicht.

Schon heute hinterlassen wir überall digitale Datenspuren. Noch beim Spaziergang im Wald sendet unser Mobiltelefon ein Signal an den nächsten Funkmast und verrät so seinen ungefähren Aufenthaltsort. Ob beim Einkauf übers Internet oder in einem Geschäft, wenn wir mit Kreditkarte bezahlen, jede SMS und jedes Telefonat erzeugen Daten, deren Verwendung wir nicht unmittelbar kontrollieren können. Unsere digitalen Spuren folgen uns wie ein Schatten. In der Form von Daten können sie mit geringen Kosten zusammengeführt werden, während die Überwacher von einst sich noch die Mühe machen mussten, schriftliche Aufzeichnungen zusammenzutragen und hinter uns her zu schleichen. Aus dem Datenschatten können Bewegungs- und Persönlichkeitsprofile abgeleitet werden. Wie bei einer digitalen Photographie kann der Ausschnitt, der betrachtet werden soll, beliebig vergrößert werden. Dann lässt sich beispielsweise nachvollziehen, welchen kurzen Videofilm wir uns bei *Youtube* zwischen 13.40 und 13.43 Uhr auf dem heimischen Rechner angesehen haben und welche Bücher wir uns danach in der städtischen Leihbücherei ausgeliehen haben, obwohl wir doch eigentlich krankgeschrieben waren. Unser persönlicher Lebensvollzug hinterlässt ein digitales Abbild, das auch nachträglich überprüft, analysiert und bewertet werden kann.

Immer größere Lebensbereiche werden von elektronischen Medien durchdrungen. Durch Satellitenortung, die Etikettierung mit Funketiketten (RFID) und die Vernetzung von Datenbanken entsteht eine Informationsinfrastruktur neuen Typs. Immer mehr Gegenstände des täglichen Gebrauchs, von der Kaffeemaschine bis zum Kraftfahrzeug, enthalten Mikroprozessoren und tauschen mit ihrer Umgebung Daten aus. »Wenn allgegenwärtige Datenverarbeitung funktioniert, wie sie soll, funktioniert sie immer auch als Überwachungstechnologie«, schreibt der Datenschutzexperte Alexander Roßnagel treffend über das *Ubiquitous Computing*.² Noch größere

2) Alexander Roßnagel (2007): Datenschutz in einem informatisierten Alltag. Gutachten im Auftrag der Friedrich-Ebert-Stiftung, Berlin, Seite 102.

Auswirkungen als die allgegenwärtige Datenverarbeitung von Gebrauchsgegenständen wird haben, dass die »Informationsinfrastruktur« langsam, aber unaufhörlich Daten über Verkehr, Energieversorgung und bald auch über Arbeit, Gesundheit und Bildung integrieren wird.

Den Datenschatten werden wir nicht los. Aber wie der Schatten, den unser Körper wirft, nur unsere Umrisse verrät, liefern auch die Daten nur einen Umriss, einen Hinweis. Wie die Farben im Schatten verlorengehen, ist der Datenschatten ein Abbild, das viele sinnliche Qualitäten nicht mehr enthält. Diese beiden Eigenschaften sind für die folgende Analyse entscheidend: Der Datenschatten ist sowohl unentrinnbar als auch mehrdeutig. Dafür bleibt er, anders als der Schatten des Lichts, auch erhalten, wenn wir schon woanders sind.

Über dieses Buch

Wie beeinflusst der Datenschatten die sozialen Beziehungen? Wie verändert er die Kräfte- und Machtverhältnisse zwischen Staat und Bürger, Polizei und Bevölkerung, im Büro und der Fabrik? Um diese Fragen zu beantworten, beschreibe ich zunächst seine historische Entstehung (Kapitel 2). Der Datenschatten ist das Ergebnis der ziel- und zweckgerichteten Datenerzeugung von Unternehmen und staatlichen Verwaltungen. Ihr Ziel war und ist, »Kontrollkosten« zu senken – was aber durchaus nicht immer und schon gar nicht dauerhaft gelingt. Besonders deutlich wird das bei der Überwachung der Arbeit (Kapitel 3). Um den Produktionsprozess zu kontrollieren, wird das subjektive Arbeits-Wissen der Beschäftigten in allgemein zugängliche Informationen verwandelt. Die Grenzen dieser Strategie finden sich auf der Ebene der »Organisationssteuerung« wieder, bei der Kennzahlen eine besondere Rolle spielen (Kapitel 4). Ob in staatlichen Behörde oder transnationalen Unternehmen, sie sind Teil einer »informatrischen Strategie«, um das Verhalten der Beschäftigten zu lenken. Dann beschreibe ich die Umrisse eines (Sozial-)Staats, der seine verstreuten Wissensbestände vernetzt und zur Kontrolle der Bevölkerung einsetzt (Kapitel 5) – keineswegs nur Zukunftsmusik. Im Gesundheitswesen dient der Datenschatten sowohl der Kostensenkung als auch der Gestaltung als Markt (Kapitel 6). Für die Sicherheitsbehörden dagegen ist die Auswertung des Datenschattens nur die jüngste Etappe in der Auseinandersetzung zwischen Gesetzeshütern und -brechern. (Kapitel 7). High-tech-Überwachung löst aber nicht das alte Problem der Polizei, dass technische Kontrolle entweder durch organisatorische Regeln ergänzt oder aber heimlich vorgenommen werden muss. Ähnliches findet in Familien und Liebesbeziehungen statt, wo Überwacher ihre eigene Unsicherheit bearbeiten

wollen und sich stattdessen in einem Kreislauf aus »Kontrolle – Unsicherheit – mehr Kontrolle« wiederfinden (Kapitel 8). Die kommerzielle Nutzung des Datenschattens, vor allem für Werbezwecke, beruht wiederum vor allem auf Heimlichkeit (Kapitel 9). Am Schluss steht die Frage, welche Kräfte einer Überwachungsgesellschaft entgegenstehen (Kapitel 10). Im Anschluss an fast alle Kapitel kommen in Interviews Menschen zu Wort, die auf die eine oder andere Art mit dem Datenschatten zu tun haben: als Überwacher, Überwachte oder als Wissenschaftler.

Dieses Buch ist eine journalistische, keine wissenschaftliche Arbeit. Ich habe mich freizügig bei den vorhandenen Theorien über Informatisierung, Technikentwicklung und soziale Kontrolle bedient und mir dabei auch die Freiheit herausgenommen, den ein oder anderen Gedanken aus seinem ursprünglichen Zusammenhang zu nehmen. Es geht um die gesellschaftlichen und psychologischen Ursachen und Wirkungen von Überwachung und Überwachungstechnik.

Videokameras überwachen nicht ...

Immer wieder wird dabei die Frage auftauchen, ob Technik, besonders Informationstechnik, zu einer neuen Qualität der Überwachung führt.³ Vieles an dem Unbehagen gegen die Videoüberwachung, wie es in Deutschland in den 90er-Jahren zu finden war, war diffus. Es speiste sich nicht zuletzt aus dem Widerwillen dagegen, dass nun statt eines Polizisten aus Fleisch und Blut ein technischer Apparat die Überwachung übernehmen sollte. Aber sowohl die Befürworter als auch die Gegner überschätzten die Wirksamkeit der Kameras gewaltig. Zwar zeichnen sie zuverlässig auf, was vor die Kameralinse kommt, das Verhalten der Überwachten steuern sie aber nur unter bestimmten Umständen und vorübergehend.⁴ Nach einer Untersuchung der *Metropolitan Police* kam im Jahr 2008 auf tausend Kameras nur eine, die überhaupt eine Rolle in einer polizeilichen Ermittlung spielte. Anders gesagt: Mit 99,9 Prozent der Videoüberwachungsanlagen konnte die Polizei in diesem Zeitraum nichts anfangen.

-
- 3) Überwachung bezieht sich im Folgenden ausschließlich auf die Beobachtung von Menschen durch andere Menschen. Die Überwachung von technischen und natürlichen Prozessen (im Sinne des *monitoring*) wird nur betrachtet, wenn die daraus entstehenden Informationen sich auf einzelne Personen oder Gruppen beziehen lassen. Der Ausdruck Technik wiederum wird im Sinne von »Maschinenteknik«, nicht wie in »Verfahrens-« oder »Verhaltenstechnik« verstanden.
 - 4) Vergleiche etwa David Skinns (1999): *Crime reduction, diffusion and displacement. Evaluating the effectiveness of CCTV*, In: Clive Norris / Jade Moran / Gary Armstrong (Hg.): *Surveillance, Closed Circuit Television and Social Control*, Aldershot, Ashgate, 175 – 189.

Technik liefert das Symbol für die Angst vor einem »Überwachungsstaat«. Schon die Bewegung gegen die Volkszählung speiste sich nicht nur aus einem grundsätzlichen Misstrauen gegen die staatlichen Behörden, sondern auch aus der Angst vor einem in jeder Hinsicht unmenschlichen »Computerstaat«. Der Gesetzesentwurf zur Reform des Bundeskriminalamts aus dem Jahr 2008 sah insgesamt 23 neue Eingriffsbefugnisse für die Polizei vor. Keine sorgte für nur annähernd so viel Empörung wie die sogenannte »Online-Durchsuchung« – der heimliche Zugriff der Polizei auf die Computer von Verdächtigen –, eine Maßnahme, deren Bedeutung völlig überschätzt wird.

Um die Gefahren der Überwachung wirklich verstehen und einordnen zu können, genügt es aber nicht, neue technische Möglichkeiten zu kennen. Eingesetzt werden diese schließlich von Individuen und Organisationen, die nicht einfach machen können, was sie wollen, sondern auf Widerstände verschiedener Art treffen. Letztlich ist der Slogan der US-amerikanischen Schusswaffen-Lobby auch in diesem Zusammenhang unbequem, aber eben nicht falsch: *Guns don't kill people – people kill people*. Entsprechend gilt: Nicht Computer überwachen Menschen, sondern Menschen überwachen Menschen. Ob Überwachung wirkt und wozu sie führt, lässt sich nur aus dem gesellschaftlichen Zusammenhang erklären, in dem sie zum Einsatz kommt. Dazu will dieses Buch Anregungen geben.