

Ein Bericht zur Überwachungsgesellschaft

Für den Datenschutzbeauftragten

Vom Surveillance Studies Network

Zusammenfassung

September 2006

Herausgeber:

Kirstie Ball und David Murakami Wood

mit Beiträgen von:

Louise Amoore
Kirstie Ball
Steve Graham
Nicola Green
David Lyon
David Murakami Wood
Clive Norris
Jason Pridmore
Charles Raab
Ann Rudinow Saetnan

Einführung

Im Juni 2006 beauftragte der britische Datenschutzbeauftragte das Surveillance Studies Network mit der Erstellung eines Berichts zur Überwachungsgesellschaft. Bei diesem

Dokument handelt es sich um eine Zusammenfassung dieses Berichts, deren drei Kapitel sich auf die wichtigsten Berichtsergebnisse beziehen. Kapitel 1 setzt die Parameter einer Überwachungsgesellschaft fest: Definitionen, Probleme und Konsequenzen. Kapitel 2 zeigt auf, wie eine Überwachungsgesellschaft funktioniert, und Kapitel 3 untersucht einige aufsichtsrechtliche Herausforderungen, die von einer Überwachungsgesellschaft gestellt werden.

1. Die Überwachungsgesellschaft: Zusammenfassung, Vorgeschichte, Definitionen

Es ist unsinnig, von der Überwachungsgesellschaft im Futur zu sprechen, denn wir leben bereits mittendrin. In allen wohlhabenderen Länder dieser Erde gehört Überwachung zum Alltag – und zwar nicht nur von Sonnenauf- bis Sonnenuntergang, sondern rund um die Uhr. Und dabei geht es nicht nur um die Videoüberwachung (CCTV), die unser Gesicht mehrere hundert Mal pro Tag aufzeichnet, oder die Kassiererin im Supermarkt, die nach unserer Kundenkarte fragt. Diese Systeme stellen eine grundsätzliche, komplexe Infrastruktur dar, in der die Erfassung und Verarbeitung von Personendaten als moderne Lebensnotwendigkeit vorausgesetzt wird.

Gegenseitige Fürsorge, Anstand und Sitte oder geheime Informationssuche – es hat schon immer die verschiedensten Arten der Überwachung gegeben. Seit ca. 400 Jahren aber stehen der organisatorischen Praxis auch „rationale“ Überwachungsmethoden zur Verfügung, mit denen wir uns schrittweise von den formlosen Sozialstrukturen und -kontrollen entfernt haben, die damals den Alltag und die Verwaltung bestimmten. Das traditionelle Sozialgefüge des Menschen war nicht mehr relevant, da familiäre Beziehungen und die individuelle Identität einer Person dem problemlosen Betrieb dieser neuen Organisationen („Bürokratien“ genannt) nur im Weg waren. Doch es gab auch Vorteile: Auf diese Weise konnten Bürger und schließlich auch Arbeiter ihre Rechte durchsetzen. Schließlich schützte sie nun nicht länger nur das Gesetz, sondern auch akkurate Aufzeichnungen. Unpersönliche und regelbasierte Praktiken vermehrten die Überwachung. Die neuen Informationstechnologien der Nachkriegszeit revolutionierten die bürokratische Verwaltung und verbesserten Bearbeitungsgeschwindigkeit, Kontrolle und Koordination. Diese Entwicklung sowie immer bessere Möglichkeiten der Identifikation und Bewegungskontrolle, wie sie für militärische und polizeiliche Zwecke entwickelt wurden, sind der Hauptbestandteil dieses Berichts. Die Überwachung wächst im Einklang mit dem modernen Zeitalter.

Und was ist so falsch an einer Überwachungsgesellschaft?

Wenn wir die Überwachungsgesellschaft als Produkt der Moderne erkennen, lassen sich gleich zwei Fallen vermeiden: Erstens gehört Überwachung nicht zu den üblen Machenschaften fragwürdiger Bösewichter und zweitens erwächst Überwachung nicht ausschließlich aus neu erfundenen Technologien (ganz Paranoide glauben natürlich, dass diese beiden Gedankengänge zusammengehören). Trotzdem: Auch wenn man die Überwachung ins rechte Licht rückt, bedeutet das noch lange nicht, dass am Ende alles gut wird. Wir müssen die Kernfragen der Überwachung auch weiterhin sorgfältig identifizieren und im Auge behalten.

Überwachung ist ein zweischneidiges Schwert – wir dürfen ihre Vorteile nicht außer Acht lassen. Doch groß angelegte Systeme bergen Risiken und Gefahren in sich, und Macht korrumpiert – oder verzerrt zumindest die Ansichten der Mächtigen. Groß angelegte Technologie-Infrastrukturen neigen auch zu großen Problemen. Ein versehentlicher oder falscher Tastendruck kann leicht Chaos verbreiten. Denken wir doch nur an das Online-Verhalten von 20 Millionen ganz normalen Bürgern, das AOL im August 2006 zu

„Forschungszwecken“ freigab. Obwohl angeblich von allen Identifikationsmerkmalen befreit, konnten die Suchanfragen in Sekundenschnelle mit Namen in Verbindung gebracht werden.¹

Ebenso wichtig sind Korruption und verzerrte Machtansprüche. Auch hier muss man nicht auf einen boshafte Tyrannen zurückgreifen, der sich der Datenbanken mit Sozialhilfeangaben oder medizinischen Daten bemächtigt. Machtmissbrauch gibt es auch bei Politikern, die sich auf das sogenannte öffentliche Wohl (wie z.B. den Sieg über einen Kriegsgegner) berufen, um un- oder gar außergewöhnliche Taktiken durchzusetzen. Im Zweiten Weltkrieg wurden japanischstämmige Amerikaner in den USA über den – normalerweise illegalen – Einsatz von Volkszählungsdaten ermittelt und inhaftiert. In jüngster Vergangenheit wurden viele muslimische Amerikaner unter Zuhilfenahme von Flugverbotslisten als reiseuntauglich eingestuft oder anderweitig in Rassenprofile aufgenommen – Praktiken, die in einem anderen Zusammenhang eindeutig als unfair eingestuft worden wären.²

In einer globalisierten Hightech-Welt gibt es ausreichend Beispiele für die unbeabsichtigten Konsequenzen gut gemeinter Maßnahmen und Richtlinien. So hieß es z.B., Konzerne könnten nur wettbewerbsfähig bleiben, wenn sie „ihre Kunden gut kennen“, ihre Werbung entsprechend ausrichten und sogar ihre Fabriken und Geschäfte an den entsprechenden Orten ansiedeln. Den Geschäftsführer eines Ladens, der nur die kreditwürdigsten Kunden anziehen möchte und daher Kreditprüfungen über Experian vornimmt, hält ja auch niemand für unaufrichtig. Im Streben nach höheren Gewinnen ist das einfach sinnvoll. Ergebnis – und damit unbeabsichtigte Konsequenz – dieser Datenerfassung zur Schaffung eines profitablen Kundenstamms ist jedoch, dass bestimmte Gesellschaftsgruppen aufgrund ihrer Zahlungsfähigkeit eine Sonderbehandlung erfahren und andere links liegen gelassen werden.³

Besonders schwer wiegt die Tatsache, dass all diese Überwachungsverfahren und -methoden eine Welt schaffen, in der uns niemand mehr vertraut. Überwachung fördert Misstrauen.⁴ Arbeitgeber installieren Tastenanschlagsanzeiger in Firmencomputern oder Routenkontrollgeräte in Dienstfahrzeugen und geben damit unumwunden zu, dass sie ihren Mitarbeitern nicht trauen. Der Sozialbeamte, der auf Sozialhilfebetrug untersucht oder nach Hinweisen für einen „Ehemann im Hause“ forscht, gibt damit zu, dass er seinen Empfängern nicht traut. Und auch Eltern, die die Aktivitäten ihrer Teenager per Webcam oder GPS-System verfolgen, erklären damit offen, dass sie ihnen nicht trauen. Man mag einwenden, dass es sich doch um reine Vorsichtsmaßnahmen handelt. Aber wie weit darf dieses Verhalten gehen? Unsere gesellschaftlichen Beziehungen basieren auf Vertrauen und wenn wir dieses Fundament untergraben, kommt das einem langsamen gesellschaftlichen Selbstmord gleich.

Überwachung – eine Definition

Wie entsteht eine Überwachungsgesellschaft

Unter einer Überwachungsgesellschaft versteht man eine Gesellschaft, die unter Zuhilfenahme überwachender Techniken organisiert und strukturiert ist. Überwachung bezieht sich hier auf den Zugriff auf Bewegungs- und Handlungsdaten, die im Auftrag der strukturgebenden Organisationen und Regierungen von technischen Hilfsmitteln aufgezeichnet werden. Diese Daten werden anschließend sortiert, gesichtet und kategorisiert sowie als Grundlage für Entscheidungen herangezogen, die Einfluss auf unser Leben haben. Derartige Entscheidungen beziehen sich auf unser Recht auf bzw. Zugang zu Sozialleistungen, Arbeit, Waren und Dienstleistungen sowie Strafrechtspflege, Gesundheit

¹ Siehe: Barbaro, A. und Zeller, T. „A face is exposed for AOL searcher no. 4417749“, *New York Times*, 9. August 2006. <http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482/>

² Siehe: Amnesty International USA (2004) *Threat and Humiliation: Racial Profiling, Domestic Security and Human Rights in the USA*, New York: Amnesty International USA, http://www.amnestyusa.org/racial_profiling/report/rp_report.pdf

³ Lacey, S. (2005) *The Glass Consumer*, Bristol UK: Policy Press; Danna, A. und Gandy, O. (2002) „All that glitters is not gold: Digging beneath the surface of data-mining“ *Journal of Business Ethics*, 40: 373-386; Lyon, D. (Hg.) (2003) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London und New York: Routledge.

⁴ Dies wird diskutiert in: Lyon, D. (2003) *Surveillance after September 11*, Cambridge UK: Polity Press, 45-48, 142ff.

und Wohlfahrt und unsere Bewegungsfreiheit im öffentlichen und privaten Raum. Dieser Überwachung begegnen wir täglich:

- Videokameras überwachen uns überall – in Gebäuden, Einkaufszonen, Straßen und Wohngebieten. Automatische Systeme können längst Kfz-Kennzeichen (und in zunehmendem Maße auch Gesichter) erkennen.
- Elektronische Fußfesseln stellen sicher, dass sich auf Bewährung Verurteilte nicht über ihre Freigangsbedingungen hinwegsetzen und von festgenommenen Personen werden – unabhängig von der Schuldfrage – DNA-Abstriche entnommen und gespeichert. „Kriminelle Tendenzen“ werden bei immer jüngeren Menschen festgestellt.
- Ob Sozialhilfe, Gesundheitsfürsorge o.ä. – ständig müssen wir unsere Identität nachweisen. Inzwischen plant die Regierung die Einführung eines neuen Personalausweises mit biometrischen Daten (Fingerabdrücke und Iris-Scans), die auch in einer riesigen Personendatenbank gespeichert werden.
- Bei Auslandsreisen wird geprüft, überwacht und gespeichert, wer wir sind, wohin wir fahren und was wir mit uns führen. Auch an unseren Pässen geht die Neuzeit nicht vorüber: Computerchips enthalten Informationen, es liegen – ähnlich wie bei den Personalausweisen – auch schon Vorschläge für biometrische Pässe vor.
- In vielen Schulen gibt es Chipkarten, biometrische Daten überwachen den Aufenthaltsort sowie die Essgewohnheiten der Kinder, oder welche Bücher sie sich aus der Bücherei leihen.
- Software analysiert unser Kaufverhalten und die Daten werden an die unterschiedlichsten Firmen verkauft. Die Höhe unserer Ausgaben, unser Wohnort, unsere gesellschaftliche Stellung – all das bestimmt, wie schnell wir den gewünschten Service oder das gewünschte Angebot erhalten, wenn wir im Callcenter anrufen oder Kredite, Versicherungen oder Hypotheken beantragen.
- Telefone, E-Mails und Internet-Zugriff lassen sich überwachen und werden von britischen und amerikanischen Nachrichtendiensten auf Schlüsselwörter oder -sätze untersucht.
- Unsere Arbeit wird mehr und mehr auf Leistung und Produktivität abgeklopft, unsere Arbeitgeber interessieren sich zunehmend für unsere Einstellung bzw. unseren Lebensstil außerhalb des Arbeitsplatzes.

Überwachung ist die absichtliche, systematische, konzentrierte Routinebeobachtung von Personendaten zu Kontroll-, Anspruchs-, Management-, Beeinflussungs- oder Schutzzwecken. Im Einzelnen heißt das:

- Die Beobachtung erfolgt *absichtlich*; da ihr Kontroll-, Anspruchs- oder andere öffentlich vereinbarte Ziele zugrunde liegen, lässt sie sich rechtfertigen.
- Sie ist *Routine*: Wir begegnen ihr überall im Alltag.
- Die Überwachung erfolgt außerdem *systematisch*, d.h. im Rahmen eines rationalen Plans, der nichts dem Zufall überlässt.
- Und sie *konzentriert* sich größtenteils auf identifizierbare Personen, deren Daten erfasst, gespeichert, übertragen, abgerufen, verglichen, geschürft und verkauft werden.

Dabei kommen die unterschiedlichsten Daten ins Spiel, wie z.B. Kamerabilder (CCTV), biometrische Daten (Fingerabdrücke oder Iris-Scans), Kommunikationsaufzeichnungen oder -inhalte oder – hauptsächlich – numerische bzw. kategoriale Daten. Da sich besonders viele der letztgenannten Daten auf Transaktionen, Austausch, Ist-Zustände, Konten usw. beziehen,

spricht Roger Clarke von dieser Art der Datenüberwachung auch als „Dataveillance“.⁵ Unter Datenüberwachung versteht man die automatische Kontrolle oder Prüfung menschlicher Handlungen oder Kommunikationen unter Einsatz von Informationstechnologie. Sie ist sehr viel kostengünstiger als die direkte oder spezifische elektronische Überwachung und bietet daher Vorteile, die für eine Erweiterung des Systems sprechen, selbst wenn die so erfassten Daten über den ursprünglichen Zweck hinausgehen.

Die Überwachungsgesellschaft aus verschiedenen Blickwinkeln: 1. Verfahren

Im Folgenden wenden wir uns verschiedenen Verfahren und Problemen zu, die in der eingangs beschriebenen Überwachungsgesellschaft eine Rolle spielen. Dieses Kapitel soll als Katalog oder Prüfliste dienen und enthält viele wichtige Punkte, die in der Debatte zur Überwachungsgesellschaft berücksichtigt werden müssen. Obwohl sie nach Zeitpunkt und Standort unterscheiden, handelt es sich doch um entscheidende Aspekte, wenn man die Parameter einer Überwachungsgesellschaft verstehen will.

In einer Überwachungsgesellschaft ist die *gesellschaftliche Kategorisierung* („*Social Sorting*“) ganz normal. Die Analyse und Kategorisierung staatlicher und kommerziell genutzter Riesendatenbanken mit Personenangaben führt zur Aufteilung in Zielmärkte und Risikogruppen.⁶ Und wer einmal klassifiziert wurde, kommt aus dieser Schublade nicht so schnell wieder heraus. Seit 9/11 hat diese Kategorisierung vielleicht zu einem sichereren Luftraum geführt (was sich jedoch nicht beweisen lässt), gleichzeitig hat sie aber auch grobe Profilgruppen (z.B. Muslime) entstehen lassen und Nachteile, Härten und sogar Folter mit sich gebracht. Die gesellschaftliche Kategorisierung definiert die Überwachungsgesellschaft immer mehr. Sie ermöglicht den unterschiedlichen Gesellschaftsgruppen unterschiedliche Chancen und führt auf oft raffinierte und zuweilen unbeabsichtigte Weise zu einer Neuordnung der Gesellschaft, zu Politik ohne demokratische Debatten.

Datenflüsse: Die von den Überwachungssystemen gesammelten Daten fließen durch die Computernetze. Viele Menschen geben ihr Einverständnis für die Erfassung ihrer Daten an einer Stelle, doch was passiert mit diesen Daten, wenn sie auf einen anderen Computer übertragen werden? Immer häufiger wird der Ruf nach dem Einsatz der unterschiedlichsten Datenbanken laut, wenn es um den Schutz vor Kindesmissbrauch oder den Kampf gegen Sozialbetrug geht. Doch weder die breite Öffentlichkeit noch die mit der Weiterleitung unserer Daten betrauten Stellen wissen genau, wohin diese Daten wandern. Man geht davon aus, dass verfahrenstechnische Richtlinien der Aufklärung dienen. Diese Idee sowie das Vernetzungs- und Datenabgleichungspotenzial der modernen digitalen Infrastruktur lassen also darauf schließen, dass die Überwachung einer ihr eigenen Logik folgt. Diese Logik muss jedoch in Frage gestellt, untersucht und geprüft werden – vor allem dann, wenn Daten von einer Station zur nächsten fließen.

Schleichende Funktionsausweitung tritt überall dort auf, wo Personendaten zu einem bestimmten Zweck erfasst und eingesetzt, dann jedoch auf andere Funktionen übertragen werden und somit die Überwachung und der Eingriff in das Privatleben über den ursprünglich beabsichtigten Umfang, d.h. über die gesellschaftlich, ethisch und rechtlich akzeptablen Grenzen hinausführen. Ein Beispiel: Die individuellen Transportdaten auf der Londoner Oyster-Card (für öffentliche Verkehrsmittel) werden bereits verstärkt von der Polizeifahndung angefordert.⁷ Die schleichende Funktionsausweitung erfolgt still und leise im Rahmen administrativer Dienlichkeit. Da diese neuen Technologien einen immer intensiveren Datenaustausch ermöglichen und organisatorische Effizienz häufig als oberste Priorität gilt,

⁵ Clarke, R. (2006[1997]) „Introduction to dataveillance and information privacy“, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV>

⁶ Siehe auch die klassische Studie von Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information*, Boulder CO: Westview Press.

⁷ Siehe: „Oyster data use rises in crime clamp-down“ *The Guardian*, 13. März 2006, <http://politics.guardian.co.uk/foi/story/0,,1730771.00.html>

werden ihre menschlichen Folgen nur allzu oft gar nicht erkannt, ignoriert oder heruntergespielt.

Technologie: Obwohl Technologie eine Grundvoraussetzung für die Überwachung ist, dürfen wir zwei wichtige Aspekte nicht außer Acht lassen: Zum einen existiert die direkte „menschliche Überwachung“ ohne technologische Hilfsmittel auch heute noch, wird aber häufig mit technologisch untermauerten Überwachungsarten in einen Topf geworfen. Zum anderen ist die Technik weder Ursache noch Gesamtheit der modernen Überwachung. Ihre Konsequenzen lassen sich nicht einfach von den jeweiligen Fähigkeiten eines neuen Systems ablesen. Wer die Überwachungsgesellschaft wirklich verstehen will, muss einen tiefen Einblick in die Arbeitsweise dieser Technologien gewinnen und ihre Funktionsweise (im Rahmen eines interaktiven Prozesses, an dem eigenes Personal ebenso teilhaben muss wie technologische Berater und Fachleute) sowie ihren Einfluss auf den Betriebsablauf verstehen lernen. Darüber hinaus müssen wir diese Dinge gut genug durchschauen, um Methodik und Praxis entsprechend beeinflussen zu können. Dies geht auch aus der an späterer Stelle folgenden Diskussion über die Bewertung der Auswirkungen hervor.

Ein weiterer Grund zur Besorgnis ist die Tatsache, dass viele die Angst vor einer Überwachungsgesellschaft (fälschlicherweise, wie sich zeigen wird) mit weiteren technischen Mitteln beruhigen möchten. Tatsächlich können moderne Datenschutztechnologien (Privacy-enhancing Technologies – PETs) die steigende technologische Überwachung einschränken und sollten deshalb, wo immer dies angemessen erscheint, eingesetzt werden. Doch das ist bestenfalls eine Teilantwort auf das Problem. Wir sollten Angebote, die sogenannte technische Probleme ausschließlich mit technischen Lösungen angehen, mit Vorsicht genießen. Wie sich zeigen wird, ist die reale Überwachungsgesellschaft viel zu komplex für solch oberflächliche Reaktionen.

Die Überwachungsgesellschaft aus verschiedenen Blickwinkeln: 2. Probleme

Privatsphäre, Ethik, Menschenrechte: Seit den 70er Jahren ist Überwachung in aller Munde, wird auch unter rechtlichen Gesichtspunkten diskutiert und hat in Europa und andernorts zu vielen neuen Datenschutzgesetzen geführt. Dieser Gesetzgebung liegt jedoch ein ganz spezielles Verständnis des Datenschutzes zugrunde. Zwar wurden die Grundsätze für einen fairen Informationsaustausch in den USA z.B. in Form der „Fair Information Principles“ – FIPs⁸ weiterentwickelt, dennoch war es recht schwierig, die Politiker auch von den tieferen *gesellschaftlichen* Dimensionen des Datenschutzes⁹ zu überzeugen, ganz zu schweigen von der Notwendigkeit, sich mit den Problemen der Überwachungsgesellschaft als solches auseinanderzusetzen. Die Überwachungsgesellschaft stellt uns vor ethische und menschenrechtliche Dilemmas, die weit über das Thema Privatsphäre hinausgehen. Man kann von Otto Normalverbraucher nicht erwarten, dass er sich selbst schützt. Dabei treten die drei folgenden Kernprobleme auf:

Gesellschaftliche Ausgrenzung, Diskriminierung

Die Überwachungsintensität unterscheidet sich je nach Standort und Gesellschaftsschicht, ethnischer Zugehörigkeit und Geschlecht. Überwachung, Eingriffe in die Privatsphäre und Datenschutz unterscheiden sich je nach Gruppe, bieten Vorteile für einen Gesellschaftsteil und Nachteile für einen anderen. Der Sozialstaat „von der Wiege bis zur Bahre“ – einst stolzes Versprechen sozialdemokratischer Regierungen – wurde auf ein simples Risikomanagement reduziert, das umfassende Kenntnis der jeweiligen Sachlagen – und damit eine Überwachungsgesellschaft – verlangt. Die Erfassung von Personendaten ist damit eine Grundvoraussetzung für die Verteilung der Ressourcen.¹⁰

⁸ FIPs sind das nordamerikanische Pendant der europäischen „Datenschutzgrundsätze“.

⁹ Siehe die ausgezeichnete Ausführung zur Sozialität des Datenschutzes in: Regan, P. (1005) *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill: University of North Carolina Press.

¹⁰ Ericson, R. und Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.

Wahlfreiheit, Macht und Ermächtigung

Normale Mitbürger können und werden Änderungen bewirken – vor allem, wenn sie auf die Einhaltung vorgegebener Richtlinien und Gesetze pochen, das System hinterfragen oder ihre Daten nicht zu ungenauen oder zweifelhaften Zwecken hergeben. Wie weit aber kann eine Einzelperson oder Gruppe ihre individuelle Überwachung kontrollieren und die Erfassung bzw. Nutzung derartiger Personendaten einschränken? Die Infrastruktur eines Systems und sein technischer Nimbus verhindern häufig einen tieferen Einblick. Da scheint es sehr viel schwieriger, den kleinen Unterschied zu bewirken. Das Ausmaß persönlicher Profilerstellung durch Großkonzerne¹¹ wird vielen Verbrauchern z.B. erst dann klar, wenn ein Identitätsdiebstahl in den Medien publik gemacht wird. Und selbst in so einem Fall scheint sich alles um Sicherheit und Vorbeugung gegen ähnlich betrügerische Aktivitäten zu drehen. Dass die Macht großer Konzerne bzw. staatlicher Behörden über den häufigen und ausgedehnten Einsatz individueller Daten eingeschränkt werden sollte, wird kaum erwähnt. Wenn es um die Auswirkungen der Überwachung auf ihr Leben geht, sind Einzelpersonen deutlich im Nachteil.

Transparenz, Verantwortlichkeit: Einzelne Personen und Gruppen können kaum feststellen, was eigentlich mit ihren Personendaten passiert oder wem sie wann und zu welchem Zweck in die Hände geraten. Schritt für Schritt verändern genau diese Personendaten unsere Lebenschancen und lenken unsere Wahlmöglichkeiten. Wenn große Organisationen aber über solch ausgereifte Überwachungskapazitäten verfügen, dann scheint es nur fair, dass auch der einzelne Bürger – und sei es nur um des Prinzips willen – ein Mitspracherecht erhält, und zwar nicht nur über spezielle Organe, sondern auch über Interessensgruppen und die Massenmedien.

Die zuständigen Organisationen müssen hier zur Verantwortung gezogen werden – vor allem dann, wenn eine intensive Überwachung routinemäßig und mit potenziellen Folgeschäden durchgeführt wird. Sicherlich lassen sich aus der Überwachung am Arbeitsplatz einige Lehren hinsichtlich der Arbeitsabläufe ziehen, doch in einigen Fällen zwangen Gewerkschaften die Arbeitgeber bereits aktiv dazu, ihre übertriebene Überwachung zurückzuschrauben. Mit Transparenz lässt sich hier viel erreichen: Wenn der Arbeitgeber das Ausmaß der Überwachung erläutert und das informierte Einverständnis seiner Belegschaft einholt. Für die Überwachung des Verbrauchers gilt dies jedoch nicht, die außerordentliche Datenmacht von Supermarktketten wie Tesco oder Walmart ist nahezu unerreichbar. Im Zuge der modernen Überwachungsgesellschaft ist hier ein Wandel vom Selbstschutz gegen Datenmissbrauch hin zur Verantwortlichkeit der Datensammler unerlässlich, und zwar parallel zu den Aufgaben der Aufsichtsbehörden, d.h. der aktiven Kontrolle und Druckausübung in Richtung minimaler Überwachung.

2. Ein Überblick über die Überwachungsgesellschaft

Das Surveillance Studies Network gab eine Reihe von Gutachten mit den folgenden Themen in Auftrag: Gesundheitswesen und medizinische Versorgung; Konsumwesen; Arbeit und Beschäftigung; Öffentliche Dienste; Bürgerrechte; Kriminalität und Justiz; Kommunikation; Urbanisierung und Infrastruktur; Landesgrenzen. Aus diesen Gutachten gehen mehrere Hauptpunkte hervor, die sich wiederum in vier verschiedene Aspekte aufteilen lassen: Die Überwachungsgesellschaft im Kontext; Überwachungstechnologien; Implementierung und Funktionsweise der Überwachung; Auswirkungen der Überwachung auf gesellschaftliche Gruppen und Einzelpersonen. Selbstverständlich überschneiden sich diese Aspekte in vielerlei Hinsicht und weisen auch weitere Gesichtspunkte auf, die jedoch hier nicht berücksichtigt wurden.

¹¹ Siehe Leitartikel der *New York Times*, „The data-fleeing of America“ 21. Juni 2005.

Die Überwachungsgesellschaft im Kontext

Zu Beginn möchten wir mehrere grundlegende Trends in westlichen Gesellschaften erläutern, auf denen eine Überwachungsgesellschaft aufbaut: Risiko und Sicherheit; Militarisierung der Überwachung; Überwachung als politischer Wirtschaftsfaktor; Wachstum der individuellen Datenschutzbemühungen.

Risiko und Sicherheit: Die moderne Gesellschaft ist risikobesessen. Das Management externer und interner Risiken ist heute integraler Bestandteil organisatorischer Aktivitäten. Dabei hat sich ein Wandel von *vorbeugenden* Maßnahmen gegen diese Risiken zu *Präventivschlägen* vollzogen.¹² Vor allem die explorative Datenanalyse (Data Mining) und die Profilerstellung, die zur Identifizierung dieser Risiken herangezogen werden, verlagern die Praxis in Richtung einer totalen Überwachung der Handlungen und Transaktionen der breiten Öffentlichkeit.¹³ Diese totale Überwachung lässt sich präventiv gegen Personen oder Personengruppen einsetzen, die entweder als gefährdet oder als Risiko für andere eingestuft werden. Grundbedingung hierfür ist die Datenerfassung und -analyse – u.a. auch von Informationen, die Rückschlüsse auf die Person zulassen. Zwar können so persönliche und gesellschaftliche Vorteile erzielt werden, doch gleichzeitig wirkt sich das Konzept Sicherheit deutlich auf die Freiheit, Privatsphäre und andere gesellschaftliche Werte sowie auf Innovation und Wandel aus.

Hier einige Beispiele für den Trend in Richtung Risikoanalyse und Präventivmaßnahmen:

- Epidemiologie und Modellierung in der medizinischen Überwachung¹⁴ zur Identifizierung isolierter Fälle, zur Aufzeichnung von Krankheitsausbrüchen zu statistischen Zwecken oder zur Identifizierung einzelner Bevölkerungsgruppen, die für bestimmte Krankheiten anfälliger sind.
- Risikoanalysen von Einzelpersonen, Familien und Gemeinschaften mit Blick auf den Kinderschutz, psychische Störungen und die Strafjustiz.
- Kategorisierung des Risikos, das Reisende für die nationale Sicherheit darstellen, unter Bezugnahme auf Landungslisten und finanzielle Transaktionen.
- Kalkulation des relativen Werts individueller Verbraucher sowie Erstellung ihres geodemografischen Profils.

Militarisierung der Überwachung: Im Zeitalter der sogenannten Globalisierung gehört die militärische Überwachung zu den wenigen Phänomenen, die tatsächlich die ganze Welt umspannen. Eine Vielzahl militärischer Überwachungssatelliten umkreist den Erdball, militärische Abhörsysteme haben die länderübergreifende Kommunikation längst infiltriert. GPS (Global Positioning System) und das Internet sind nur zwei moderne Systeme, die sich auch militärisch nutzen lassen. Die Geschichte der modernen Überwachung mit dem Ziel, unseren Planeten verteidigen zu können und sicher zu machen, lässt sich aber bis zur Entwicklung der C3I-Systeme (Command, Communications, Control and Intelligence) zurückverfolgen, die im Zweiten Weltkrieg und im nachfolgenden Kalten Krieg zur Kommunikation, Kontrolle und Aufklärung entstanden¹⁵. Diese Wechselwirkung zeigt sich nicht nur in den einzelnen Bestandteilen von Regierung und Technologie, sondern auch in der Tatsache, dass die alltägliche Sicherheit verstärkt mit militärischen Ausdrücken beschrieben wird. Öffentliche Organe und Massenmedien reden von der „Analyse des

¹² Ewald, F. (2002) „The return of Descartes’ malicious demon: an outline of a philosophy of precaution”, in Baker, T. und Simon, J. (Hg.), *Embracing Risk: The Changing Culture of Insurance and Responsibility*, Chicago: University of Chicago Press.

¹³ Valverde, M. und Mopas, M. (2004) „Insecurity and the Dream of Targeted Governance”, in Lerner, W. und Walters, W. (Hg.) *Global Governmentality: Governing International Spaces*, London: Routledge.

¹⁴ Zum Machtanstieg der Gesundheitswirtschaft, einem Feld, das epidemiologische Methoden und Ergebnisse weitgehend auf die Bewertung medizinischer Technologie anwendet, siehe z.B.: Ashmore, M., Mulkay, M. J. und Pinch, T. J. (1989) *Health and Efficiency: A Sociology of Health Economics*, Buckingham: Open University Press.

¹⁵ de Landa, M. (1991) *War in the Age of Intelligent Machines*, Cambridge MA: MIT Press; Edwards, P. (1997) *Computers and the Politics of Discourse in Cold War America*, Cambridge MA: MIT Press.

Bedrohungspotenzials“, vom „Krieg gegen Drogen“, vom „Krieg gegen die Kriminalität“ und sogar vom „Krieg gegen den Terror“, von gesetzlicher Härte, von „Nulltoleranz“ usw. Der „Informationskrieg“ hat sich aus dem Schatten geheimer Militäroperationen gelöst und steht nun im Rampenlicht kommerzieller Ziele, wo Industriespionage grassiert und Experten für Computer-Hacking und Sicherheit in „Wissenskrieger“ umbenannt werden. Viele Unternehmen für Überwachungstechnologie sind eng mit dem Militär verbunden, bieten ihre Produkte aber auch für zivile Zwecke an. So entwickelte sich TRW, ein wichtiger Partner des US-Verteidigungsministeriums, auch zum führenden Unternehmen für zivile Biometrik. Und das französische Unternehmen Sagem produziert das gesamte Spektrum – von Handys über Überwachungsalgorithmen bis hin zu unbemannten Spionageflugkörpern.

Überwachung als politischer Wirtschaftsfaktor: Gemeinsam mit traditionellen Sicherheitsdiensten sowie großen Militärlieferern stellen diese neuen Unternehmen einen Teil des allgemein als „Sicherheitsbranche“ bekannten Sektors dar. Für die wachsende Überwachung sind aber auch andere Bereiche wichtig, vor allem Telekommunikation und Computer sowie das Bank- und Versicherungswesen. Sie alle haben die Sicherheitsbranche in den vergangenen Jahren massiv vorangetrieben. Laut dem 100-Firmen-Index des US-amerikanischen Beratungsunternehmens Security Stock Watch¹⁶ schlägt das Wachstum dieser Branche insgesamt regelmäßig den Dow Jones sowie den Hightech-Index NASDAQ¹⁷. Zum Ende des Geschäftsjahres 2005/6 hatte sich der Index mit geschätzten Börsenwerten aller 100 aufgeführten Unternehmen auf über 400 Milliarden US-Dollar gesteigert und damit innerhalb von drei Jahren mehr als verdoppelt.

Individuelle Datenschutzbemühungen: Doch die Überwachung wird nicht nur vom Staat oder großen Organisationen sondern auch vom Bürger selbst durchgeführt. Nach den Bombenattentaten auf die Londoner U-Bahn im Jahr 2005 hielten sowohl Fernsehsender als auch die Polizei die Bürger dazu an, verdächtige Personen mit ihren Handy-Kameras zu fotografieren. Immer mehr Menschen, vor allem Kinder und Jugendliche, stellen ihr Leben inzwischen gern zur Schau und beobachten das Leben anderer – sei es über Online-Webcams¹⁸ oder private Netzwerk-Webseiten wie *MySpace* und *Bebo*. Außerdem beginnen Computerkenner langsam mit dem Management ihres „Daten-Doubles“, u.a. in den Datenbanken von Kreditprüfungsagenturen wie *Experian* oder *Equifax*, die Einzelpersonen den Online-Zugriff auf ihre persönlichen Kreditdaten sowie die Hinterfragung und Korrektur irreführender Informationen ermöglichen. Diese Kombination aus freiwilliger Unternehmenstransparenz und privaten Autodidakten darf jedoch nicht als gesetzliche Regelung missverstanden werden, auch wenn die nachfolgenden Generationen zu Bürgern heranwachsen, denen die aktive und passive Überwachung sowie deren Handhabung längst normal erscheint.

Überwachungstechnologie

Auch wenn man die Bedeutung der nicht-technologischen Überwachung (also z.B. Lauschangriffe, Spionage und direkte, persönliche Überwachung) nicht außer Acht lassen darf, konzentriert sich dieser Abschnitt doch vorrangig auf Brennpunkte, die sich aus der Überwachungstechnologie ergeben. Dabei richten wir unseren Fokus zuerst auf sich überschneidende Fortschritte in vier Bereichen: Telekommunikation, Videoüberwachung, Datenbanken, Biometrik und Technologien zur Standortbestimmung und Ortung (Locating) sowie zur Bewegungskontrolle (Tagging) und Hausarrestüberwachung (Tracking). Anschließend widmen wir uns den Abhängigkeiten zwischen den einzelnen Technologien und dem Trend in Richtung einer unsichtbaren und gleichzeitig allgegenwärtigen

¹⁶ Zu diesem Index gehören die folgenden Branchen: „Bioverteidigung“, „Umweltsicherung“, „Betrugsprävention“, „militärische Verteidigung“, „Netzwerksicherheit in der Telekommunikation“ und „physische Sicherheit“ (Barrieren, Videoüberwachung usw.).

¹⁷ *SecurityStockWatch.com 100 Index*, August 2006, <http://www.securitystockwatch.com/>

¹⁸ Koskela, H. (2004) „Webcams, TV Shows and Mobile phones: Empowering Exhibitionism“, *Surveillance & Society*, CCTV Special (Hg. Norris, McCahill und Wood), 2(2/3): 199-215, <http://www.surveillance-and-society.org/cctv.htm>

Überwachungstechnologie. Abschließend befassen wir uns mit den Grenzen der technologischen Entwicklung.

Technologische Entwicklung: Niemand kann bestreiten, dass sich die Überwachung mithilfe neuer Technologien gewandelt hat. Und diese neuen Systeme lassen sich nicht in „gut“ und „böse“ einteilen. Effiziente Datenbanken auf Landesebene können einer gezielten Gesundheitsversorgung, aber auch der Schikanie von politischen Gegnern dienen. Und das Problem geht weit über die eigentliche Nutzung hinaus. Alle Technologien werden von individuellen Organisationen entwickelt, die bestimmte Ziele und Interessen verfolgen. Deshalb möchten wir an dieser Stelle einige Technologien und ihre Fähigkeiten vorstellen.

Telekommunikation: Die Überwachung in der Telekommunikation bezieht sich auf das Ausmaß, mit dem Einzelpersonen, Organisationen und Unternehmen Informationen über Häufigkeit und Inhalt der Telekommunikation zwischen einzelnen Geräten oder zwischen Geräten und Personen überprüfen, sortieren und speichern können. Seit es staatliche „Lauschangriffe“ gibt, werden im Bereich Telekommunikation für eine immer intensivere Überwachung zunehmend ausgereifere Technologien eingesetzt. Der Standort eines mobilen Geräts lässt sich z.B. mittels Triangulation, d.h. der sukzessiven Verbindung des Gerätesignals mit den Empfängern an verschiedenen Bodenstationen, ermitteln. Diese Informationen können später zur explorativen Datenanalyse (Data Mining) verwendet werden. Das „ECHELON-System“, das weltweit einsetzbare Überwachungsnetz des amerikanischen Nachrichtendienstes NSA, unterhält in Menwith Hill in Nord-Yorkshire (GB) eine riesige Basis, die routinemäßig die gesamte Telekommunikation in Großbritannien auf Schlüsselwörter und -sätze untersucht und zunehmend ausgereifere Algorithmen für hochwertige Sprach- und selbst Bedeutungserkennung einsetzt¹⁹.

Videoüberwachung (CCTV): Fotografische Überwachung gibt es schon seit Ende des 19. Jahrhunderts. Die jüngste Flut an CCTV-Installationen (seit Anfang der 60er Jahre des 20. Jahrhunderts) wurde von dem Versuch ausgelöst, die Verödung innerstädtischer Einkaufsbereiche aufzuhalten, sowie von der Angst vor Terrorismus und Kriminalität. Inzwischen gibt es wohl rund 4,2 Millionen CCTV-Kameras in Großbritannien, d.h. eine Kamera je 14 Einwohner²⁰, eine einzige Person kann täglich von mehr als 300 Kameras aufgenommen werden.²¹ In den 90er Jahren gab das britische Innenministerium 78% seines Etats zur Verhütung von Kriminalität für CCTV-Anlagen²² aus. Diese CCTV-Infrastruktur kostete den Steuerzahler im vergangenen Jahrzehnt laut Schätzungen rund 500 Millionen GBP²³. Dennoch kam eine Studie des britischen Innenministeriums zu dem Schluss, dass „die bewerteten CCTV-Programme insgesamt nur geringen Einfluss auf die Kriminalitätsraten hatten“.²⁴ Die Digitalisierung erlaubt den zunehmend automatisierten Einsatz von CCTV-Anlagen, derzeit allerdings hauptsächlich im Straßenverkehr. Kfz-Kennzeichen dienen zur Identifizierung des Fahrzeughalters. Die Kameraüberwachung von Geschwindigkeitsbegrenzungen steigerte sich von gerade einmal 300.000 Strafzetteln im Jahr 1996 auf mehr als zwei Millionen im Jahr 2004 und bringt dem britischen Staat damit

¹⁹ Campbell, D. (1999) *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control)* Band 2/5: *Interception Capabilities 2000*, Luxemburg: Europa-Parlament, Generaldirektorat Forschung, Direktorat A, STOA-Programm; Wood, D. (2001) *The Hidden Geography of Transnational Surveillance*, unveröffentlichte Doktorarbeit, University of Newcastle, GB.

²⁰ McCahill, M. und Norris, C. (2003), „Estimating the extent, sophistication and legality of CCTV in London“, in M. Gill (Hg.) *CCTV*, Perpetuity Press.

²¹ Norris, C. und Armstrong, G. (1999), *The Maximum Surveillance Society: The Rise of Closed Circuit Television*, Oxford: Berg.:42.

²² *ibid.*: 54.

²³ Norris, C. (2006) „Closed Circuit Television: a review of its development and its implications for privacy“, ein Referat für die Quartalsversammlung des Department of Home Land Security Data Privacy and Integrity Advisory Committee vom 7. Juni in San Francisco, Kalifornien.

²⁴ Gill, M. und Spriggs, A. (2005) *Assessing the impact of CCTV*. London, Home Office Research, Development and Statistics Directorate, 43, 60-61.

alljährlich Bußgelder in Höhe von 113 Millionen GBP ein.²⁵ Dieser Anstieg staatlicher Überwachung sorgt für einen Strom negativer Presse²⁶ – und das, obwohl die Geschwindigkeitsüberwachung per Kamera (ganz im Gegenteil zur normalen CCTV-Überwachung) die Zahl der Todesfälle und Verletzten im Straßenverkehr deutlich reduziert.²⁷ Es gibt bereits Pläne, die Verarbeitungskapazität des britischen Datenzentrums für automatisch erkannte Kfz-Kennzeichen (Automatic Number Plate Recognition – ANPR) bis 2008 von derzeit 35 Millionen automatisch erkannter Kfz-Kennzeichen pro Tag auf 50 Millionen zu steigern.

Die Datenbank: Im Vergleich zu herkömmlichen Papierakten, ehemals Kennzeichen einer modernen Bürokratie, lassen sich Mehrfachdaten heute sehr viel schneller und genauer sammeln, registrieren und querverweisen. Die Überwachung per Datenbank wird daher auch als Datenüberwachung (Dataveillance) bezeichnet. In Verbindung mit anderen Überwachungssystemen ist auch eine algorithmische Überwachung möglich, d.h. die Bearbeitung gespeicherter Bilder oder Daten mittels entsprechender Software und ihre Abgleichung mit bereits vorhandenen Datenbankinformationen – siehe auch die Entwicklung der Biometrik. Datenüberwachung greift vor allem im Marketing, in der Medizin sowie bei Polizei- und Grenzkontrollen immer mehr um sich.

Im *Marketing*bereich sammeln z.B. viele Unternehmen im Privatsektor angesichts immer kostengünstigerer Datenbanken so viele Informationen über ihre Kunden wie nur möglich und machen damit ihr Marketing wesentlich spezifischer. Transaktionsdaten (über den Einsatz von Kreditkarten, Handys usw.) werden mit weiteren Daten von Kundenkarten, Kundenumfragen, Fokusgruppen, Preisausschreiben, Bitten um Produktinformationen, Callcenter-Anrufen, „Cookies“ auf Webseiten, Verbraucherforen und Kredittransaktionen abgeglichen. Danach werden diese *internen* und zumeist firmeneigenen Daten häufig mit Daten aus *externen* Quellen überlagert, so z.B. vom statistischen Bundesamt, von gemeinnützigen Organisationen oder speziellen Unternehmen für die Datenerhebung. In Verbindung mit Postleitzahlen entstehen so individuelle Straßenprofile, deren Bewohner sich als „vorsichtige Rentner“, „junge Familien“ oder „alteingesessene Arbeiter“ entpuppen.²⁸ Die einfache Abgleichung und geodemografische Profile werden durch den ausgereifteren „heuristischen“ (Lern-)Prozess des Data Mining bereichert, der als Knowledge Discovery in Databases (KDD) bekannt ist. KDD identifiziert versteckte und *nicht-offensichtliche* Muster innerhalb vorgegebener Informationsgruppen²⁹ und liefert anschließend neue Daten, die meist als Grundlage personalisierter Websysteme sichtbar werden. So nutzt *Amazon* unterschiedliche Datenquellen, um den zukünftigen Bedarf seiner Kunden zu prognostizieren.³⁰

Biometrische Daten: Alle neuen ID-Systeme nutzen die eine oder andere Form biometrischer Daten oder Körpermerkmale: Fingerabdrücke, Iris-Scans, Gesichtskonturen und Hand-Scans

²⁵ Wilkins, G. und Additcott, C. (1998) *Motoring Offences England and Wales 1996*, Home Office Statistical Bulletin, London: Home Office; Ransford, F., Perry, D., Murray, L. (2005) *Motoring Offences and Breath Test Statistics: England and Wales 2003*, Home Office Statistical Bulletin, London: Home Office.

²⁶ McCahill und Norris, 2003 *op cit.* n.44.

²⁷ PA Consulting (2004) *Denying Criminals the Use of the Road*, http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10.000_Arrests.pdf?view=Binary

²⁸ Die erste Kategorie stammt aus dem Klassifikationssystem ACORN des Unternehmens CACI und die beiden letzteren aus der MOSAIC-Klassifikation von Experian. Weitere Informationen über die Produkte finden Sie unter <http://www.caci.co.uk/acorn/> und <http://www.business-strategies.co.uk/Content.asp?ArticleID=629>. Siehe auch: Burrows, R. und Gane, N. (i.E.) „Geodemographics, software and class.“ *Sociology*.

²⁹ Weitere Unterschiede zwischen KDD und Data Mining finden sich bei Tavani, H. T. (1999) „KDD, data mining, and the challenge for normative privacy.“ *Ethics and Information Technology* 1: 265-273. In vielen Quellen wird Data Mining als Oberbegriff für die Arbeit an Daten zu den hier beschriebenen Zwecken verwendet. Siehe Rygielski, C., Wang, J.-C. und Yen, D. C. (2002) „Data mining techniques for Customer Relationship Management.“ *Technology in Society* 24: 483-502. Danna und Gandy (2002) *op cit.* n.6. Aus Gründen der Vereinfachung beschreibt der Begriff KDD hier gesamttechnische Verfahren, aus denen sich bestimmte (offensichtliche oder nicht-offensichtliche) Affinitäten innerhalb von Datensets ablesen lassen, und Data Mining als Sammlung kritischer Daten zur weiteren Analyse.

³⁰ Fink, J. und Kosba, A. (2000) „A review and analysis of commercial user modeling servers for personalization on the World Wide Web.“ *User Modeling and User-Adapted Interaction* 10: 209-249.

werden in verschiedenen Pässen bzw. Personal- oder ID-Ausweisen längst eingesetzt. Der Reiz liegt darin, dass sich Informationen oder Daten scheinbar in der physischen Identität einer Person „verankern“ lassen – das biometrische Identifikationsmerkmal als Zugangsberechtigung für gespeicherte Daten. Dies entspricht der Konvergenz von Data Mining und der Integration von Informationen mit biometrischen Identifikationsfaktoren. Man geht davon aus, dass ihre Genauigkeit optimiert und betrügerische Aktivitäten damit reduziert werden können. PIN-Nummern und Passwörter kann man vergessen oder verlieren. Körpermerkmale stellen jedoch eine konstante, direkte Verbindung zwischen Aufzeichnungssystem und Person her. Seit Beginn des „Kriegs gegen den Terror“ sprudelt eine wahre Geldquelle für die biometrische Forschung und Implementierung. Und seit 9/11 werden biometrische Erkennungsmethoden, die bereits kommerziell genutzt wurden oder kurz vor ihrer Einführung standen, noch intensiver gefördert und als Wunderwaffe in diesem neuen Krieg gepriesen.³¹ Der US Patriot Act, ein gesetzlicher Rahmen mit weit über die USA hinausreichenden Auswirkungen, führte eine Reihe biometrischer Anwendungen ein und erlaubt nun den nahezu grenzenlosen Einsatz für die Fahndung nach und Identifikation von terroristischen Aktivitäten. In Großbritannien führte der bereits erwähnte Wechsel zur CCTV-Überwachung im Anschluss an erste Experimente in Newham (London), Birmingham und anderswo zu weiteren Forschungsprojekten im Bereich des praktischen Einsatzes biometrischer CCTV-Anlagen sowie der Gesichtserkennung.

Ortung (Locating), Bewegungskontrolle (Tracking) und Hausarrestüberwachung (Tagging)
Abgleich, Organisation und Ortung der Überwachung erfolgt zunehmend über GIS (Geographic Information Systems)³². Oft lässt sich die Bewegungskontrolle von einzelnen Personen, Fahrzeugen oder Waren auch über RFID-Chips, GPS (Global Positioning Systems), intelligente ID-Ausweise/Personalausweise, Transponder oder die Funksignale von Handys bzw. tragbaren Computern durchführen, so z.B. heute bei der Strafverfolgung, Grenzkontrolle oder am Arbeitsplatz.

Strafverfolgung: Im Zeitraum 2004/5 erhielten 631 Erwachsene und 5751 Jugendliche (manche nicht älter als zwölf Jahre) in Großbritannien eine elektronische Fußfessel, mit der sie ihren Prozess zu Hause und nicht in Untersuchungshaft abwarten konnten.³³ Auch Gefangene, die ihre Haftstrafe abgesessen haben, werden verstärkt elektronisch überwacht, sei es als Bedingung ihrer vorzeitigen Entlassung im Rahmen einer Hausarrest-Überwachung per Fußfessel (Home Detention Curfew Scheme)³⁴ oder im Rahmen einer bedingten Haftentlassung³⁵.

US-Grenzkontrolle: An der Grenze zu Mexiko wird mit Grenzausweisen mit RFID-Chips experimentiert. Die RFID-Branche hebt dabei das Potenzial für die Bewegungskontrolle oder Standortüberwachung von Gastarbeitern hervor, die die Grenze nur für kurze Zeit überschreiten. Inzwischen erhalten auch Lebewesen – allen voran Tiere – RFID-Implantate. In den USA wurde 70 Patienten mit degenerativen Hirnkrankheiten ein RFID-Chip eingepflanzt, um den Pflegern ihre Ortung zu erleichtern.³⁶

Arbeitsplatz: Ein Unternehmen setzte zweien seiner Mitarbeiter RFID-Chips ein, um ihnen Zutritt zum Unternehmensgelände zu gewähren.³⁷ Die kontinuierliche Entwicklung beim Einsatz von Echtzeitstandortdaten für Verbraucherprofile liefert eine weitere Datenschicht,

³¹ Amore, L. (2006) „Biometric borders: governing mobilities in the war on terror“, *Political Geography* 25: 2: 336-351; Gates, K. (2005) „Biometrics and post-9/11 technostalgia“, *Social Text* 23(2): 35-53. Irma Van der Ploeg, „Biometrics and the body as information“, in Lyon, D. (Hg.) (2003) *op cit.* n.3.

³² Institute for the Future (2004) *Infrastructure for the New Geography*, Menlo Park, Kalifornien: IFTF.

³³ NPS (National Probation Service) (2006) *Electronic Monitoring* 6.

<http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes>

³⁴ Das HDC-Programm ermöglicht Verurteilten mit einer Gefängnisstrafe von drei Monaten bis maximal vier Jahren eine frühzeitige Entlassung für einen Zeitraum zwischen zwei Wochen und 4½ Monaten. Voraussetzung ist jedoch eine Ausgangssperre, die über elektronische Fußfesseln kontrolliert wird. Im Zeitraum 2004/5 wurden 19.096 Personen im Rahmen dieses Programms frühzeitig entlassen. (*ibid.*: 6).

³⁵ NPS *op cit.*

³⁶ Bei diesem Unternehmen handelt es sich um die Verichip Corporation. <http://www.verichipcorp.com/>

³⁷ Waters, R. (2006) „US group implants electronic tags in workers“, *Financial Times*, 12. Februar 2006. <http://www.ft.com/cms/sec414700-9bf4-11da-8baa-0000779e2340.html>

die Unternehmen bei der gezielten Ausrichtung ihrer Marketingkampagnen auf individuelle Verbraucher unterstützt. Es ist daher mehr als wahrscheinlich, dass sich diese Technologien auch an anderer Stelle „einschleichen“ werden.

Technologische Synergien und schleichende Funktionserweiterung: Zwar sind die Funktionsmerkmale einzelner Technologien und Systeme von großer Bedeutung, doch lässt sich auch eine immer größere technologische Synergie bzw. Konvergenz unterschiedlicher Überwachungstechnologien feststellen. Dieser Langzeittrend bei Computersystemen wird u.a. von dem Wunsch nach Größenvorteilen motiviert. Immer mehr Systeme sind auf eine Wechselwirkung mit anderen angelegt. Daher können aus den älteren Technologien (deren Funktion von den Aufsichtsorganen verstanden und kontrolliert wurde) völlig unvorhergesehen neue und unkontrollierte Produkte hervorgehen. Ein Beispiel:

- ID-Ausweise, die mehreren Zwecken dienen: Grenzüberschreitung, Betrugskontrolle, Zugriff auf staatliche Informationen und ggf. sogar kommerzielle Zwecke (Videoverleih) oder halbkommerzielle Zwecke (Büchereien). Beeinflussen jedoch der „Krieg gegen den Terror“, das Ziel unerwünschte Einwandererströme zu zügeln oder die Suche nach einer Lösung gegen Sozialbetrug die Entwicklung neuer ID-Systeme, wird das „unpersönliche“ Ethos der klassischen Bürokratie untergraben.
- Die in London eingesetzte automatische Erkennung von Kfz-Kennzeichen (ANPR) wurde ursprünglich für militärische Zwecke entwickelt, dann zur Identifikation von Bombenlegern der IRA eingesetzt und dient heute der Verkehrsregelung, der kommunalen Ertragssteigerung und der Absicherung gegen eine neue Terroristengeneration.

In Richtung einer allgegenwärtigen Überwachung: Technologie wird vor allem dann besonders wichtig, wenn sie immer und überall vorhanden ist und ihre – nahezu unsichtbare – Existenz als gegeben vorausgesetzt wird. Allgegenwärtige und flächendeckende Rechner (Ubicomp), die auch als „umgebende Intelligenz“ (Ambient Intelligence – AmI) bekannt sind, bereiten auf eine allgegenwärtige und flächendeckende Überwachung vor, die sich in die physische und virtuelle Umwelt einbetten lässt.³⁸ Im Vergleich zu Stadtstraßen sind elektronisch gesteuerte Dienstleistungen und Bereiche relativ leicht zu kontrollieren, doch auch im Alltag durchqueren wir immer mehr „Übergänge“, die eine enge Zusammenarbeit sowohl elektronischer als auch physischer Bestandteile voraussetzen. Die Kombination von CCTV, biometrischen Daten, Datenbanken und Bewegungskontrollen gilt heute als Teil einer sehr viel breiter angelegten Forschung (häufig über den britischen/amerikanischen „Krieg gegen den Terror“ finanziert), die den Einsatz miteinander verbundener „intelligenter“ Systeme zur zeitlichen und geografischen Bewegungs- und Verhaltenskontrolle von Millionen Menschen untersucht. Im Industriejargon spricht man auch von „multiscale spatiotemporal tracking“ (vielschichtige, zeit- und ortsgebundene Bewegungskontrolle).³⁹

Die Grenzen der Technologie:

Natürlich verspricht uns die Technik meist mehr als sie tatsächlich halten kann. Die biometrischen Anlagen für das amerikanische USVISIT-Programm wurden z.B. aus logistischen Gründen von den geplanten Iris-Scans auf digitale Fingerabdrücke reduziert. Und auch die Zuverlässigkeit gibt Anlass zur Besorgnis⁴⁰: Biometrische Daten, die vom System nicht erkannt werden, sind ebenso möglich wie fälschlicherweise nicht akzeptierte Personenmerkmale bei einer zweiter Lesung. Trotzdem werden weitreichende Implementierungsentscheidungen oft schon vor ausführlichen Tests gefällt. Schätzungen

³⁸ Kang, R. und Cuff, D. (2005) „Pervasive Computing: Embedding the Public Sphere,“ *Washington and Lee Law Review* 62(1): 93-146. Cuff, D. (2002) Immanent domain: Pervasive computing and the public realm, *Journal of Architectural Education*, 57: 43-49.

³⁹ Hampapur, A. et al. (2005), „Smart video surveillance“, *IEEE Signal Processing Magazine*, März: 38-51.

⁴⁰ Siehe: Zureik, E. mit Hindle, K. (2004) „Governance, security and technology: the case of biometrics“ *Studies in Political Economy*, 73: 113-137.

zufolge wird einer von sechs Briten seinen von der Regierung beantragten ID-Ausweis aufgrund technischer Probleme nicht nutzen können.⁴¹ Und auch die Technologien in der Strafverfolgung, wie z.B. die Gesichtserkennung oder die automatische Erkennung von Kfz-Kennzeichen, weisen ähnliche Probleme auf.

Technologische Bindung (Lock-in) und aufsichtstechnische Probleme: Mit fast schon spielerischer Leichtigkeit werden Überwachungstechnologien oft als „perfekte Lösung“ für die verschiedensten Bedrohungen präsentiert, so jüngst für die Terrorismusgefahr. Je mehr wir uns jedoch auf Überwachungstechnologien verlassen, desto mehr entsteht eine technologische Bindung, andere Möglichkeiten mit dem gleichen Ziel werden kaum noch in Betracht gezogen. Es entsteht ein Verständnisgefälle, das unsere Abhängigkeit von Experten außerhalb des demokratischen Systems verstärkt. Die Aufsichtsbehörden hinken technischen Innovationen ständig hinterher und tun sich schwer, deren Funktionsweise tatsächlich zu verstehen. Bei diesem Katz-und-Maus-Spiel müssen wir uns fragen, ob dem Staat tatsächlich alle notwendigen Werkzeuge für eine sinnvolle Steuerung zunehmend komplexer Überwachungstechnologien und -methoden zur Verfügung stehen. Wie bei allen technischen Neuerungen stellt sich auch hier die Frage, ob wir die Geister, die wir riefen, auch wieder loswerden. Über die Umkehrbarkeit der entsprechenden Geräte und Systeme schweigen sich Patenteigentümer oder Anbieter gern aus.

Überwachungsverfahren

Die Bedeutung einer präventiv ausgerichteten Risikoanalyse sowie die Verordnung von Überwachung als Lösung allen Übels hat zu einer Reihe einzigartiger Verfahren und Phänomene geführt: Gesellschaftliche Kategorisierung („Social Sorting“), unvorhersehbare Konsequenzen, die gemeinsame Nutzung von Netzwerkinformationen („Information Sharing“) sowie verwischte Grenzen zwischen öffentlichen und privaten Bereichen sind nur vier Beispiele.

Social Sorting, Kategorisierung und zielgenaue Werbung (Targeting). Social Sorting, also die Kategorisierung der Bevölkerung in unterschiedliche Risiko-, Anspruchs- oder Wertgruppen, lässt sich vielerorts beobachten:

- Der Verbraucher überlässt Unternehmen einen kontinuierlichen Strom an Transaktionsdaten und wird damit Teil einer dynamischen Feedback-Schleife, die seine Käufe mit Datenerfassung und Profilerstellung verbindet.⁴² Längst orientiert sich das jeweilige Dienstleistungsniveau eines Callcenters an der relativen Ausgabenhöhe des Kunden. Und auch die Telekom-Branche speichert Verkehrsdaten, um die besten Werberouten zu identifizieren (z.B. Marketing per SMS).
- Gesellschaftliche und Lifestyle-Faktoren spielen bei der Einstellung von Callcenter-Mitarbeitern eine Rolle, damit sie dem bedienten Marktsegment besser entsprechen.
- Auf vielen Inlands-, Flug- und Seehäfen gehört die „bevorzugte Schnellabfertigung“ längst zum Alltag, so z.B. durch das System „Privium“ auf dem niederländischen Flughafen Schiphol, das lange Warteschlangen an der Passkontrolle durch Iris-Scans ersetzt.

Unbeabsichtigte Kontrolle: Überwachung darf nicht mit einer direkten Kontrolle der Gesellschaft verwechselt werden.⁴³ Häufig verfolgt die Überwachung einfach nur das Management effizienter und nahtloser Waren-, Personen- und Informationsflüsse.⁴⁴ Was dem

⁴¹ Siehe: Grayling, A.C. (2005) *In Freedom's Name: The Case Against Identity Cards*, London: Liberty.

⁴² Genauere Erläuterungen in: Elmer, G. (2004). *Profiling Machines: Mapping the Personal Information Economy*. Cambridge, MA: The MIT Press.

⁴³ Lianos, M. (2001) *Le Nouveau Contrôle Social: toile institutionnelle, normativité et lien social*. Paris: L'Harmattan-Logiques Sociales.

⁴⁴ Graham, S. und Wood, D. (2003) „Digitising surveillance: categorisation, space and inequality,“ *Critical Social Policy*, 23: 227-248.

einen jedoch als reine „Effizienz“ erscheint, heißt für den anderen „Kontrolle der Gesellschaft“. Dies gilt vor allem für besonders personenbezogene Systeme wie den Abruf von ID-Daten, die konstante und einzigartige Identifikationsmerkmale individueller Bürger beinhalten.⁴⁵

Die gemeinsame Nutzung von Netzwerkinformationen (Information Sharing): Die gesellschaftliche Kategorisierung (Social Sorting) benötigt genaue und leicht abrufbare Informationen. In vielen Ländern, darunter auch Großbritannien, geht der Trend daher in Richtung eines integrierteren öffentlichen Dienstes mit Informationsaustausch, häufig im Rahmen von Partnerschaften oder Teamarbeit über mehrere Ämter hinweg. Eine Vielzahl lokaler Partnerschaften sorgt also zunehmend für die Zusammenführung verschiedener Ämter und Metiers, deren Wissenspool dem Bürger einen umfassenderen Service liefert.⁴⁶ Eine Nebenwirkung dieser wichtigen Entwicklung ist allerdings, dass Grenzen, die einst eine, wenn auch schwache, so doch relativ gute Absicherung des Datenschutzes und Einschränkung der Überwachung boten, nun in Frage gestellt werden. Sowohl die Öffentlichkeit als auch die Dienstleister selbst sind sich nicht darüber im Klaren, wie persönlich Personendaten nun eigentlich sind oder gemanagt werden sollen.⁴⁷ Dies gilt für den öffentlichen Dienst, die Strafverfolgung, Grenzkontrollen und Marketing. So haben z.B. mehr als 50% der britischen Bevölkerung eine Nectar-Kundenkarte des Unternehmens Loyalty Management UK. 216 Versandhäuser in Großbritannien gehören zum Data-Sharing-Konsortium, über das ein gemeinsamer Zugriff auf die Datensätze von 26 Millionen Verbrauchern im Rahmen des Claritas Lifestyle Universe möglich ist. Dazu gehören Einkommen, Lebensstil und Daten zur aktuellen Lebenssituation eines jeden Verbrauchers.⁴⁸

Verwischte Grenzen zwischen öffentlichen/privaten Bereichen: Mehr und mehr staatliche Aktivitäten werden über eine komplexe Verbindung von öffentlichen, privaten und freiwilligen und marktorientierten Mechanismen abgewickelt und führen damit zum Informationsaustausch zwischen dem öffentlichen und dem privaten Sektor. Dies wiederum lässt die Grenzen zwischen öffentlichem und privatem Interesse verwischen. Eine Vielzahl lokaler Partnerschaften sorgt also zunehmend für die Zusammenführung verschiedener Ämter und Metiers, deren Wissenspool dem Bürger einen umfassenderen Service liefert.⁴⁹ Werden für den öffentlichen Dienst gesammelte Informationen jedoch auch der Privatwirtschaft zur Verfügung gestellt, wie dies bereits für die britische Zentraldatenbank (National Identity Register – NIR) vorgeschlagen wurde, müssen die Grenzen der persönlichen Einverständniserklärung von Bürger und Verbraucher unbedingt ausgelotet und festgelegt werden. Auch die Privatisierung der Telekommunikation, der Grenzkontrollen (Projekt „Semaphore“ von IBM, das britische e-Borders-Programm) und der öffentlichen Sicherheit an individuellen Standorten (z.B. das „Citizen Corps“ in den USA, das „ungewöhnliche Aktivitäten“ überwacht) muss hinterfragt werden.

⁴⁵ Kritische Ansichten eines Computerwissenschaftlers finden sich in: Clarke, R. (2006) „National identity cards? Bust the myth of 'security über alles'!“, <http://www.anu.edu.au/people/Roger.Clarke/DV/NatID-BC-0602.html>

⁴⁶ 6, P., Raab, C. und Bellamy, C. (2005) „Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part I“. *Public Administration* 83 (1): 111-133; Bellamy, C., 6, P. und Raab, C. (2005) „Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part II“. *Public Administration* 83 (2): 393-415.

⁴⁷ Ein Beratungsdokument des britischen Innenministeriums, das um eine Machtausweitung im Kampf gegen organisierte und finanzielle Kriminalität ersucht, beschwert sich über „den äußerst lückenhaften Datenaustausch mit anderen Bereichen des öffentlichen Sektors, während ein Austausch über die öffentlich-privaten Gräben hinweg selten auch nur versucht wird.“ Es verlangt eine Verbesserung dieser Informationsflüsse, darunter auch – mit Blick auf die Berichte über verdächtige Aktivitäten (Suspicious Activity Reports – SAR) – den Datenabgleich zwischen der neuen Strafverfolgungsbehörde zur Bekämpfung der organisierten Kriminalität (Serious Organised Crime Agency – SOCA) und den Datenbanken der verschiedensten Regierungsbehörden (z.B. das britische Finanzamt, die britische Kfz-Zulassungsbehörde, das britische Ministerium für Arbeit und Renten und die Meldebehörde). Inzwischen gibt es neue Initiativen, darunter auch der Ministerialausschuss zum Data Sharing (MISC 31), dessen Aufgabenstellung die „Entwicklung einer Regierungsstrategie zum Datenaustausch im öffentlichen Sektor“ umfasst.

⁴⁸ Evans, M. (2005) „The data-informed marketing model and its social responsibility.“ in Lacey, S. (2005) *op cit.*, n.3.

⁴⁹ 6 *et al.* 2005 *op cit.* n.24; Bellamy *et al.*, 2005 *op cit.* n.46.

Gesellschaftliche Konsequenzen der Überwachung

Im Folgenden befassen wir uns eingehender mit den gesellschaftlichen Konsequenzen der Überwachungstechnologien und -verfahren, die wir im Vorfeld untersucht haben. Die Kritik an der Überwachung bezieht sich in erster Linie auf die Privatsphäre und damit zweifellos auf einen wichtigen Bereich, den wir jedoch lieber als einen Aspekt der individuellen Willensfreiheit untersuchen möchten. Außerdem möchten wir die sehr viel seltener diskutierten Auswirkungen auf die Wahlfreiheit und das Einverständnis der Bürger in den Vordergrund stellen, ebenso – und dies ist besonders wichtig – die Auswirkungen der Sortierungs-, Kategorisierungs- und gezielten Werbemaßnahmen auf die Lebenschancen jedes Einzelnen bzw. ganzer Gruppen oder Gemeinschaften, auf ihre relative Mobilität und Chancengleichheit.

Willensfreiheit: Anonymität und Privatsphäre: Die Überwachung wirkt sich auf die Willensfreiheit eines Menschen und damit auf seine Anonymität und Privatsphäre aus. Generelle Anonymität erlaubt einer Person, ihre Identität über Handlungen und Beziehungen zu definieren. Im Rahmen einer allgegenwärtigen Überwachung (und dies gilt vor allem für ID-Systeme) fällt diese Anonymität, die es dem Menschen normalerweise erlaubt, der intensiven Überwachung kleinerer Gemeinschaften zu entgehen, als erstes weg. Die Privatsphäre ungeschützter Menschen oder Randgruppen verringert sich ständig. Die Insassen britischer Gefängnisse unterliegen einer nahezu konstanten Überwachung. Selbst nach ihrer Entlassung erhalten sie immer häufiger elektronische Fußfesseln, sei es als Bedingung ihrer vorzeitigen Entlassung im Rahmen einer Hausarrestüberwachung per Fußfessel (Home Detention Curfew – HDC)⁵⁰ oder im Rahmen einer bedingten Haftentlassung.⁵¹ Auch die Mittel und Wege, mit denen Arbeitgeber das Privatleben ihrer Belegschaft auskundschaften können, müssen ständig eingehend geprüft werden. Die Reichweite mehrerer Datenbanken innerhalb der britischen Zentraldatenbank (National Identification System – NIS) gibt, vor allem wenn sie sowohl den öffentlichen als auch den privaten Sektor überspannt, weiteren Anlass zu großer Besorgnis. Ende 2002 berichtete die BBC z.B., dass die Strafjustiz mehr als 400.000 Verkehrsdatenabfragen an mobile Netzbetreiber gerichtet hatte.⁵² In ihrer Untersuchung eines neuen Überwachungsnetzes sprach die US-amerikanische Bürgerrechtsorganisation ACLU (American Civil Liberties Union) daher von Unternehmen und Bürgern, die „zum Aufbau einer Überwachungsgesellschaft zwangsverpflichtet“ würden.⁵³

Wahlfreiheit und Einverständnis: In der nordamerikanischen Debatte um Überwachung und Datenschutz spielt die Wahlfreiheit eine große Rolle. Im Vergleich zu anderen Schutzmaßnahmen steht sie in Großbritannien jedoch auf keinen Fall an erster Stelle. Kann man sich aussuchen, ob man überwacht wird oder nicht, wenn man gleichzeitig ein normales Leben führen möchte? Lässt sich das Argument überhaupt noch halten, dass wir der Überwachung ja zugestimmt hätten? Die Frage der Wahlfreiheit stellt sich z.B. in der Strafjustiz. Kein Brite, der sich an öffentlichen Plätzen aufhält, hat sich für eine Videoüberwachung (CCTV) entschieden. Kein britischer Fahrzeughalter hat die automatische Aufzeichnung seiner Fahrzeugbewegungen über sein Kennzeichen durch den Verband leitender Polizeibeamter (Association of Chief Police Officers – ACPO) beantragt. Verhaftete geben ihre Fingerabdrücke und DNA-Abstriche nicht freiwillig und werden in der Tat dazu genötigt. Diese Daten werden dann für immer in die zentrale Datenbank der Polizei eingespeist, auch wenn sich der Inhaftierungsvorwurf nicht halten lässt. Und obwohl eine Person im Rahmen eines Drogentests nicht zu einer Urinprobe gezwungen werden darf, kann

⁵⁰ Das HDC-Programm erlaubt Verurteilten mit einer Gefängnisstrafe von drei Monaten bis maximal vier Jahren die frühzeitige Entlassung für einen Zeitraum zwischen zwei Wochen und 4½ Monaten. Voraussetzung ist jedoch eine Ausgangssperre, die über elektronische Fußfesseln kontrolliert wird. Im Zeitraum 2004/5 wurden 19.096 Personen im Rahmen dieses Programms frühzeitig entlassen. Siehe: NPS (2006) *op cit.* n. 82.

⁵¹ *ibid.*

⁵² „Phone firms ‘flooded’ by crime checks“. *BBC News*, 20. Dezember 2002, <http://news.bbc.co.uk/1/low/uk/2592707.stm>

⁵³ Stanley, J. (2004) *The Surveillance-Industrial Complex*, Washington DC: ACLU.

http://www.aclu.org/FilesPDFs/surveillance_report.pdf

man hier wohl kaum von Wahlfreiheit sprechen, wenn sich aus der Ablehnung eine Geldstrafe, Inhaftierung oder sogar beides ergeben kann. Für eine Einzelperson ist es nahezu unmöglich, die Nutzung dieser Informationen und die – subtilen – Auswirkungen auf ihr Leben zu prüfen, z.B. wenn ihr Fahrzeug häufiger von der Polizei angehalten wird oder sie Waren und Dienstleistungen im Voraus bezahlen muss.

Eine Antwort wäre der freiwillige (nicht-obligatorische) Dialog zwischen der staatlichen Überwachung und dem Bürger, wie er in Großbritannien in Sachen ID-Ausweise vorgeschlagen wurde. Dies ist jedoch größtenteils illusorisch: Zum einen wird ein ID-Ausweis *de facto* obligatorisch, wenn nur so eine Reihe unterschiedlicher Dienstleistungen genutzt werden kann, zum anderen gibt das ID-System der Regierung die Macht, Menschen nicht nur hinsichtlich ihrer Bürgerpflichten zu überwachen, sondern auch im Hinblick auf andere Rollen (Autofahrer, Verbraucher, Tourist).

Diskriminierung: Geschwindigkeit, Zugriff und gesellschaftliche Ausgrenzung:

Diskriminierung in Form unterschiedlicher Bearbeitungsgeschwindigkeiten, Zugriffsmöglichkeiten und verschiedener Arten der gesellschaftlichen Ausgrenzung ist eine der Hauptfolgen der gesellschaftlichen Kategorisierung, die sich im Rahmen der Überwachung entfaltet. Hier hat sich die staatliche Logik einem Wandel unterzogen. Während das bürgerrechtliche Verständnis des 20. Jahrhunderts die *Einbeziehung* aller Berechtigten in die Gesundheits-, Sozial- und Rechtsfürsorge vorsah, scheinen sich jüngere Bürgerrechtspraktiken, darunter auch die ID-Systeme, vor allem mit der *Ausgrenzung* unerwünschter Elemente⁵⁴ zu befassen. Menschen, denen Ressourcen zur Verfügung stehen (internationale Geschäftsleute, Touristen usw.), sind sehr mobil, was normalerweise durch Identifikationssysteme (von Kreditkarten bis zu Vielfliegerkarten) erleichtert wird. Andere jedoch, also Arbeiter (oder noch schlimmer, Arbeitslose), Einwanderer, Flüchtlinge oder Asylbewerber, ganz zu schweigen von Personen mit eindeutig „muslimischen“ oder „arabischen“ Namen, werden von diesen Systemen eher daran gehindert, sich im Land oder zwischen verschiedenen Ländern zu bewegen.

Die intensivere Überwachung des städtischen Lebens führt außerdem zu einer enormen gesellschaftlicher Ausgrenzung. Personen und Orte, die auf die eine oder andere Weise als unrentabel oder risikoreich eingestuft werden, werden einfach ausgegrenzt. Die neuen Überwachungstechnologien können das Leben eines Menschen daher auch deutlich *verlangsamen*, indem seine logistischen Anstrengungen schwieriger, nicht leichter, gemacht werden. Im Anschluss an ihre Einführung werden diese Zugriffs- bzw. Blockiermaßnahmen dann verstärkt automatisch geprüft⁵⁵ und führen damit zu einer technologischen Bindung (Lock-in), die die moderne Gesellschaft noch intensiver in schnell reagierende, hochmobile und eingebundene bzw. langsam reagierende, kaum mobile und ausgegrenzte Klassen einteilt. Diese Ausgrenzung findet sich auch in den Preisstrukturen für Waren. Die DVD-Preise von *Amazon.com* werden längst je nach Kunde verschieden gestaltet. Es stellt sich hier allerdings die Frage, ob der Staat eine so groß angelegte, kommerzielle Preisfestlegung nicht unterbinden sollte. Und während sich aus der Überwachung am Arbeitsplatz und der gesellschaftlichen Ausgrenzung aufgrund bestehender Berufs- und Gesellschaftsfaktoren im Arbeitsmarkt nur schwerlich Schlüsse ziehen lassen, gibt es doch einen Bereich, in dem die Jobchancen definitiv ungleich verteilt sind: e-Recruitment. Aus den damit verbundenen Lebenslaufstapeln und der Suche nach potenziellen Kandidaten ergeben sich nämlich zwei Fragen zur Diskriminierung. Erstens unterliegt dieses e-Recruitment Vorurteilen und einfachen „Faustregeln“, die sich schon in der Schlagwortsuche manifestieren^{56 57}, und

⁵⁴ Bigo, D. (2004) „Globalized in-security: the field of the professionals of unease management and the ban-opticon.“ *Traces*, 4.

⁵⁵ Lianos, M. (2001) *op cit.* n.109; Lianos, M. (2003) „Social control after Foucault“ *Surveillance & Society* 1(3): 412-430.
[http://www.surveillance-and-society.org/articles1\(3\)/AfterFoucault.pdf](http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf)

⁵⁶ Tversky, A. und Kahneman, D. (1974) „Judgement under uncertainty: heuristics and biases“ *Science* 185(4157): 1124-1131.

⁵⁷ Mohamed, A. A., Orife, J. und Wibowo, K. (2002) „The legality of key word search as a personnel selection tool“ *Employee Relations* 24(5).

zweitens haben bestimmte gesellschaftliche, wirtschaftliche und ethnische Gruppen kaum die Möglichkeit, aufs Internet zuzugreifen.

Dies kann sich tief in die Infrastruktur einer Gesellschaft eingraben. In einer Zeit, in der das menschliche Urteilsvermögen einem sich stets wandelnden Kodex unterworfen ist und die kulturelle und nationale Identität eine besonders umkämpfte Dimension des Lebens voller Lebenschancen und Wahlmöglichkeiten, Erinnerungen und Hoffnungen darstellt, ist es ironisch, dass gleichzeitig Anstrengungen unternommen werden, dieses Leben zur Erleichterung bürokratischer, polizeilicher und unternehmerischer Verwaltung auf maschinenlesbare Formeln und Algorithmen zu reduzieren.

Demokratie, Verantwortlichkeit und Transparenz: Hier stellen sich viele Fragen. Wo liegen die Grenzen der öffentlichen Überwachung? Wie werden die Grenzen zwischen kommerziell orientierten Datenbanken und der öffentlichen bzw. staatlichen Sicherheit kontrolliert? Wie lassen sich Privatunternehmen für Irrtümer und falsche Angaben in ihren Datenbanken zur Verantwortung ziehen? Derzeit ist es dem betroffenen Bürger z.B. nur bedingt möglich, die Überwachungslisten „intelligenter Grenzen“ einzusehen. Während viele Stellen und Behörden auf das System zugreifen oder dort Daten einspeisen können, gibt es kaum Möglichkeiten, diese Daten zu löschen oder zu korrigieren. Und schließlich muss auch die Verantwortlichkeit gewählter Regierungen gegenüber den Bürgern sowie die undurchsichtige „Offshore-Struktur“ vieler Privatdienstleister im modernen Überwachungssystem deutlich hinterfragt werden. Tatsächlich dürfen kommerzielle Datenbanken internationaler Großkonzerne (z.B. für Kreditkartentransaktionen oder Aufzeichnungen von Handy-Telefonaten) „offshore“ und damit außerhalb einer direkten politischen Gerichtsbarkeit liegen. Jüngste Beispiele, die sich auf die Informationserfassung von internationalen Großkonzernen beziehen, stellen die öffentliche Überprüfung und Beaufsichtigung vor ganz spezielle Herausforderungen. Dies gilt vor allem dann, wenn ein Unternehmen über kommerzielle Daten verfügt und *gleichzeitig* vertraglich vereinbarte Überwachungsfunktionen durchführt.

In vielen Ländern gibt das Gesetz dem Bürger das Recht, in Erfahrung zu bringen, welche Informationen über ihn gespeichert und wie diese genutzt werden. Es gibt allerdings auch Ausnahmen. Im Rahmen dieses Rechts muss ein „Datenkontrolleur“ jeder Einzelperson Informationen über alle über sie gespeicherten Daten und deren Verwendung zukommen lassen. Im Machtgefüge der Überwachung stellen diese Maßnahmen das Gleichgewicht fast wieder her – vor allem dann, wenn unser Einverständnis zur Nutzung dieser Personendaten eher stillschweigend denn ausdrücklich vorliegt. Viele Menschen kennen ihre Rechte jedoch nicht, machen davon keinen Gebrauch und erhalten dabei auch kaum Hilfe von Dritten.

Die intensive Datenüberwachung (Dataveillance) entwickelt sich verstärkt zu einem normalen Kennzeichen des modernen Staats und ist – für sich allein gestellt – im öffentlichen Interesse sicherlich vertretbar. Häufig wird sie von der Regierung ausdrücklich gutgeheißen. Problematisch wird sie jedoch durch die Manipulation von Personendaten, die weit über die von Datenschutzrichtlinien und -gesetzen (hier kommt wieder die Regierung ins Spiel) sowie anderen Einschränkungen bzw. Richtlinien zur Erfassung, Zusammenstellung und Weitergabe von Informationen gestellten Grenzen hinausgeht. Vielleicht gewöhnen wir uns an die Überwachung und daran, dass all unsere Aktivitäten und Bewegungen verfolgt oder sogar vorhergesehen werden, ohne dass wir es wirklich merken und – vor allem im öffentlichen Dienst – ohne uns dafür oder dagegen entscheiden zu können oder die Nutzung unserer Daten wirklich vollends zu verstehen. Vielleicht entsinnen wir uns unserer Bürgerpflicht und akzeptieren damit Einschränkungen unseres Privatlebens, die wir normalerweise abgelehnt hätten. Es ist keineswegs sicher, ob sich die Datenschutzrechte der Bürger angesichts der politischen Lage letzten Endes auch dann gegen die im „öffentlichen Interesse“ vertretenen Standpunkte der Regierungen durchsetzen können, wenn dieses öffentliche Interesse offensichtlich und von vorrangiger Bedeutung erscheint. Wenn eine Überwachung „angemessen“ sein soll, dann hängt viel von der Auslegung dieses Begriffs und der

auslegenden Partei ab, ebenso wie von den Schutzvorrichtungen gegen diese neuen, einschneidenden Entwicklungen.

3. Die Kontrolle der Überwachungsgesellschaft

Überwachung braucht Aufsicht, wobei wir mit „Aufsicht“ nicht nur Rechtsmittel zur Kontrolle der Systeme und Verfahren meinen, sondern alle Methoden, die kontrollierende Auswirkungen haben⁵⁸, die also Richtlinien in Form von Grenzwerten und Kontrollen für die Überwachung und Datenverarbeitung bieten. Die meisten Systeme zur Kontrolle der Verarbeitung von Personendaten wurden im Zusammenhang mit dem Datenschutz, also mit dem Ziel der Sicherung der Privatsphäre, entwickelt. Unsere Ausführungen in diesem Abschnitt beziehen sich hauptsächlich auf diese Strategien. Die Kontrolle der *Überwachung* ist dagegen ein ganz anderes Thema. Hier ließe sich sicher vertreten, dass der Schutz vor Überwachung ein eigenständiges Feld ist, da die unerwünschten Auswirkungen nicht ausschließlich mit einem Eingriff in die Privatsphäre zusammenhängen und diese erste Verteidigungslinie zwar nicht vernachlässigt werden darf, aber dennoch recht anfällig ist. In diesem Berichtsabschnitt gehen wir auf die Erfahrungen in Sachen Aufsicht ein und bewerten die Angemessenheit der entsprechenden Maßnahmen. Darüber hinaus werden wir Verbesserungsvorschläge vorstellen.

Was ist so falsch an dieser Kontrolle?

Die Kontrolle des Datenschutzes und der Überwachung leidet unter einigen allgemeinen Mankos. Dabei lassen sich mindestens sechs Problembereiche identifizieren:

- Bisher gestaltete sich diese Kontrolle eher reaktiv – als Antwort auf bereits eingeführte technologische Entwicklungen, Implementierungen und Praktiken.
- Die Kontrolle konzentrierte sich hauptsächlich auf technische und verwaltungstechnische Punkte auf der Basis von Verhaltenskodexen, der Einhaltung allgemeiner Rechtsansprüche und des Einsatzes von Datenschutztechnologie – ohne jedoch vorausschauende Aspekte zu berücksichtigen.
- Ein Großteil der Kontrollbestimmungen bezieht sich lediglich auf den persönlichen Datenschutz und seinen Wert für jede Einzelperson. Sie reflektieren damit (notwendigerweise) die aktuelle Denkweise der politischen Entscheidungsträger, die das „öffentliche Interesse“ oft nur aus einem eingeschränkten Blickwinkel sehen.
- Kontrolle wurde bisher größtenteils nichtöffentlich diskutiert und implementiert. Die Debatte fand nur in Fachkreisen statt, so z.B. im Bereich des Datenschutzes oder der Strafjustiz. Mit einigen der wichtigsten Themen unserer Zeit hat sich der normale Bürger also kaum befasst.
- Unter politischen Gesichtspunkten wird Kontrolle häufig als unfaire Belastung der Wirtschaft und des Staates gesehen, die Initiative, Risikofreude und Produktivität drosselt. Um diese Belastung zu senken, gab es in Großbritannien einen deutlichen Rutsch in Richtung Deregulierung oder „besserer Kontrolle“. Daher wird in der Praxis nur selten (in der Theorie schon eher) anerkannt, dass sowohl die Wirtschaft als auch die Regierung vom öffentlichen Vertrauen sowie dem Nutzeffekt ausgereifter Kontrollverfahren profitieren könnten.
- In den Medien konzentriert sich diese Debatte vor allem auf „Horrorgeschichten“ über Datenschutzverletzungen oder utopische und Orwellsche Visionen der Überwachung. Zwar sind Berichte über entsprechende Vorfälle wichtig, doch

⁵⁸ Baldwin, R. und Cave, M. (1999) *Understanding Regulation: Theory, Strategy and Practice*. Oxford: Oxford University Press.

allzu häufig werden die komplexen ethischen und gesellschaftlichen Fragen zur Überwachung in diesem Zusammenhang nicht gestellt. Die Überwachungsdiskussion dreht sich meist um simple Ursache- und Wirkungsketten („CCTV verhindert kriminelle Handlungen“) oder schürt Ängste („Wir werden alle kontrolliert“). Gleichzeitig werden abweichende Meinungen mit dem ebenso trügerischen wie gefährlichen Argument „Wer nichts zu verbergen hat, braucht auch nichts zu fürchten“ mundtot gemacht.

Kontrolle – der aktuelle Stand

Seit ca. 35 Jahren geht der Datenschutz um die Welt. Kern dieser Entwicklung sind einige fest verankerte Grundsätze, die Folgendes von einer Organisation verlangen:

- Sie zeichnet für alle Informationen in ihrem Besitz *verantwortlich*.
- Sie muss den *Zweck* der Datenverarbeitung bei oder noch vor der Datenerfassung *identifizieren*.
- Sie darf Personendaten nur *mit Wissen und Einverständnis* einer Einzelperson erfassen (Ausnahme: besondere Umstände).
- Sie muss die *Erfassung* der Personendaten auf das für die Verfolgung der identifizierten Zwecke erforderliche Maß *beschränken*.
- Sie darf Personendaten ausschließlich mit dem Einverständnis einer Einzelperson nutzen oder weitergeben (Grundsatz der *Endgültigkeit*).
- Sie darf Informationen nur solange *aufbewahren* wie nötig.
- Sie muss sicherstellen, dass die Personendaten jederzeit *korrekt, komplett und aktuell* sind.
- Sie muss Personendaten durch entsprechende *Sicherheitsmaßnahmen* schützen.
- Sie muss hinsichtlich ihrer Methoden und Verfahren *Transparenz* an den Tag legen und darf keine geheimen Informationssysteme unterhalten.
- Sie muss den Betroffenen den *Zugriff* auf ihre Daten sowie im Falle von falschen, unvollständigen oder veralteten Daten eine entsprechende Aktualisierung ermöglichen.⁵⁹

Inspiziert von diesen oder ähnlichen Prinzipien für die faire Datenerhebung haben die Aufsichtsorgane auf internationaler und regionaler Ebene allgemeine Gesetze, Gesetze für bestimmte Sektoren (z.B. Telekommunikation) oder Verfahren (z.B. Data Matching) und internationale Dokumente und Erklärungen entworfen, mit denen Eingriffe in die Privatsphäre und Überwachung kontrolliert werden sollen. Am bekanntesten ist wohl die Europäische Datenschutzrichtlinie 95/46/EG, aber auch Richtlinie 2002/58/EG über Datenschutz und Kommunikation reflektiert dieses Thema. Aufsichtsbehörden und Datenschutzkommissionen wurden auf nationaler, sub-nationaler und sogar auf regionaler Ebene gegründet. Außerdem haben Privatunternehmen, Handelsverbände und Behörden eigene Verhaltenskodexe und Protokolle eingeführt, Online-Händler bieten Datenschutzerklärungen und Richtlinien an. Bei Zuwiderhandlung drohen im Rahmen der einschlägigen Gesetze Strafen oder Sanktionen. In jüngster Zeit helfen auch moderne Datenschutztechnologien (Privacy-enhancing Technologies – PETs), die Datenerfassung einzuschränken, die Anonymität zu wahren oder das Überwachungspotenzial der Technologie selbst zu entschärfen. Die Verfechter des Datenschutzes haben laut und aktiv vor den Gefahren gewarnt, fragwürdige Praktiken aufgedeckt und das öffentliche Bewusstsein für den Einfluss der Überwachung und der Datenschutzübergriffe auf das Privatleben gestärkt. Auch die Medien haben sich häufig zu den Gefahren einer Überwachung geäußert, obwohl sie von Übergriffen auf das Privatleben von Stars oder „normalen“ Bürgern profitieren.

⁵⁹ Bennett, C. und Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge MA: MIT Press, 12.

Viele sind der Ansicht, dass ein praktisches System zur Kontrolle der Überwachung nicht auf dem schwachen Fundament des Datenschutzes basieren sollte. Andere wiederum⁶⁰ gehen davon aus, dass der Datenschutz auch andere, direkte, Übergriffe abdecken kann, bei denen zwischen der Einzelperson und dem Überwacher ein Ungleichgewicht entsteht – z.B. bei der Videoüberwachung. Die neuen Überwachungsmethoden zeichnen sich jedoch zunehmend durch Diskriminierung und andere gesellschaftliche „Negativa“ aus, die große und ungerechte Auswirkungen auf Lebenschancen haben, deutlich über einen Eingriff in die Privatsphäre hinausgehen und hauptsächlich Einzelpersonen betreffen. Daher sollte erörtert werden, ob die Kontrollmaßnahmen für Überwachung und Datenschutz nicht neu überdacht oder zumindest überarbeitet werden müssen, um Entwicklung, Einführung und Effekt neuer, intensiverer und umfangreicherer Überwachungstechnologien beeinflussen zu können. Die moderne Überwachung besteht aber nicht nur aus Technologie. So kann man mit Fug und Recht behaupten, dass Kontrollsysteme nicht nur mit dem Problem umgehen müssen, wie man diesen Technologien gerecht wird, sondern auch, wie man die Verfahren und Ziele der Entwickler und Anwender, aber auch die Gesellschaften und Bevölkerungsgruppen, die ihr ausgesetzt sind, beeinflussen kann.

Kontrollinstrumente: Vor- und Nachteile

Die folgenden politischen Werkzeuge, die zum Schutz von Privatsphäre und Personendaten eingeführt wurden und sich daher auf weite Bereiche der Überwachung beziehen⁶¹, gibt es bereits:

Internationale Werkzeuge: Die europäische Menschenrechtskonvention und andere internationale Deklarationen geben dem Schutz der Privatsphäre rechtliche und moralische Macht, die auch bei der Eindämmung von Überwachungsexzessen eine wichtige Rolle spielen kann. Diese und damit verbundene Dokumente haben in vielen Ländern und Gerichtsbarkeiten eine entsprechende Gesetzgebung und Implementierung beeinflusst. Diese internationalen Maßnahmen zeichnen größtenteils verantwortlich für die wichtigsten Grundsätze, die den Datenschutz – und im weiteren Sinne auch die Überwachung – seit langer Zeit bestimmen.

Gesetze: Die globale Ausweitung von Gesetzen zur Kontrolle von Personendaten und ihrer Verwendung hat sich seit den 70er Jahren deutlich beschleunigt. Viele Länder haben sektorspezifische und allgemeingültige Datenschutzgesetze erlassen, wobei das Gros dieser Gesetze jeweils eine spezielle Form der Aufsicht oder Exekutive nach sich zog. Die Aufsicht in Form von Datenschutzbeauftragten ist eine Grundlage der Sicherung der Privatsphäre. Dass die USA auch weiterhin kein Mitglied dieses „Clubs“ aller Länder mit einer umfassenden Gesetzgebung sind und nur bruchstück- und lückenhafte Lösungsansätze zeigen, schwächt die weltweiten Anstrengungen zur Überwachungskontrolle deutlich. Die Schwachstellen vieler Gesetze und ihrer Durchsetzung im Bereich der Personendatenverarbeitung sind schon seit langem Anlass für Beschwerden. Angesichts gesetzlicher Lösungen, die eine Überwachung eher gutheißen als sie zu kontrollieren⁶², zeigen sich Kritiker mit Recht ungehalten. Darüber hinaus haben es Gesetze zum Schutz unserer Daten und Privatsphäre nicht leicht, eine breit gefächerte Palette von Überwachungsmethoden zu kontrollieren (so z.B. Verfahren im Rahmen der modernen Telekommunikation), und lassen sich auch nur schwer dahingehend auslegen. Zudem fallen die Gefahren einer Überwachung für Einzelpersonen, Gruppen und ganze Gesellschaften nicht unter die von entsprechenden Gesetzen abgedeckten Auswirkungen.

⁶⁰ Z.B.: Dubbeld, L. (2004) *The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance*. Enschede: Ipskamp Printpartners.

⁶¹ Eine detaillierte Typologie und Debatte findet sich in *op cit.* n. 59: Kap. 4-7.

⁶² Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill NC: University of North Carolina Press.

Selbstkontrolle: Sektoren und Unternehmen, Fachorgane und Staaten haben die unterschiedlichsten Verhaltenskodexe und -praktiken entwickelt, um die Überwachung in vielen Bereichen zu kontrollieren. Außerdem existieren Online-Werkzeuge zur Selbstkontrolle, die von Internet-Händlern in Form von Datenschutzrichtlinien entworfen und von anderen Organisationen verbürgt werden. Zum Teil ist diese Selbstkontrolle auch im Gesetz verankert, ebenso wie Verhaltenskodexe im britischen Datenschutzgesetz von 1998 sowie der EU-Datenschutzrichtlinie 95/46/EG von 1995. Mit Blick auf das „Versagen“ der Gesetzgebung und dem weniger kontrollierten Wirtschaftsklima, das als erstrebenswert angesehen wird⁶³, gilt die Selbstkontrolle zunehmend als bessere Option. Dennoch sind derartige Kodexe und andere Vorschriften ohne eine vorherige und zeitgleiche Gesetzgebung bzw. internationale Instrumente, also die Quellen genau der Normen und Richtlinien in diesen Kodexen, kaum vorstellbar.

Datenschutztechnologien (Privacy-enhancing Technologies – PETs): Seit Beginn der 90er Jahre gibt es die Erkenntnis, dass auch Technologien selbst leistungsstarke Kontrollen für Überwachung und Schutz der Privatsphäre bieten können. Das Überwachungs- bzw. Nichtüberwachungspotenzial bestimmter Technologien hängt also stark von ihrer Konzeption und ihrem Einsatzbereich ab. So kann eine Verschlüsselung von gespeicherten bzw. über Domains oder andere Grenzen fließenden Personendaten entweder ganz fehlen oder sehr ausgeprägt sein. Netzwerkdesign und Softwarekodierung können daher durchaus eine Kontrollwirkung haben.⁶⁴ Verschlüsselung, anonymes Web-browsing, Filter, Smart Agents, P3P und ähnliche Tools unterstützen jeden Einzelnen. Dabei bleibt jedoch unklar, ob diese Tools allein wirklich leistungsstarke Lösungen für die Online-Überwachung sind.

Individuelle Selbsthilfe: Dies ist eine weitere breit gefasste Kontrollkategorie, bei der jeder Einzelne die Offenlegung privater Informationen selbst in der Hand hat – entweder über PETs oder über den Einstieg in oder Ausstieg aus bestimmten Datenverarbeitungsverfahren, aber auch im Rahmen seines eigenen Wissens, Bewusstseins und seiner Wachsamkeit hinsichtlich Überwachungsmethoden und Gefahren für den Datenschutz. Allen Methoden ist jedoch gemein, dass sie nur von jemandem mit ausreichendem Interesse am Datenschutz und dem entsprechenden „kulturellen Kapital“ eingesetzt werden können, d.h. jemand mit der Fähigkeit und den Mitteln, die Vorgänge zu verstehen, sich gegen Fortschritte durchzusetzen oder sich gegen bereits erfolgte Übergriffe zu wehren. Da es in den USA keine Kontroll- oder Aufsichtsbehörden gibt, ist Selbsthilfe, u.a. auch über die Gerichte, das wichtigste Mittel des Datenschutzes – die Kritik an diesem Modell ist daher auch unüberhörbar. Andere Datenschutzsysteme verlassen sich zum Teil auf Einzelpersonen, die den Aufsichtsbehörden Beschwerden vorlegen und im Falle dubioser Praktiken als wichtigste Informanten dienen.

Darüber hinaus halten wir auch die Aktivitäten der folgenden Gruppen für bedeutend:

- Interessensgruppen für Datenschutz und gegen Überwachung, die – zusammen mit bestimmten Medien – das öffentliche Bewusstsein für Probleme und Gefahren stärken, Situationen überprüfen und Druck auf die Regierungen und Unternehmen ausüben, die Überwachung einsetzen.
- Technologen, die Überwachungs- und Informationssysteme konzipieren, und deren Aus- und Weiterbildung sowie Einhaltung der Verhaltenskodexe Einfluss auf das Bewusstsein ihrer Mitarbeiter sowie auf die Form des Produkts nehmen.
- Akademiker, deren Arbeiten Geschehnisse an die Öffentlichkeit bringen und erklären sowie Theorien zum richtigen und legitimen Einsatz von Überwachung in den Gesellschaften von gestern, heute und morgen entwickeln und testen. Auf diese Weise wird die öffentliche Debatte mit entsprechendem Fachwissen gespeist.

⁶³ US Department of Commerce, National Telecommunications and Information Administration (NTIA) (1997) *Privacy and Self Regulation in the Information Age*. Washington DC: Department of Commerce, NTIA.

⁶⁴ Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York NY: Basic Books.

Allgemeine Probleme bezüglich der Kontrollwerkzeuge

Drei der wichtigsten Probleme im Hinblick auf aufsichtstechnische Praktiken beziehen sich auf *Fragmentierung* und *schlechte Koordination*. Das erste betrifft die wichtigsten *Kontrollwerkzeuge*, das zweite das Chaos gerichtlicher *Instanzen*, die sich angeblich mit dieser Kontrolle befassen. Beide müssen sich der Herausforderung einer potenziell homogeneren und weltweiten Überwachung stellen, die sich mit Blick auf die wohl auch weiterhin beharrlichen Trends für die Kontrolle ergibt. Bei beiden Problemen bleibt die Frage, wie sich die Sachlage verbessern lässt. Kann man Feuer mit Feuer bekämpfen? Wenn die Kräfte zur Expansion der Überwachung zunehmend integriert und „gemeinsam“ agieren, ob nun landesweit oder international, wie gut sind dann Kontrollwerkzeuge und einzelne Schutzmechanismen zu ihrer Kompensierung integriert? Das dritte Problem ist der Einsatz dieser Werkzeuge gegen die gesellschaftlichen Auswirkungen der Überwachung – und hier vielleicht vor allem der „neuen Überwachung“ – über Datenschutzverletzungen hinaus oder die Entwicklung völlig neuer Werkzeuge. Für alle drei Probleme muss die Palette der Kontrollmaßnahmen jedoch auf ihre Kohärenz und Effektivität untersucht werden. Außerdem muss die mögliche Bewertung der Auswirkungen von Datenschutz und Überwachung auf jeder Ebene, in jedem Bereich, jeder Domain und jedem Anwendungsgebiet überdacht werden. Auch diese Punkte können hier nur angeschnitten werden.

Alternativen für eine zukünftige Kontrolle

Bewertung der Auswirkungen von Datenschutz (Privacy Impact Assessment – PIA): Unserer Ansicht nach ergeben sich aus dem PIA-Ansatz bedeutende Vorteile für die Kontrollmethoden der Gerichtsbarkeiten auf jeder relevanten Ebene.⁶⁵ PIA lässt sich am besten als Instrument beschreiben, das Befürworter neuer oder überarbeiteter Datenverarbeitungssysteme zur Minderung potenziell abträglicher Auswirkungen auf die Datengeber einsetzen können. Dabei zeigt die PIA-Bewertung ggf., wie sich der Datenschutz bei einem Datenaustausch nicht als Hindernis, sondern als wichtige ethische und gesetzliche Anforderung erweisen kann, mit der sich bedeutende gesellschaftliche und politische Ziele erreichen lassen, so z.B. bürgerorientierte Dienste oder Sicherheit.

Von der Bewertung der Auswirkungen von Datenschutz zur Bewertung der Auswirkungen von Überwachung (Surveillance Impact Assessment – SIA): Um die potenziell abträglichen Auswirkungen der Überwachung auf eine breitere Basis als den reinen Datenschutz zu stellen, würden wir die Weiterentwicklung der PIA-Bewertung über ihre derzeitige Konfiguration hinaus in Richtung einer sogenannten „*Surveillance Impact Assessment*“ (SIA), also der Bewertung der Überwachung an sich vorschlagen. Dies hätte selbstverständlich eine Bedeutungsveränderung zur Folge, da PIA die Auswirkungen der *Datenverarbeitung auf den Datenschutz* untersucht, SIA jedoch die Auswirkungen der *Überwachung auf die verschiedensten Gesellschaftswerte*, einschließlich des Datenschutzes, aber auch darüber hinaus.

Da PIA als Werkzeug für einen Einblick in den *Datenschutz*, also mit Bezug auf die Rechte des Individuums, entwickelt wurde, eignet sie sich noch nicht unbedingt für die weitreichenderen Konsequenzen der Überwachung, also mit Bezug auf eine Vielzahl weiterer gesellschaftlicher oder persönlicher Auswirkungen. Die Berücksichtigung dieser Aspekte würde einen Paradigmenwechsel voraussetzen, bei dem sich die Bewertung der Auswirkungen auf die *Einzelperson* (wie dies im Datenschutz der Fall ist) in Richtung einer

⁶⁵ Stewart, B. (1999) „Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies“, *Privacy Law & Policy Reporter* 5 (8): 147-149; eine detaillierte Beschreibung von PIA siehe Raab, C., 6. P., Birch, A. und Copping, M. (2004) *Information Sharing for Children at Risk: Impacts on Privacy*. Edinburgh: Scottish Executive.

Bewertung des Datenschutzes und der Nachteile einer Überwachung in *gesellschaftlicher* Hinsicht verschiebt.⁶⁶ Datenschutz ist eben nicht nur ein Wert für das Individuum, sondern auch für die gesamte Gesellschaft, und zwar als Basis für das Allgemeinwohl und gemeinsame Werte wie Demokratie, Vertrauen, Gemeinsinn und eine freie, gleichberechtigte Gesellschaft. Gerade weil der Wert des Datenschutzes über jeden Einzelnen hinausgeht, nehmen wir alle Anteil am Recht (und der Möglichkeit) eines Menschen, seine Privatsphäre zu schützen. Es handelt sich um einen allgemeingültigen Wert, der als gemeinsames Gut nicht aufgeteilt, von dessen Schutz keiner ausgenommen und der vom Markt nicht effizient genug bereitgestellt werden kann.⁶⁷ Deshalb könnte die SIA-Bewertung eine wichtige Rolle spielen, indem sie den Datenschutz mit einbezieht, jedoch auch die Untersuchung der Auswirkungen von Überwachung und Eingriffen in die Privatsphäre auf die Gesellschaft selbst sowie auf andere, nicht den Datenschutz betreffende Interessen von Einzelpersonen, Kategorien und Gruppen umfasst und damit über die PIA-Bewertung hinausgeht.

Mögliche Fragen im Rahmen einer SIA-Bewertung:⁶⁸

- Verursacht diese Vorgehensweise ungerechtfertigte physische oder psychische Schäden?
- Überschreitet diese Vorgehensweise unerlaubt eine persönliche Grenze (entweder durch Nötigung, Irreführung oder eine beziehungsbasierte, körperliche bzw. räumliche Grenze)?
- Missachtet diese Vorgehensweise bestimmte Annahmen zur Handhabung von Personendaten, z.B. dass keine geheimen Aufzeichnungen gemacht werden?

Alternativen: Wenn SIA auf PIA aufbaut, bauen andere Alternativen ebenfalls auf vorhandenen Aspekten auf:

- Aufbau eines technologischen Wissens- und Bewusstseinspools, sodass die Aufsichtsbehörden mit der technischen Entwicklung Schritt halten können.
- Beratung von Managern und Technologen zur verantwortungsbewussten Konzeption von Überwachungstechniken mit besonderem Augenmerk auf Strategien, organisatorische Veränderungen, Mitarbeiterschulungen und die soziale Verantwortung.
- Begriffliches Umdenken: Datenschutz als gesellschaftliches Allgemeinwohl und nicht als Individualwert.
- Die Unterstützung einer öffentlichen Debatte zur Überwachung, die alle einschließt und nicht bevormundend wirkt.
- Unabhängige Einschätzung der Kosten für Datenschutz, Überwachungskontrolle und deren Einhaltung. Sind diese Kosten übertrieben oder verhindern eventuell sogar Innovationen? Werden die Vorteile öffentliches Vertrauen und Wirtschaftlichkeit ausgeglichen – unter Berücksichtigung der Tatsache, dass dieser „Ausgeglichenheitstest“ selbst nicht zulänglich ist und eingehend hinterfragt werden muss.
- Aufklärung in den Medien über Klischees, Sensationsberichte und Panikmache hinaus.

Abschließend muss im Rahmen einer Verbesserung dieser Kontrolle auch darüber nachgedacht werden, inwieweit sich die jeweiligen Beziehungen und Wechselbeziehungen zwischen den einzelnen Aufgaben überhaupt für eine Kontrolle eignen: d.h. die Beziehungen zwischen Kontrollsystemen der unterschiedlichsten Ebenen bis hin zur globalen sowie zwischen den unterschiedlichen Stakeholdern, darunter auch Kontrollbehörden und zivile Interessensgruppen. Weiterhin sollte z.B. erörtert werden, inwieweit die Kooperation, die in der EU-Richtlinie 95/46/EG erwähnt wird, nicht nur der Durchsetzung und Einhaltung, sondern auch der Aufklärung und Bewusstseinsweiterung in punkto

⁶⁶ Regan (1995) *op cit.* n.9, Kap. 8.

⁶⁷ *ibid.*

⁶⁸ Gary T. Marx, „Ethics for a the New Surveillance“, *The Information Society*, 14, 3, 1998: 174.

Überwachungsmethoden und -technologien dient. Des Weiteren: Inwieweit existiert eine gegenseitig vorteilhafte Beziehung zwischen den Kontrollbehörden und zivilen Interessensgruppen, die diese Behörden unterstützen, wenn sie Probleme aufdecken, ihnen nützliche Informationen oder Wissen zukommen lassen und als Bremse fungieren, sofern die Kontrolle ins Wanken gerät oder die Praktiken von Regierung und Wirtschaft die Überwachung auszuweiten scheinen. Ob – zusätzlich zu engagierten Kontrollorganen und ebenso engagierten Überwachungsgegnern – auch im gesamten Kontrollsystem weiterer Innovationsbedarf in Form von unabhängigen Experten besteht, geht über den Umfang dieses Berichts hinaus, wird aber vielleicht ein wenig veranschaulicht.