Erscheint in:

Gaycken, S.; Kurz, C. (Hg.): *1984.exe - Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien*, Bielefeld

Die Spezifik technisierter Überwachung: Überlegungen zu Überwachung und Macht aus technikphilosophischer Sicht

NIELS GOTTSCHALK-MAZOUZ

Einleitung

Wenn man »technisierte Überwachung« hört, dann weiß man ungefähr, was gemeint ist, zumal dann, wenn der Band den Verweis auf George Orwells Roman *1984* bereits im Titel herstellt. Der erste Teil dieses Bandes führt die zu bedenkenden Entwicklungen weiter aus, unter den Stichworten: Mobiltelefon- und Videoüberwachung, Biometrie, Vorratsdatenspeicherung, Datamining, Bundestrojaner. Einerseits scheint also ganz klar, worum es geht. Andererseits aber, so könnte man sagen, war doch jede Überwachung schon immer technisiert: es werden technische Artefakte eingesetzt (Fernglas, Mikrofon usw.) oder zumindest bestimmte Handlungsweisen (der Beschattung, Bespitzelung und Spionage etwa), d.h. bestimmte Techniken. Wenn man sich also allgemein fragen möchte, was das Spezifische gerade *technisierter* Überwachung ist, sollte man neu nachdenken. Dann lässt sich vielleicht auch besser sagen, wohin sich die technisierte Überwachung entwickeln könnte. Beides soll im Folgenden geschehen, und zwar aus technikphilosophischer Perspektive. Die Analyse verwendet dabei Kategorien praktischer Philosophie und fragt: welche Handlungen, welche Handlungstypen sind wie im Spiel? Wie verändern sich Handlungsmöglichkeiten und (möglicherweise) das Selbstverständnis von Handelnden? Damit sind zwar auch An-

satzpunkte für eine ethisch-politische Bewertung geliefert. Aber nicht die Bewertung selbst. Hier kommt es vor allem darauf an, die mit den oben genannten Stichworten verbundenen Phänomene auf eine allgemeine und dennoch treffende Art zu beschreiben.

Technisierung der Überwachungsmittel

Wenn man von der These ausgeht, dass Überwachung schon immer technisiert war, kann man sich weiter fragen, ob Technisierung vielleicht eine Frage des Grades ist. Man würde dann genauer sagen, dass Überwachung schon immer *mehr oder weniger* technisiert war. Dies könnte quantitativ gemeint sein, d.h. dass bessere und bessere Artefakte technische Artefakte oder Methoden eingesetzt werden. Wann ergäbe sich aber etwas qualitativ Neues? Genau dann, wenn qualitativ neue Artefakte oder Methoden zum Einsatz kommen, oder wenn bestehende auf neue Weise kombiniert werden. Technologische »Surveillance Milestones« lassen sich rückblickend bereits im frühen 19. Jh. ausmachen, nämlich mit der Erfindung der Photographie, dann der Telegraphie usw. (ACLU 2007). Diejenigen Techniken, die in unserem Zusammenhang relevant zu sein scheinen, nämlich Informations- und Kommunikationstechniken, ermöglichen vor allem auch die neuartige Kombination, allgemein gesagt die Speicherung und Verarbeitung der Überwachungsergebnisse. Es ist also nicht in erster Linie die Verbesserung der Ferngläser, Kameras, Mikrofone usw. gemeint, sondern dessen, was danach kommt, was also mit audiovisuellen Signalen geschieht, nachdem man sie in (und sei es verbesserter Qualität) erhalten hat.

Die Technisierung der Überwachung verbessert zwar auch unsere »verlängerten Ohren und Augen« (Richtmikrofone und Teleobjektive), bzw. unsere Nasen (wenn man an chemische Detektoren denkt, wie etwa im »Spürpanzer« *Fuchs*), sowie auch den Tast- und den Gleichgewichts-/Orientierungssinn (man denke an GPS). Technik dient insofern der Verlängerung oder dem Ersatz von (Sinnes-) Organen (vgl. Kapp 1877, S. 42, ähnlich auch McLuhan 1964, S. 9ff.), zunehmende Technisierung der Überwachung lässt sich an stetig verbesserten entsprechenden technischen Artefakten (»Sensoren«) festmachen. Qualitativ neue Überwachungsmöglichkeiten entstehen damit dadurch, dass der Abstand immer größer wird, aus dem überwacht werden kann, und dass der Bereich dessen, was erfasst werden kann, durch eine Ausweitung von Frequenzbereichen (z.B. ins Infrarote oder in den elektromagnetischen Bereich) zunimmt, sowie dadurch,

dass die Sensoren nicht mehr von Menschen vor Ort bedient oder auch nur in Position gebracht werden müssen, wodurch sich die Zahl der Überwachungsfälle gesteigert, die Überwachung unauffälliger gestaltet und die Zahl der Mitwisser von Überwachungsaktionen verringert werden kann.

Auch die Überwachungstechniken im Sinne von Handlungsweisen und Strategien lassen eine Technisierung erkennen. So bedienen sich überwachende Personen selbstverständlich Mobiltelefonen und Computer, um sich untereinander zu koordinieren oder um die Sensorik zu steuern. Ortsbestimmung z.B. per GPS verändern Beschattungs- und Verfolgungstechniken. Verbesserte Präparations- und Nachweistechniken ermöglichen eine stetig verbesserte nachträgliche Auswertung von Spuren. Die qualitativ wichtigeren Technisierungen in der Überwachung hat es wohl aber in den nachgelagerten Instanzen gegeben: nicht so sehr in der Präsentation besserer oder üppigerer Daten also, sondern in ihrer technischen Speicherung und Auswertung. Hier nun kommen die Informations- und Kommunikationstechniken wirklich ins Spiel: bereits aus einzelnen Datenströmen lassen sich automatisch Informationen extrahieren, etwa Personen bzw. Sprecher zählen, Worte und Schrift erkennen usw. Durch den Abgleich verschiedener Datenquellen und den Abgleich mit technisierten Wissensspeichern (Datenbanken, WWW) lassen sich diese Informationen weiter aufwerten (Personen erkennen, Autokennzeichen zu Personen zuordnen usw.). Die Technisierung der Speicherung ermöglicht dabei zusätzlich die Erkennung von Mustern über die Zeit (Bewegung von Personen z.B.).

In der Technikphilosophie werden Werkzeug- und Maschinentechnik unterschieden; in unserem Zusammenhang interessiert besonders ihre handlungstheoretische Unterscheidung (vgl. Hubig 1993, S. 53ff.). Während Werkzeuge noch flexibel unterschiedlichen Zwecken zugeordnet und in unterschiedlichen Funktionen verwendet werden können, sind bei Maschinen die Abläufe fest vorgegeben (man denke an die Programme einer Waschmaschine) und es ist nur noch die Frage, welchen Ablauf, welches Handlungsschema, man aktiviert. Mir scheint, dass man die Technisierung der Sensorik im wesentlichen Werkzeugcharakter hat und die Technisierung der Auswertung im wesentlichen Maschinencharakter. Denn bei der Auswertung kommen zentral Algorithmen und Programme ins Spiel, die die Arbeit leisten und durch deren Design vorgeben, was wie erkannt werden kann.

Technisierung der zu überwachenden Handlungen

Zweitens betrifft die Technisierung jedoch nicht nur die Überwachungsmittel, sondern auch die zu überwachenden Vorgänge, d.h. die Überwachungsgegenstände (in einem weiten Sinne von Gegenstand oder Objekt). Schließlich geht es ja nicht im eigentlichen Sinne darum, Dinge oder Personen zu überwachen, sondern deren Veränderungen bzw. deren Tun. Anders gesagt: eine Person zu überwachen, heißt ja gerade, festzuhalten, was diese Person tut. Einen Gegenstand, ein Gebäude oder ein Gelände zu überwachen, heißt ja gerade, festzuhalten, was sich an ihm, in ihm oder auf ihm so alles tut. Und dieses Tun nun ist zunehmend technisiert.

Zunächst sind dies automatische Prozesse wie etwas das Öffnen einer Tür oder eines Tores, das Einschalten der Beleuchtung o.ä. Wichtiger aber ist, dass die Tätigkeiten der zu überwachenden oder in den Fokus von nicht von vornherein personenbezogenen Überwachungsmaßnahmen geratenen Personen selbst mehr und mehr technisiert sind. Technisierung würde hier also, auf den Gegenstand und nicht die Mittel bezogen, bedeuten, dass mehr und mehr eine Überwachung technisierter Handlungen stattfindet. Und genau das scheint mit Informations- und Kommunikationstechniken einherzugehen: Personen rufen Informationen aus dem Internet ab, stellen diese über das Internet anderen zur Verfügung, oder kommunizieren dort und per Mobiltelefon direkt miteinander. Wo also früher papierne Dokumente den Besitzer wechselten, Gespräche mit direkten Gegenübern oder (und dann bereits ein Stück weit, nämlich analog technisiert) über Telefonleitungen stattfanden, werden jetzt neue, in (weiter) zunehmenden Maße technisch gestützte Handlungsmuster überwachungsrelevant. Doch nicht nur die Kommunikation selbst, sondern auch die vor- und nachgelagerten Instanzen erfahrene eine Technisierung: die Generierung der Inhalte, die kommuniziert werden (Textverarbeitung, Sprach-/Videoaufzeichnung usw.), die Archivierung und die Auswertung.

Synergien beider Technisierungen

Die beiden bisher benannten Technisierungsbereiche wechselwirken nun jedoch auch miteinander, und es kommt zu einer gewissen Konvergenz, die ich »TT-Überwachung« nennen möchte.

Von Wechselwirkungen kann man sprechen, weil Wirkungen in beiderlei Richtungen auftreten: einerseits greifen die zu überwachenden Personen vielfach gerade deshalb zu besonderen technischen Hilfsmitteln, weil es eine bestimmte Technisierung der Überwachungsmittel gegeben hat. Dies ist die bekannte Dynamik eines technisierten Wettrüstens durch Mittel- und Gegenmittelentwicklung. Anderseits macht die Technisierung von (Alltags-)Handlungen bestimmte Überwachungstechniken allererst möglich oder erfolgreich. So ermöglicht die heutige Mobiltelefonie die Erfassung von Ortsveränderungen von Personen auch, wenn diese nicht telefonieren oder ihr Gerät vermeintlich ausgeschaltet haben, quasi als Mehrwert dieser Technologie. Ebenso ermöglicht die Verwendung von Computern bei der Erstellung von Dokumenten, die Dokumente nicht mehr beim Austausch abfangen zu müssen o.ä., um in sie Einsicht nehmen zu können.

Insgesamt ist es daher nicht verwunderlich, dass technisierte Überwachung Resultat sowohl einer Technisierung der Überwachungsmittel als auch einer Technisierung der zu überwachenden Handlungen ist. Ich denke, man kann von einer Konvergenz beider Aspekte hin zu einer Form technisierter Überwachung sprechen, die ich »TT-Überwachung« nennen möchte: überwacht werden, aus Bequemlichkeits- oder Praktikabilitätsgründen heraus, mit technisch hochgerüsteten Mitteln genau diejenigen Handlungsvollzüge, die in hohem Maße technisiert sind. Denn gerade technisierte Handlungen bieten für Überwachungstechniken geeignete Ansatzpunkte, teils ganz ausdrücklich in Form von Schnittstellen (wie bei der E-Mail-Kommunikation). Bei manchen technisierten Handlungen ist die handlungsermöglichende Technik sogar mit der Überwachungstechnik identisch (»ITT-Überwachung«), d.h. überwacht zu werden ist ein notwendiger Teil der Handlungsunterstützung (z.B. bei Medizintechnik, bei location-based services, wenn die Buddy-List automatisch angezeigt, wer gerade online ist und wer nicht, oder wenn bei Phishing-Filtern jede URL die man ansteuert, an einen Server übertragen wird, der sie auf Indizien für einen Betrugsversuch hin untersucht). Hier ist dann nur noch die Frage, wem die (intrinsisch erzeugten) Ergebnisse der automatisierten Überwachung zugänglich sind. Dies wird de facto vom Besitzer der jeweiligen System-Infrastruktur bestimmt, wenn auch juristische Standards und das Nutzerverhalten (u.a. als »consumer power«) ebenfalls eine Rolle spielen bzw. den Besitzer beeinflussen können.

Systemische Effekte

Teils unterwerfen wir uns aus Bequemlichkeit oder Neugier der Möglichkeit, technisch überwacht zu werden, indem wir auf technisierte Weise handeln, ohne es zu müssen. Teils tun wir dies, weil wir auf bestimmte (technisierte oder nicht technisierte) Handlungen nicht verzichten wollen oder können. Teils lassen wir uns ganz bewusst darauf ein, überwacht zu werden, weil wir bestimmte Handlungen sonst gar nicht tätigen könnten, teils begeben wir uns auch aktiv in Überwachungssituationen, dann nämlich, wenn wir uns dadurch geschützt sehen (d.h. wenn auch andere mitüberwacht werden, etwa in einem öffentlichen Raum, einem Internet-Chatroom o.ä.) oder wenn uns anderweitige Vorteile versprochen werden (wie etwa beim Payback-Verfahren, wo man sein Kaufverhalten hersteller- und verkaufsstellenübergreifend überwachen und auswerten lässt und dafür Rabatte bzw. Prämien erhält, vgl. http://www.bigbrotherawards.de/2000/.com/index.html).

Dies vielleicht der Ort, über die positiven Seiten von technisierter Überwachung genauer nachzudenken. Überwachung begrenzt nicht nur Räume (vgl. Gaycken 2007, S. 32), seien es psychische »needed to feel autonomous, free, authentic, individual, to have values, to decide freely and to judge ethically« oder soziale »needed to think and live, for reform and change« oder tatsächliche »of acting and communicating«, sondern eröffnet auch solche. Sei es durch Sicherheitsgefühle (man traut sich unter Überwachung wieder an bestimmte Orte, muss nicht permanent auf Bedrohungen reagieren und gewinnt dadurch Zeit und Sicherheit für autonome Entscheidungen), sei es durch die Ermöglichung stabiler Erwartungen (dass andere korrekt handeln, sich an Spielregeln halten), sei es durch einen gemeinsamen Hintergrundkonsens in überwachten Räumen (so dass man unterstellt, dass der andere sich deshalb in diesen Raum begibt, weil er mit dem Ziel der Überwachung einverstanden ist, z.B. weil er bestimmte Gesprächsthemen, Gewaltdarstellungen o.Ä. ebenfalls unangenehm findet). In diesen Hinsichten ist (technische) Überwachung auch nur Ausdruck (und Agens) allgemeiner Normierung. Recht und Moral dürften ähnliche Effekte haben; die öffentliche Normsetzung und – vor allem – Entscheidung von Fällen im Recht, die informelle Saktionierung bei moralischen Verfehlungen: dies bewirkt eine Internalisierung von Werten und Normen, die ebenfalls auf gegenseitiger Überwachung fußt und deren Doppelwirkung einerseits der Beschränkung und andererseits der Ermöglichung von Handlungen durch Normen ein klassisches Thema der Rechts- und Sozialphilosophie ist.

Nicht immer aber, und das wird in der Diskussion leicht übersehen, nehmen wir Überwachung nur mehr oder weniger zähneknirschend hin. Teils begeben wir uns nämlich auch in Überwachungssituationen, weil wir es gut finden, beobachtet zu werden. So ist es für einige ganz angenehm, von einer höheren Instanz überwacht zu werden, etwa vom Vorgesetzten, da dieser einem gegebenenfalls ja schon sagen wird, wenn man etwas falsch macht: Überwachung kann einem also auch Sicherheit geben, da sie von Verantwortung entlastet. Doch damit nicht genug: so scheint es für manche Jugendliche regelrecht Teil des Identitätsbildungsprozesses zu sein, die persönlichsten Erlebnisse Freunden und Fremden öffentlich zur Kenntnis zu geben, d.h. sich auf bestimmte Weise zur Schau zu stellen und die Schau, die andere veranstalten, zu rezipieren – in einer Art reziproker juveniler Überwachungskultur. Dies mag in anderen Kulturen, etwa buddhistischen, durchaus noch stärker ausgeprägt sein und dort auch mit traditionellen Techniken etwa der Läuterung und Befreiung vom Selbst durch öffentliche Preisgabe von Privatheit verbunden sein (vgl. Nakada/Tamura 2005, S. 29-31).

Private Akteure, Individuen stellen sich also freiwillig selbst aus, in Wort und Ton, in Bild und Film. Es ist schick, alles von sich preiszugeben, sei es aus eitlem Selbstmarketing oder uneitler Befreiung vom Selbst. Vielleicht will man so auch nur seine technische Kompetenz demonstrieren, gegen die Eltern rebellieren oder was auch immer. Früher: ich habe nichts zu verbergen (dem Staat gegenüber). Heute: dito, sich selbst und anderen gegenüber. Entweder: ich habe viel zu zeigen (jedem, der es sehen will), oder: ich habe mich von Privatem freigemacht. So diametral entgegengesetzt diese Motivationen sein mögen, so ähnlich ist doch das Resultat. Und selbst für diejenigen, die diese Motivationen nicht teilen, dürfte es mehr und mehr normal scheinen, überwacht zu werden (und vielleicht auch, zu überwachen oder überwachen zu können).

Und selbst wenn wir es nicht gut oder normal finden, überwacht zu werden: bei vielen unserer Handlungen können wir auf den Einsatz mehr und mehr technisierter Mittel nicht verzichten, da ihr Gelingen nicht nur von uns abhängig ist. Sei es, dass die bisherigen technischen Artefakte nicht mehr repariert werden können oder dass sie keinen Sinn mehr machen, weil niemand sonst sie noch benutzt. Teilweise sind unsere bisher verwendeten Artefakte auch nicht mehr anschlussfähig, d.h. nicht nur unsere Handlungen müssen zu denen anderer Personen passen, sondern auch unsere Artefakte zu anderen Artefakten: dies ist der Systemcharakter moderner Technik, der einen Werkzeug- oder Maschinencharakter ablöst (vgl. zu diesen Unterscheidun-

gen Hubig, a.a.O.). In diesem Sinne sind wir also sozialen und technischen Zwängen ausgesetzt, zu technisierten Handlungen und zur Akzeptanz dadurch möglicher (und wirklicher) technisierter Überwachung.

Ganzheitliche Überwachung

Betrachtet man den Handlungskreis von Planung, Ausführung, Reflexion (und dann neuer Planung, Ausführung usw.), dann scheint sich Überwachung zunächst vor allem auf die Ausführung zu richten, d.h. auf das beobachtbare Tun. Doch schon immer wurden auch Pläne und Reaktionen ausgekundschaftet, sofern das möglich und wichtig genug war. Durch den Zugriff auf Informations- und Kommunikationsprozesse gelingt das nun erstmals im großen Stil. Das Handeln von Personen soll also nun *übergreifend*, d.h. in allen seinen Phasen überwacht werden (nicht nur in der Aktion). Auch in anderen Hinsichten lassen sich angesichts technisierter Überwachung Begehrlichkeiten ausmachen, die man als Ausdruck eines Wunsches nach »ganzheitlicher Überwachung« bezeichnen könnte:

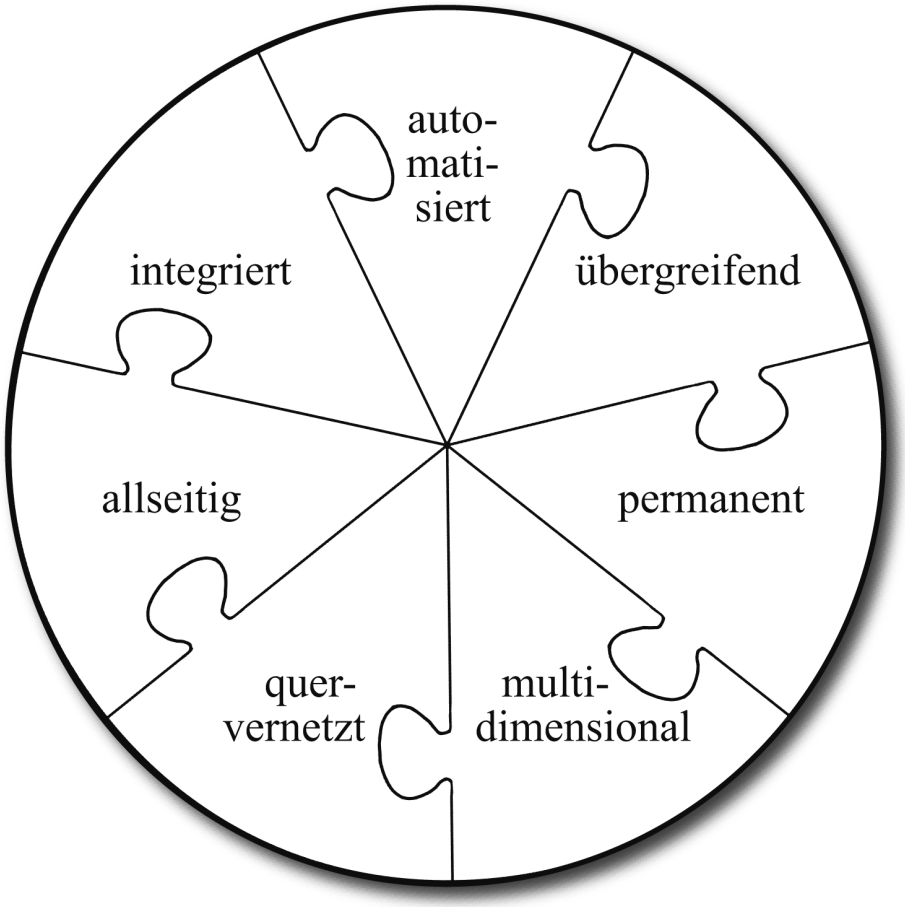
Die Überwachung geschieht *multidimensional*, auf allen Kanälen. Mit der Informatisierung basaler menschlicher Vollzüge wie mündlicher und schriftlicher Kommunikation, Bewegung (typische Autos enthalten über ein Dutzend Mikroprozessoren, loggen die Fahrgeschichte mit usw.; Bahnfahrten werden online gekauft oder elektronisch bezahlt usw.), Tausch (Kauf und Verkauf mit elektronischer Zahlung oder gleich bei ebay) wird die althergebrachte audiovisuelle Überwachung um viele weitere Kanäle ergänzt.

Die Überwachung geschieht nicht mehr temporär, sondern ist *permanent*, da mit jeder Aktualisierung technisierter Handlungsvollzüge gegeben. Alle diese Vollzüge können jederzeit überwacht werden (wenn sie überhaupt überwacht werden können). Und die Resultate dieser Überwachung können auf unbestimmte Zeit verfügbar gehalten werden: nichts muss aus technischen Gründen mehr gelöscht werden (ein großer Online-Buchhändler z.B. speichert jeden Mausklick jedes Besuchers auf ewig).

Die Überwachungsergebnisse werden *quervernetzt*: einerseits über die Zeit (diachron), andererseits zwischen den Kanälen (synchron wie diachron) wird nach Querverbindungen und Vernetzungen gesucht. Zudem werden die Ergebnisse vor dem Hintergrund weiterer, immer komfortabler maschinell zugänglicher Wissensbestände interpretiert und ausgewertet.

Die Überwachung ist *allseitig*: jede/r macht mit, nicht nur der Staat (oder eine ähnliche Zentralmacht, wie in Orwells Roman »1984«), sondern auch Individuen, Unternehmen, Hacker, Terroristen usw. – daher sollte man auch besser von einer Überwachungsgesellschaft sprechen und nicht mehr von einem Überwachungsstaat (vgl. auch Stanley/Steinhardt 2007).

Abbildung 1: Ganzheitliche Überwachung



Quelle: Autor

Die Überwachung ist *integriert*: ähnlich wie beim »integrierten Umweltschutz« wird bei der integrierten Überwachung »von der Wiege bis zur Bahre« einer Technik auf Überwachungsmöglichkeiten geachtet: bereits bei der Produktentwicklung, dem Setzen von Systemstandards etc. (»surveillance built in«, »surveillance by design«). Und es werden gezielt die schwer zu überwachenden Technologien zuerst zu

entsorgen gesucht, z.B. durch Veränderung von Standards oder das Einstellen der Produktion von Ersatzteilen.

Die Überwachung ist *automatisiert*: niemand muss »es« mehr tun, es geschieht von selbst. Und ist damit auch nicht mehr durch das zur Verfügung stehende Personal in Umfang und Intensität begrenzt oder von der Kooperation einer großen Zahl von Menschen abhängig, wie es bei früheren Bespitzelungsinitiativen noch der Fall war (beispielhaft sei hier das Ministerium für Staatssicherheit MfS der früheren DDR genannt, mit ca. 90.000 hauptamtlichen und 180.000 inoffiziellen Mitarbeitern – »Zuletzt kommt auf 62 Einwohner der DDR ein MfS-Mitarbeiter«, so das Deutsche Historische Museum 2000).

Von Überwachung zu Kontrolle

Zwei Phänomene vor allem sind es, an denen man m.E. die weitere Entwicklung technischer Überwachung besonders gut diskutieren kann.

Erstens: automatisierte ganzheitliche Überwachung liefert viel zu viele Informationen, diese kann kein Einzelner mehr auswerten; das wurde bereits gesagt. Daher geschieht die Auswertung einerseits arbeitsteilig, andererseits aber (und das mehr und mehr) im wesentlichen ebenfalls automatisch. Doch nicht nur auswerten, auch entsprechend reagieren muss man – und hier stellt sich dasselbe Problem. Eine adäquate Reaktion ist, außer in besonderen Fällen vielleicht, personell nicht zu leisten. Also wird man nicht nur die Auswertung automatisieren wollen – sondern auch die Reaktion.

Zweitens: bei technisierten Handlungen ist prinzipbedingt der Handlungserfolg von Funktionieren der Technik abhängig. In steigendem Maße ist das Funktionieren der handlungsunterstützenden Artefakte ausdrücklich daran gebunden, sich überwachen zu lassen (Aktivierung von Software, Integritätsprüfung bei Online-Computerspielen, Zwangs-Firmwareupdates bei Handys und, über die Datenträger, bei HD-DVDs). Technisierte Handlungen bieten also, vielfach intrinsisch, Möglichkeiten und Schnittstellen zur Ausführungsverweigerung oder –erzwingung.

Sowohl also aus Überwachersicht aus Praktikabilitätsgründen gewünscht, als auch bei technisierter Überwachung von technisierten Handlungen (TT-Überwachungen) technisch gleich eingebaut, ist damit die Möglichkeit von *Kontrolle,* nicht mehr nur von Überwachung: man weiß nicht nur, wer was tut oder tun kann, sondern man kann darüber verfügen, wer was tun kann oder tun muss. Dieses Verfügen-Können wird erleichtert durch den Systemcharakter moderner Technik (s.o.),

d.h. durch ein wechselseitiges Aufeinandergewiesen-Sein der Geräte bzw. von Funktionsakten der Geräte. Die Effektivität einer solchen Kontrolle ist daher, denke ich, nicht zu überschätzen. Schon jetzt betreffen diese Kontrollversuche den klassischen Personal Computer, in Hardware (Schoen 2003, Anderson 2003) und Software (Gutmann 2006). Und demnächst dürfte es mehr und mehr auch um die Kontrolle von zeitkritischen Informationssystemen und schließlich auch von Aktuatoren gehen. Am besten drahtlos und unbemerkt. Spätestens seit dem 11. September und der Aufmerksamkeitskarriere terroristischer Bedrohung sind private, zivil-öffentliche und militärische Aspekte der Überwachung kaum noch zu trennen, werden auch die entsprechenden Infrastrukturen zusammengelegt (Gorman 2007, Stanley/Steinhardt 2007, S. 6-8). Im Lichte der Möglichkeiten, die eine Kontrolle gegenüber einer bloßen Überwachung bietet, wären entsprechende Begehrlichkeiten ebenfalls nur zu gut verständlich: Niemand muss dann mehr Terroristen-Autos aus Hubschraubern mit Raketen beschießen, wenn er sich auch in die Fahrzeug-Elektronik einhacken und diese nach Wunsch manipulieren kann!

Zwei Visionen der Evolution des Internet verstärken den Systemcharakter und kommen automatisierter Auswertung und Kontrolle entgegen: das Semantic Web (der automatischen Recherche) und Ubiquitous Computing (der automatischen Kontrolle).

Vom »Erfinder des Internet« Tim Berners-Lee wurde 2001 darüber nachgedacht, wie man dem Internet semantische Strukturen beibringen kann, d.h. durch Zuordnung von Kategorien zu Inhalten usw. Die Konzepte dazu sind alle da, aber bisher werden sie einfach nicht genutzt. Die Inhalte wachsen schneller und werden mit heuristischen Methoden einigermaßen gefunden werden. Wenn das semantische Netz doch noch vorankommen sollte, würde das die automatischen Überwachungs- und Kontrollmöglichkeiten wesentlich erweitern, denn vor allem sind es Algorithmen und Agenten, die die semantischen Metainformationen brauchen; Menschen können auch so sehr zuverlässig unterscheiden, ob ein Text von Fischernetzen, Spinnennetzen, Beziehungsnetzen oder vom Internet handelt, wenn in ihm von »Netzen« die Rede ist.

Ubiquitous Computing ist im Prinzip die Konsequenz aus dem Systemcharakter der Technik und der Miniaturisierung: Handy, DSL-Router, PCs, Server, Laptops, PDAs, MP3-Player, Digitalkameras, Naviationssysteme, KFZ-Steuerungssysteme – aber auch Drohnen und Kameranetze zur Überwachung des privaten oder – wie in GB – des öff. Raums, Wahlcomputer, Verkehrsleitsysteme, Mautstellen usw. sowie eine Funketikettierung nicht selbst aktiver Gegenstände (sog. RFID-Tags, die drahtlos auf kürzere Distanzen ausgelesen wer-

den können und eine computergerechte Verbindung zwischen [bisher] passiven und den vernetzten aktiven Gegenständen schaffen, bieten u.a. eine eindeutige Identifizierbarkeit von [»intelligent shop«] Waren und [»elektronischer Personalausweis«] Menschen, drahtlos und unbemerkt) – all das könnte nur der Anfang sein. Zukunftsforscher sehen in den nächsten Jahren und Jahrzehnten eine vernetzte intelligente Infrastruktur entstehen (Sharpe/Hodgson 2006, S. 3), ähnliches scheint sich auch im militärischen Bereich abzuzeichnen (vgl. Boes 2005). Mark Weiser beschrieb bereits 1996 seine einflussreiche Vision einer intelligenten Infrastruktur, die Menschen – wie ich sagen würde – in ihrem Wissen-wie, in ihrem Können unterstützt, so:

»Inspired by the social scientists, philosophers, and anthropologists at PARC, we have been trying to take a radical look at what computing and networking ought to be like. We believe that people live through their practices and tacit knowledge so that the most powerful things are those that are effectively invisible in use. This is a challenge that affects all of computer science. Our preliminary approach: Activate the world. Provide hundreds of wireless computing devices per person per office, of all scales (from 1" displays to wall sized). … We call our work ‚ubiquitous computing'.«

Einiges davon ist ja schon da und wurde weiter oben aufgezählt. Was ist da drin? Sie haben: modular aufgebaute Geräte, Embedded-PCs, teils auch mit Aktuatoren (die können also etwas tun, nicht nur etwas signalisieren), mit genormten Softwaregrundlagen (Middleware) von Großrechner bis Waschmaschine und Armbanduhr, die im Kern identisch sein kann (wie bei Linux). Diese Geräte laufen alle mit genormten Mikroprozessoren, und allein ein modernes Auto hat über ein Dutzend davon. Dass es irgendwann normal sein könnte, dass Geräte alle mit Mikroprozessoren versehen sind, kommt auch ganz gut in Neal Stephensons Roman *The Diamond Age* zum Ausdruck: hier bauen zwei Kinder eine Uhr auseinander und stellen ganz überrascht fest: das ist ja *nur* Hardware!

Der gegenwärtige Trend scheint eindeutig, die Dinge alle miteinander elektronisch zu vernetzen, und zwar möglichst drahtlos und selbstgesteuert, d.h. ohne Benutzereingriffe vorzusehen. Interdependenz einerseits sowie die Verwendung von Standardkomponenten relativ hoher Komplexität andererseits schaffen eine Infrastruktur, deren Lücken es sich lohnt, zu finden (weil man dann etwas tun oder andere an etwas hindern kann, d.h. andere kontrollieren) bzw. auf die es sich lohnt, Bundes-Trojaner oder deren Kontrollpendant, »Bundes-Bots« würde ich sie nennen, anzusetzen. Und in vernetzter Struktur

dann wo nicht automatisch, dann bei Bedarf ad hoc aus der Ferne zu intervenieren (Tätigkeiten blockieren oder erzwingen, Informationen verfälschen oder unterdrücken, usw.) Gleichzeitig eröffnet diese Struktur aber auch die gezielte Modifikation dieser Geräte seitens der User: so kann man für fast alle der oben genannten Geräte modifizierte Firmware bekommen, die irgendeine wohlmeinende (oder übelmeinende) Seele mit neuen Funktionen versehen hat (Mehr oder weniger normal scheint das bei Set-Top-Boxen für Fernseher und bei Handys zu sein, beim Auto vielleicht noch nicht gleichermaßen, dort hat es aber auch schon einen Namen: »Chipsatz-Tuning«).

Beide mögliche Entwicklungen, das Semantic Web und Ubiquitous Computing, haben zunächst einmal Konsequenzen für die Dynamik von Information und Wissen (vgl. Gottschalk-Mazouz i.E.), und damit auch für technisierte Überwachung. Ubiquitous Computing aber will mehr, es zielt direkt auf das »knowing-how« der Subjekte, auf ihr Können. In diesem will es sie unterstützen, von deren Funktionieren werden Handelnde abhängig. Dadurch werden sie kontrollierbar. Ich glaube daher, dass eine entsprechenden Evolution des Internet auch die Richtung für die Evolution der Überwachungsgesellschaft vorgeben würde: hin zur Kontrollgesellschaft.

Kontrolle und Macht

Eine erfolgreiche Überwachung verschafft dem Überwachenden ein Wissen, das er ausnutzen kann. Aber verschafft es ihm auch Macht? Gilt denn nicht: »Wissen ist Macht« (so das Francis Bacon zugeschriebene Zitat, das es zu einer Binsenweisheit gebracht hat)? Wenn man sich genauer klarmacht, was »Wissen« in der Wissensgesellschaft heißt, lässt sich auch genauer sagen, inwiefern Wissen Macht ist (vgl. Gottschalk-Mazouz 2007, S. 35ff.): insofern nämlich, als Wissen Handlungen ermöglicht, verleiht es einem Macht, etwas zu tun, das man sonst nicht tun könnte (sei es gegenüber dem Überwachten, sei es Dritten gegenüber). Und aus demselben Grund verleiht es einem Macht, wenn man Wissensbestände verändern oder vorenthalten kann. Insofern schließlich, als Wissen einen autokatalytischen Effekt hat, also mehr und mehr Wissen und Können hervorbringen kann, wird Wissen nicht nur einer operativen, sondern auch zu einer strategischen Ressource.

Kontrolle hingegen ist noch viel enger mit Macht verbunden. Macht, so kann man allgemein sagen, besteht geradezu im Kontrollieren von Handlungen. Das lässt sich bereits an Max Webers klassischer Definition ablesen (»Macht bedeutet jede Chance, innerhalb ei-

ner sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel worauf diese Chance beruht«, so Weber 1980, S. 28). Anders als in Herrschaftsbeziehungen ist hierfür kein Gehorsam der Betroffenen erforderlich; deshalb lässt sich machtförmigen Verhältnissen auch nicht einfach entgehen. Er schreibt weiter dazu: »Der Begriff ›Macht‹ ist soziologisch amorph. Alle denkbaren Qualitäten eines Menschen und alle denkbaren Konstellationen können jemand in die Lage versetzen, seinen Willen in einer gegebenen Situation durchzusetzen.« Wenn jemand also Herr über den Erfolg der Handlungen anderer Personen ist, andere in diesem Sinne nicht nur überwacht, sondern auch kontrolliert, kann er seinen Willen jederzeit durchsetzen, sei es durch die Eliminierung von Widerstand seitens der Betroffenen oder durch die (ungewollte) Hilfe Dritter.

Die soziopolitisch interessante Frage ist, wem diese Macht zufällt. Das lässt sich nämlich häufig gar nicht genau sagen. Einerseits ist es sicher wichtig, angesichts des Systemcharakters moderner Technik, wer die Infrastruktur besitzt (Gaycken, a.a.O.). Doch das Funktionieren der Infrastruktur ist wiederum von Standards abhängig, die der Besitzer nicht allein festlegen oder fortschreiben kann, muss politisch-juristische Rahmenbedingungen reflektieren, muss von Nutzern, Komponentenherstellern usw. akzeptiert werden. Und auch innerhalb fixer Infrastruktur lässt sich eine Menge machen. Somit denke ich, dass der Kreis weiter zu ziehen ist, Macht teils auch nicht einzelnen Personen oder Korporationen zufällt, sondern in einem reichlich unübersichtlichen Geflecht von Interessen Schritt für Schritt täglich neu ausgehandelt und verteilt wird. Dies scheint mir auch ein zentraler Aspekt der Überwachungs- und Kontrollgesellschaft.

Oben wurde auf das Phänomen hingewiesen (so es wirklich eines ist), dass wir uns teilweise ganz gerne überwachen lassen. Der Vorgesetzte, der ein Auge auf einen hat, überwacht aber nicht nur, sondern greift, wenn es sein muss, auch ein – er kontrolliert einen also auch. Könnte man sich vorstellen, analog zum oben zur Überwachung ausgeführten, dass auch Kontrollverhältnisse intrinsisch positiv bewerteter Teil einer, sagen wir, Jugendkultur oder buddhistischen Selbst-Überwindung werden?

Eine buddhistische Variante kann man sich leicht zusammenreimen, zumal sie sich mit dem derzeit öffentlich propagierten Credo der Hirnforscher trifft, nämlich als Ad-acta-Legen des Ichs als (vermeintlich) ausschlaggebender Instanz kontrollierten Tuns. Wenn die Steuerung des eigenen Tuns durch ein »Ich« aber sowieso nur eine eitle Illusion ist, die es zu durchschauen gilt, dann ist es nur konsequent und Ausdruck dessen, dass man diesen eitlen Anspruch aufgegeben hat,

wenn man sich äußeren Determinanten komplett öffnet. Man findet es dann nicht mehr negativ, sondern genießt es regelrecht, nicht mehr »selbst« handeln zu müssen.

Auch eine Jugendkultur mit Spaß am reziproken Kontrollieren lässt sich vorstellen. Dies muss dabei gar nicht masochistisch interpretiert werden, d.h. als Lust an der eigenen Erniedrigung oder Ohnmacht, da es ja wechselseitig geschieht und sich so jeder mal auf dieser und mal auf jener Seite wiederfindet. Wechselseitig lässt man andere bei einem/mit einem tun, was sie wollen. Oder man kreiert Orte, an denen keiner allein bestimmte Dinge tun kann. In der Gesellschaft gibt es für freiwillige reziproke Kontrolle viele Beispiele, denke ich, Ehen z.B. und viele Gesellschaftsspiele haben diese Struktur.

Mit fortschreitender Medizintechnik (Prothesen, Implantate usw.) würde zudem auch die Grenze zwischen Biologie und Technologie zunehmend verwischt. Technisierte Überwachung und Kontrolle könnte daher auch dasjenige katalysieren, was Michel Foucault Biopolitik oder auch Biomacht genannt hat (Foucault 1974/2001), eine Kontrolle über Lebendiges, die nur teilweise (als Fremd- oder Selbstkontrolle) Personen klar zurechenbar ist. Für einen Cyborg schließlich wären Bio- und Technopolitik ohnehin nicht mehr unterscheidbar.

Vielleicht sind die Phänomene wechselseitiger Kontrolle aber auch viel greifbarer und auch ohne viel Spekulation zu benennen. Wenn eine Person als Filesharer anderen die Möglichkeit gibt, bei sich Dateien herunterzuladen, d.h. sich zum Anbieter bestimmter Dateien machen lässt, wenn sie andere ihr offenes Wlan nutzen lässt, einen Tor-Exit-Node oder einen offenen Proxy bereitstellt, Speicherplatz für das Peer-to-Peer-Netz Freenet bereitstellt, durch die Nutzung von Skype ihren Rechner als Relay für die Kommunikation Dritter zur Verfügung stellt o.ä., dann lässt sie sich bereits von anderen kontrollieren, denn andere können Aktionen vornehmen, die dieser Person (auch juristisch) zugerechnet werden. Ähnlich ist die Situation, wenn eine Person nachts auf seinem Rechner von Seti@home aufgefangene Signale nach Botschaften außerirdischer durchsuchen lässt oder von Einstein@home Gravitationswellen suchen lässt o.ä..

Wenn eine Person modifizierte Firmware herunterlädt und einspielt, wenn sie Hacks und Cracks benutzt, dann gibt sie anderen die Möglichkeit, bestimmte Dinge zu kontrollieren (häufig übrigens in der Absicht, Einschränkungen und Kontrolle durch wieder andere, etwa den sich des Branding bedienenden Herstellers, zu kontern). Auch wenn sie das (Windows-)Autoupdate einschaltet oder auch nur einen Virenscanner oder eine Personal Firewall installiert, gibt sie an-

deren die Möglichkeit der Kontrolle, d.h. des Verfügens darüber, ob die eigenen Handlungen gelingen oder nicht.

Doch ist das nicht schon damit der Fall, das man überhaupt ein Textverarbeitungsprogramm, ein Betriebssystem, einen Computer benutzt, und war das nicht auch schon früher der Fall, als man noch eine Schreibmaschine oder einen Stift benutzte? Die Grenzen sind insofern tatsächlich fließend, vielleicht auch generell in arbeitsteiligen Gesellschaften nicht scharf zu ziehen. Bisher jedoch nutzte man zwar sehr komplexe, aber dennoch »statische« Mittel, deren Funktionen sich nicht unangekündigt verändern und an denen zwar Defekte auftreten, die jedoch nicht von außen deaktivierbar waren. Der entscheidende Unterschied, was Kontrolle betrifft, besteht also im Übergang zu „dynamischen“ Mitteln, deren Dynamik für den Benutzer weder vorausgesehen noch letztlich bestimmt werden kann: diese Mittel bleiben stets auf Dritte bezogen, denen sie letztlich gehorchen. Und an die sie den Benutzer ggf. verpetzen, wenn er Dinge tut, die er nicht tun soll. Bzw. an die sie melden, was der Benutzer mit ihnen tut, egal was er tut. Und wenn diese Mittel das heute noch nicht machen, dann vielleicht nach dem nächsten automatischen Update.

Eben deshalb lassen sich Kontrolle und Überwachung auch nur begrenzt durch Offenlegung demokratisieren (obwohl sich damit halbwegs überschaubare statische Strukturen wirkungsvoll demokratisch kontrollieren lassen, so dass es zu offenen Standards, Sourcecodes, Kryptographiealgorithmen usw. m.E. keine sinnvolle Alternative gibt). Umso wichtiger werden Tugenden und Vertrauen: Vertrauen darin, dass bestimmte Personen oder Gruppen bestimmte Dinge einfach nicht tun (werden), vor bestimmten Dingen schon warnen würden, wenn sie bedenklich wären usw. Solches Vertrauen ist heutzutage schwer zu erwerben, aber leicht zu verspielen, wie z.B. die Marktführer von PC-Betriebssystemen und WWW-Suchdiensten erfahren haben, die sich seit Jahren redlich bemühen, den Ruf als »Datenkraken« los zu werden – bislang wenig erfolgreich.

Überwachungsphilosophien

In unübersichtlichen, sich schnell verändernden Situationen sind starre Regeln oft wenig hilfreich. Haltungen, Leitlinien oder »Philosophien« ermöglichen hier häufig die bessere Orientierung. Zumindest helfen sie aber, sich prinzipiell darüber zu verständigen, wo man hin will und wo nicht. In diesem Sinne lassen sich auch Überwachungsphilosophien bzw. Kontrollphilosophien unterscheiden. Für Überwachung (und

Kontrolle) gibt es ja ganz unterschiedliche *rationales*, die eine versteckte, verdeckte, offene oder gar öffentliche Überwachung leiten. Teils möchte man nicht, teils möchte man gerade, dass die Betroffenen oder weitere Personen (oder gar die allgemeine Öffentlichkeit) erfahren, dass überwacht wird oder, was die Überwachung ergeben hat. Teils möchte man bestimmte Schwellen der Intimität nicht überschreiten. Nach letzterem geordnet könnte man verschiedene Philosophien verdachtsunabhängiger Überwachung unterscheiden:

1. Da wäre zunächst das Monitoring als Erfassung bestehender öffentlich zugänglicher Daten und ihrer Veränderung, d.h. das kontinuierliche Durchforsten von öffentlich zugänglichen Registern wie dem Telefonbuch, dem WWW usw. (inklusive der Tausende Chinesen, die das chinesische WWW nach Auffälligkeiten durchsuchen). Dieses Monitoring erledigt man selbst, oder ruft andere dazu auf, inadäquate oder unstimmige Inhalte anzuzeigen, usw. Dies entspricht, lose gesprochen, dem Aus-dem-Fester-schauen und Die-Augen-Offenhalten.
2. Dann haben wir die Installation von Beobachtern. Dies geschieht meist gut sichtbar, da es von etwas abschrecken soll, aber nicht immer. Mit der Nutzung einer bestimmten Ressource, mit dem Betreten eines bestimmten Ladens, mit dem Betreten eines bestimmten öffentlichen Raumes willigt man darin ein, dass man fotografiert und gefilmt wird. Dieselbe Struktur, wenn auch für die meisten Benutzer weniger offensichtlich, dürfte das Benutzen eines Geldautomaten haben (bei dem man ebenfalls obligatorisch, aber verdeckt gefilmt wird) oder das Erzeugen von Verbindungsdaten. Das Beobachten von Personen- und Datenbewegungen bleibt aber insofern äußerlich, als dass nur das »dass« von Interaktion und Kommunikation erfasst wird, nicht auch das »was«.
3. Als nächste Stufe würde ich das Lauschen an Gateways betrachten, bei dem auch inhaltlich ausgewertet wird. Es werden also z.B. Bewegungen nicht nur gefilmt, sondern es werden die Personen bzw. Kennzeichen auch identifiziert. Oder es wird staubsaugerartig nach Stichworten in E-Mails und Telefongesprächen an den übermittelnden Netzknoten gesucht. Nun wird also erfasst, wer was tut, schreibt oder sagt.

Bei diesen drei Stufen wird zwar u.U. auch schon die Privatsphäre massiv verletzt und die rechtsstaatliche Unschuldsvermutung eingeschränkt, aber es wird aus Sicht des Benutzers dennoch eine bestimmte Distanz gehalten. So wird der persönliche Besitz nicht angetastet, die eigenen technischen Artefakte nicht verändert (sondern höchstens deren Infrastruktur). Die mit der Online-Hausdurchsuchung bzw. dem Bundestrojaner diskutierten Bestrebungen sind nun jedoch weitergehend. Ein verdachtsabhängiges Szenario (4*) würde z.B. so aussehen: Eine Tür wird on demand angebracht und aufgemacht. »On demand« heißt: Nur

wenn es einen konkreten Verdacht gibt, wird das technische Gerät (sagen wir: der Computer) mit einer Tür oder Hintertür versehen und dann, offen oder verdeckt, durchsucht. Der Unterschied zu einer nicht technisierten Überwachung besteht dann vor allem darin, dass nicht ein Schlüssel zu einer bestehenden Tür ausgehändigt werden muss oder eine bestehende Tür aufgebrochen.

Abbildung 2: Stufen verdachtsunabhängiger Überwachung

Quelle: Autor

Davon ausgehend lässt sich nun aber die oben begonnene Liste von Philosophien verdachtsunabhängiger Überwachung fortsetzen:
4. Die Tür wird per default angebracht und on demand aufgemacht. Bei möglichst jedem interessanten technischen Gerät oder jedem Erzeugnis dieses Geräts (z.B. Nachrichten) jedes Benutzers wird eine Tür oder Hintertür angebracht. Das könnte durchaus öffentlich geschehen, wenn man nur den Schlüssel gut genug hütet (vgl. das US-Vorhaben eines entsprechenden Verschlüsselungschips namens Clipper). Diese Tür wird also, idealerweise z.B. gleich per Microsoft-Update, großflächig eingebaut. Aufgemacht wird sie aber nur, wenn es einen konkreten Verdacht gibt. Nur dann wird fremder Code zur Analyse eingebracht und, z.B., durchsucht. Die nicht technisierte Analogie wäre vielleicht die Anfertigung eines Generalschlüssels für alle Wohnungen.

5. Die Tür wird per default angebracht und durchschritten, das Innere wird präpariert. Hier wird der fremde Analysecode schon eingebracht, d.h. die Kamera schon in der Wohnung aufgebaut, und bei konkretem Verdacht aktiviert.
6. Die Tür wird per default angebracht und durchschritten, im Inneren wird eine permanente Suche installiert, die dann nach außen liefert, wenn sie fündig wird – unterschiedslos bei jedem. Hier würde die Kamera in der Wohnung schon angeschaltet und es würden eventuell belastende Bilder automatisch nach außen gesendet.

Wenn man sich anhört, was die »Remote forensic software« leisten soll, denkt man, es solle durchgängig nur auf konkreten Verdacht hin gehandelt werden (wie in 4*). Entsprechend hat sich z.B. auch LKA-Chef Wolfgang Gatzke geäußert, als ich ihn nach einem Vortrag zu Unscharfen Grenzen im Recht und Handlungserfordernissen aus Sicht der polizeilichen Praxis traf, in dem er sich nachdrücklich für die Schaffung rechtlicher Grundlagen für eine Online-Durchsuchung aussprach (ohne klar zu sagen, was er sich darunter vorstellt), mit den hier unterschiedenen Philosophien. Wenn man sich hingegen anhört, was Kritiker vom Bundestrojaner erwarten, dann denkt man, es ginge um die durchgängig verdachtsunabhängige Philosophie sechs. Damit einhergehend bleibt unklar, welchen Grad von Konkretheit eine Gefahr haben muss, um die in den Philosophien eins bis sechs zum Ausdruck kommenden verdachtsunabhängigen Elemente zu rechtfertigen. Hier besteht also weiterer Klärungsbedarf.

Die Attraktivität verdachtsunabhängiger Elemente liegt u.a. darin, dass mit ihr dezentrale Lösungen etabliert werden können, die den mehr und mehr dezentralen Kommunikations- und Interaktionsstrukturen entgegenkommen und das Flaschenhals-Problem lösen könnten, das eine konventionelle Strategie hat: Daten erst zu speichern und dann (bei Verdacht ggf. rückwirkend) zu analysieren, überforderte angesichts von täglichen geschätzten 500 Petabytes allein an Internetverkehr sogar den weltweit größten Lauscher, die US-amerikanische NSA, die inzwischen unter dem Titel *Turbulence* darauf setzt, die Ressourcen der verdachtsunabhängig überwachten Systeme selbst einzusetzen (vgl. Rötzer 2007). Doch nicht nur die Analyse, auch die Reaktion soll teilweise dezentral erfolgen: Ziel von *Turbulence* ist es nämlich auch, die Übermittlung verdächtiger Datenpakete zu verhindern, d.h. es ist beabsichtigt, automatisiert nicht nur zu überwachen, sondern auch zu kontrollieren.

Aus technischer Sicht dürfte einerseits interessant sein, inwiefern es sich durchsetzen wird, dass einige dieser Philosophien »by design« verfolgt werden, d.h. nicht unterlaufen werden können, ohne dass grundlegende (System-)funktionen gefährdet wären. Andererseits

dürfte, wenn die Analyse der Verlängerung der Überwachungsgesellschaft in die Kontrollgesellschaft plausibel ist, auch interessant sein (oder werden), inwiefern nicht nur Überwachungs-, sondern auch Kontrollfunktionen bzw. Schnittstellen dafür gleich mit vorgesehen sind (oder sein werden). Inwiefern also z.B. ein »external override« vorgesehen ist, ein Funktionieren an eine erfolgreiche Online-Abfrage gebunden ist oder an einen während des späteren Gebrauchs nicht zurückgezogenen Schlüssel, im Zuge eines vollendeten sogenannten Digital Rights Managements (Gieselmann/Kuri 2006), das jedoch, da es nicht um Rechte sondern um das Funktionieren selbst geht, tatsächlich wie von Kritikern vorgeschlagen treffender »Digital Restrictions Management« zu nennen wäre.

Fazit

Die zentralen Thesen dieses Textes lauten: Überwachung war in einem weiten Sinne schon immer technisiert. »Technisiert« ist doppeldeutig, es kann auf Überwachungsmittel oder auf Überwachungsobjekte bezogen verstanden werden. Das fällt mehr und mehr zusammen, und das macht das Besondere gegenwärtiger technisierter Überwachung aus: mit technischen Mitteln wird der Einsatz technischer Mittel überwacht. Mehr und mehr wird er aber auch kontrolliert, d.h. die Möglichkeit des Einsatzes selbst wird gesteuert. Gleichzeitig löst sich die klassische Frontstellung des Bürgers gegenüber dem Staat auf: aktuell ist nicht mehr (nur) der Überwachungsstaat, sondern die Überwachungsgesellschaft. Diese ist gekennzeichnet durch eine aktive Rolle der großen Unternehmen, eine freiwillige Preisgabe der Privatsphäre, eine Selbstdemontage des Rechtsstaats im Zuge einer Eskalation der Mittel und Gegenmittel und einer Vernetzung privater, öffentlicher und militärischer Instanzen, die ihre Ressourcen zusammenschalten oder gleich selbst miteinander fusionieren. Die kulturelle Akzeptanz technisierter Überwachung steigt, diejenige technisierter Kontrolle könnte folgen, zumindest lassen sich hierfür Ansatzpunkte ausmachen oder vorstellen.

In der Kontrollgesellschaft wäre nicht mehr die Frage: wer weiß was?, sondern: wer kann was?, oder kurz: was geht? Für Technikaktivisten würde damit eine ausgesprochen spannende Zeit beginnen.

Literatur

ACLU American Civil Liberties Union (2007): Surveillance Milestones: Technology, Policy. http://www.aclu.org/html/surveillance_timeline.html, 10.9.07

Anderson, Ross (2003): 'Trusted Computing' Frequently Asked Questions, http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html, 10.7.06.

Boes, Hans (2005): »An der Schwelle zum automatischen Krieg«, in: telepolis 11.10.2005, http://www.heise.de/tp/r4/artikel/21/21121/1.html, 10.7.06.

Berners-Lee, Tim (2001): W3C Semantic Web Activity http://www.w3.org/2001/sw, 10.7.06.

Foucault, Michel (1974/2001): »La naissance de la médecine sociale«, Vorlesung von 1974, in: ders., Dits et écrits, Bd. 2. Paris, S. 207-228

Gaycken, Sandro (2007): Arguments against surveillance, Vortrag auf dem Chaos Communication Camp 2007, http://events.ccc.de/camp/2007/Fahrplan/attachments/1310-SandroGayckenAgainst....pdf, 16.9.07.

Gieselmann, Hartmut/Kuri, Jürgen (2006): »Mit HDTV zur geschlossenen Kopierschutzkette«, in: *c't* 6/2006, S. 148-152

Gorman, Siobhan (2007): »NSA to defend against hackers. Privacy fears raised as spy agency turns to systems protection«, in: The Baltimore Sun 20.9.2007, http://www.baltimoresun.com/news/nation/balte.nsa20sep20,0,5183239,full.story

Gottschalk-Mazouz, Niels (2007): »Was ist Wissen? Überlegungen zu einem Komplexbegriff an der Schnittstelle von Philosophie und Sozialwissenschaften«, in: Sabine Ammon (Hg.): Wissen in Bewegung. Dominanz, Synergien und Emanzipation in den Praxen der »Wissensgesellschaft«. Weilerswist, S. 21-40.

Gottschalk-Mazouz, Niels (2007): »Internet and the flow of knowledge: which ethical challenges will we face?«, in: Herbert Hrachovec und Alois Pichler (Hg.)*:* Philosophy of the Information Society. Papers of the 30th International Wittgenstein Symposium. Frankfurt usw.: Ontos, (i.E.).

Gutmann, Peter (2006): A Cost Analysis of Windows Vista Content Protection, http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.txt, 10.7.06.

Hubig, Christoph (1993): Technik- und Wissenschaftsethik. Ein Leitfaden, Berlin u.a.

Deutsches Historisches Museum und Haus der Geschichte der Bundesrepublik Deutschland (2000): »Ministerium für Staatssicherheit«. In: Lebendiges virtuelles Museum Online, Berlin und Bonn (http://www.dhm.de/lemo/html/DasGeteilteDeutschland/JahreDesAufbausInOstUnd-West/SEDStaat/ministeriumFuerStaatssicherheit.html, 16.9.07).

Kapp, Ernst (1877): Grundlinien einer Philosophie der Technik. Braunschweig.

McLuhan, Marshall (1964): Understanding Media: The Extensions of Man, NY.

Nakada, Makoto und Tamura, Takanori (2005): «Japanese conceptions of privacy: An intercultural perspective«, In: Ethics and Information Technology 7:27–36.

Rötzer, Florian (2007): »NSA-Programm für die Internetüberwachung kommt nicht voran«, in: telepolis 13.02.2007, http://www.heise.de/tp/r4/artikel/24/24640/1.html, 16.9.07.

Schoen, Seth (2003): Trusted Computing: Promise and Risk, http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php, 10.7.06.

Sharpe, Bill/Hodgson, Tony (2006): Intelligent Infrastructure Futures: Technology Forward Look 2006 (A Report of the Foresight Programme of the Office of Science and Technology, GB), http://www.foresight.gov.uk/Intelligent%20Infrastructure%20Systems/Reports%20and%20Publications/Intelligent_Infrastructure_Futures/Technology_Forward_Look.pdf, 5.5.06.

Stanley, Jay/Steinhardt, Barry (2007): Even Bigger, Even Weaker: The Emerging Surveillance Society: Where Are We Now? New York: The American Civil Liberties Union, http://www.aclu.org/pdfs/privacy/bigger_weaker.pdf

Weber, Max (1980): Wirtschaft und Gesellschaft: Grundriß der verstehenden Soziologie. Fünfte, revidierte Auflage, besorgt von Johannes Winckelmann. Tübingen.

Weiser, Mark (1996): Ubiquitous Computing, 1996 (http://www.ubiq.com/ubicomp/, 5.5. 06). Vgl. auch Mark Weiser: »The Computer for the 21st Century«. In: Scientific American, 1991, S. 94-100 (s. http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html).