Erscheint in U. Richtmeyer (Hg.): *PhantomGesichter: Zur Sicherheit und Unsicherheit im biometrischen Überwachungsbild*, Paderborn: Wilhelm Fink 2014, 73-84.

Werkzeug, Maschine, System. Bemerkungen zu „biometrischen Bildern“ und biometrischer Überwachung aus technikphilosophischer Sicht

Niels Gottschalk-Mazouz

Technik wird häufig verstanden als ein an sich wertneutrales Mittel zu beliebigen Zwecken. Diese Sichtweise ist zu einfach, und das auch schon für vormoderne Techniken. Der Umgang mit Technik sollte vielmehr von einer handlungstheoretischen Schematisierung geleitet werden, die unterschiedliche Typen von Mittel-Zweck-Verhältnissen ausdrücken kann. Werkzeug-, Maschinen- und Systemtechnik zu unterscheiden, wie dies die Technikphilosophie getan hat, hilft hierbei weiter. Ich möchte im Folgenden diese Unterscheidung erläutern und darlegen, wie sich verschiedene Umgangsweisen mit Biometrie in Ihren Varianten diskutieren lassen. Ein besonders kontroverses Einsatzgebiet von Biometrie ist die Überwachung. Deshalb werde ich den Begriff der Überwachung klären und schließlich versuchen, die Spezifika und die Perspektiven biometrischer Überwachung darzulegen.

1. Werkzeug, Maschine, System

Keine Technik ist universell, kein technisches Artefakt kann alles. Mit einem Hammer kann man nicht schrauben, mit einem Schraubenzieher nicht kneifen usw. *Die* Technik als Mittel zu beliebigen Zwecken gibt es nicht. Was es aber gibt, sind mehr oder weniger variable Mittel. *Werkzeuge* sind hochgradig variable Mittel, die der Werkende direkt kontrolliert, die er führt und denen gegenüber er sich darin korrigieren kann, wie er das tut. Anders bei *Maschinen*, die keine ebenso variablen Mittel mehr sind, sondern feste Mittel-Zweck-Zusammenhänge, d.h. Mittel-Zweck-Schemata verkörpern. Variieren lässt sich nur noch, welches Mittel-Zweck-Schema aktiviert wird (z.B. Programmwahl) und welche Randbedingungen vorliegen (z.B. Materialzufuhr). Die am wenigsten variablen Mittel sind die *Systeme*. Denn hierbei geschehen die Auswahl des aktivierten Schemas sowie die Kontrolle der Randbedingungen (sowie vielfach auch die Aktivierung des Schemas selbst) innerhalb des Systems. Die Teile des Systems sind für sich genommen nutzlos, erst zusammen ergeben sie ein Gefüge von zueinanderpassenden Teilen, die bestimmte Funktionen erfüllen. Ein konkretes Artefakt, wie

etwa eine elektrische Nähmaschine, kann dabei durchaus alle drei Aspekte aufweisen, also in bestimmter Hinsicht Maschine sein, in anderer Werkzeug und in wieder anderer Teil eines Systems. Der Maschinencharakter liegt auf der Hand: Es gibt Programme zu wählen und der Benutzer gestaltet die Randbedingungen (legt z. B. Faden und Stoff ein). Doch anders als etwa bei einer Waschmaschine arbeitet der Benutzer mit der Maschine, führt und kontrolliert sie beim Maschinennähen ähnlich wie ein Werkzeug, jedoch im Rahmen des gewählten Zweck-Mittel-Schemas. Schon die normale Nutzung hat also auch Werkzeugcharakter. Doch lässt sich die Nähmaschine auch „zweckentfremden", etwa als Musikinstrument verwenden oder als Stichsäge, was ihr einen noch ausgeprägteren Werkzeugcharakter gäbe. An ihr lassen sich jedoch auch Systemeigenschaften aufweisen: Ohne Strom läuft sie nicht, sie braucht eine bestimmte Art von Nadeln und von Zubehör, und wenn sie Programme von Datenträgern einspielen kann, dann erfordert das ebenfalls eine genau passende weitere Technik. In der folgenden Tabelle, vgl. Hubig/Jelden 1995 und Hubig 2006, sind typische qualitative Unterschiede von Werkzeug-, Maschinen- und Systemtechnik dargestellt:

	Werkzeug	**Maschine**	**System**
Beispiele:	Hammer, Waschbrett	Waschmaschine, mech. Webstuhl	Eisenbahn, Telefon
Artefakt verkörpert:	Variables Mittel	Mittel-Zweck-Schema	Struktur möglicher Mittel und möglicher Zwecke im Rahmen einer Funktionserfüllung
Wirkende Kräfte:	Physische und geistige Kraft des Menschen	Darüber hinaus die physische Kraft der Maschine	Darüber hinaus die „geistige" Kraft der Maschine (Regelung).
Verfügung des Nutzers:	Direkt über den gesamten Prozess	Nur noch über Programm- und Randbedingungenwahl	Nur noch über Einstieg/Ausstieg
Status der Folgen der Verfügung:	Reale Folgen	Hypothetische Folgen	Möglichkeitsspielräume für Werkzeuge und Maschinen
Umgang:	Direkte Kontrolle und Korrektur	Steuerung (Zielauswahl und Schemaaktivierung) sowie kollektiv: indirekte Korrektur	Nutzung/-austritt sowie kollektiv: inkrementelle Modifikation, Standardisierung

2. Biometrische Bilder

In den Anfängen der Fotografie hatte diese Werkzeugcharakter. Die Geräte wurden von Hand bedient und während des Einsatzes (Aufnahme, Entwicklung, Abzug) werkzeugartig geführt. Doch schon zu Zeiten der analogen Fotografie ließ sich eine Tendenz zur Maschinentechnik erkennen, im Zuge derer die einzelnen Schritte automatisiert ablaufen und der Nutzer nur noch Auslöser schematisierter Prozesse ist. Und schon an der klassischen Situation von analoger Fotoausrüstung und eigener Dunkelkammer lässt sich der Systemcharakter der Fotografie erkennen, denn diese funktioniert nur in einem System von Chemikalien, von Film- und Papierproduktion und genau aufeinander abgestimmtem Zubehör. Dennoch kann man der Fotografie insgesamt eher einen Werkzeugcharakter zusprechen, denn die Bildnahme geschieht durch den Fotografen, ist angelegt auf einen menschlichen Betrachter und damit auf deren – prinzipiell offene – Zwecksetzungen bezogen. Biometrische Bilder hingegen sind von vornherein nicht auf einen menschlichen Betrachter, sondern auf weitere technische Artefakte bezogen und das unter einem ganz bestimmten Zweck (eben der Biometrie). Alles ist nicht durch und auf das menschliche Auge hin ausgerichtet, sondern optimiert auf einen fixierten Zweck. Vergleichen wir das kurz mit einem Fotoautomaten und mit herkömmlicher Videoüberwachung. Wie bei der Biometrie auch ist – wenn auch in je unterschiedlicher Weise – der Fotograf aus dem Spiel. Die Bilder sind auf mehr oder weniger fixierte Zwecke bezogen. Doch es bleiben diese Formen von Bildnahme auf menschliche Betrachter bezogen. Genau das ist nun anders bei der Biometrie: Die Aufnahme muss nun nicht nur physisch (wie bei der üblichen Fotografie, also chemisch oder vom Datenformat her), sondern auch inhaltlich systemisch anschlussfähig sein. Denn eine biometrische Erkennung (und teils wird Biometrie mit automatisierter Erkennung von Personen anhand ihrer körperlichen Merkmale in eins gesetzt, vgl. BSI o.J. – dazu gleich noch genauer) erfordert eine automatische Abstraktion (ggf. aus mehreren Bildern) von Merkmalen, deren den Vergleich mit Datenbankbeständen (der „Gallery“) und dann erst eine Signalisierung (an Menschen) oder eine Aktivierung (weiterer Geräte oder Funktionen). Biometrie, und die Bildnahme als Teil von ihr, ist die Aktivierung eines großen Schemas, das algorithmisiert abläuft und Maschinencharakter hat. Doch in Abstraktion, Vergleich und Signalisierung/Aktivierung liegen Verknüpfungen mit anderen maschinellen Prozessen, und zwar auch inhaltliche, so dass Biometrie teils auch als Systemtechnik angesprochen werden kann.

3. Überwachung und Kontrolle

Wie gerade bemerkt wird Biometrie teils mit biometrischer Erkennung gleichgesetzt. Wörtlich genommen bedeutet Biometrie zwar zunächst erst einmal nur die Messung biotischer Eigenschaften, d.h. die Erfassung von biologischen und damit in der Regel natürlichen Merkmalen. Anhand dieser Merkmale nun sollen Personen möglichst eindeutig identifiziert werden. Doch ich glaube, dass der paradigmatische Anwendungskontext damit nur unzureichend beschrieben ist. Denn wozu dient eine solche Messung bzw. Erkennung? Vielfach jedenfalls der Überwachung und der Kontrolle. Ich möchte „Überwachung" hier in einem relativ weiten Sinn verwenden und noch freihalten von negativen oder politischen Konnotationen: *Überwachung* ist die Beobachtung oder Erfassung (von Beobachtungsergebnissen) mit einem Ziel. Und um dieses Ziels willen wird beobachtet oder erfasst. Dieses Ziel nun besteht grob gesagt darin, sicherzustellen, dass bestimmte Dinge passieren oder nicht passieren. Das Ziel der Überwachung liegt daher ganz allgemein gesagt darin, entscheiden zu können, ob eine bestimmte Handlung oder Unterlassung des Überwachenden (oder seiner nachgelagerten Instanzen) erforderlich ist oder nicht. Es ist ein praktisches Ziel, des Überwachenden.

Gegenstand der Überwachung, so wird häufig angenommen, ist eine Person: der Überwachte. Das Modell wäre damit: Person 1 überwacht Person 2. Doch ist das zu einfach gedacht: Denn genau genommen sind es Zustände oder Ereignisse, die überwacht werden, und hier dann oft Zustände von Personen oder Ereignisse, an denen eine Person beteiligt ist – d.h., was diese Person tut oder was ihr widerfährt. Doch noch die Rede davon, einen Zustand zu überwachen, ist elliptisch: Denn man wacht eigentlich darüber, dass ein bestimmtes Ereignis eintritt oder nicht eintritt, dass diesen Zustand ändert oder ändern könnte. Gegenstand der Überwachung sind also, allgemein gesagt, Ereignisse.

Überwachende Instanz, so wird häufig angenommen, ist ebenfalls eine Person. Auch wenn die oben genannten Ziele der Sicherstellung auf Personen und deren Absichten bezogen sind, muss man doch zweierlei bedenken: Erstens muss die Beobachtung nicht unbedingt von einer Person durchgeführt werden. Die Extraktion von (Warn-)Signalen aus dem Beobachteten kann auch von einer Maschine durchgeführt werden (Bsp.: Selbstmordkandidatenidentifikation per Videoüberwachung von U-Bahnsteigen). Zweitens muss auch die auf die Signalisierung folgende Handlung oder Unterlassung, von der oben die Rede war, nicht ausdrücklich von dieser Person (dem „man in the loop") veranlasst werden. Wird sie dies nicht, wäre das ein Schritt von automatisierter Überwachung zu automatisierter

Kontrolle, verstanden als unmittelbarer Sicherstellung dessen, dass das Gewünschte geschieht: Per Intervention in die versuchte Handlung. Die Überwachung eines Zugangs würde bedeuten, dass z.B. ein Alarm ausgelöst wird, wenn jemand, der dies nicht soll, das Tor passiert. Die Kontrolle eines Zugangs würde bedeuten, dass das Tor gar nicht erst aufgeht. Kontrolle bedeutet, allgemein gesagt, damit immer die Ausübung von Macht, verstanden als Bereitstellen oder Verweigern von Handlungsmitteln, d.h. davon, etwas ganz konkret und direkt tun zu können. Zwar kann die Überwachung im Endeffekt etwas Ähnliches leisten wie die Kontrolle, jedoch stets eher indirekt, über mögliche Konsequenzen (und eventuell auch vorauseilenden Gehorsam mit Blick auf diese Konsequenzen) dessen, was man nicht tun soll, das man aber – anders als bei der Kontrolle – sehr wohl tun kann.

Was wir gegenwärtig beobachten können, ist ein Technisierungsschub der Überwachung. Technisierte Überwachung (T-Überwachung) ist eine solche, bei der technische Mittel eingesetzt werden. In einem allgemeinen Sinne wurden sie das schon immer, nun jedoch – durch Informations- und Kommunikationstechnologien – nicht nur, was die Sensorik betrifft, sondern auch, was die Verarbeitung der Sensordaten, ggf. unter Hinzuziehung von Datenbanken, betrifft. Während die Technisierung der Sensorik noch Werkzeugcharakter hat, da sie für verschiedene menschliche Zwecke zumindest des Betrachters offenbleibt, hat die Technisierung der Verarbeitung Maschinencharakter. Hier sind es feste Schemata, die technisch implementiert sind, und diese Schemata sind auf andere Maschinen bezogen (und damit nicht mehr zweckoffen). Die gegenwärtig diskutierte Überwachung ist in genau diesem Sinne eine mehr und mehr technisierte Überwachung (vgl. Gottschalk-Mazouz 2008).

Der Fluchtpunkt solcherart technisierter Überwachung nun aber liegt in technisierter Kontrolle, d.h. in einer automatischen Reaktion auf Überwachungsresultate. Dies liegt nicht nur daran, dass es zu aufwändig oder zu langwierig wäre, die in größerer und größerer Zahl anfallenden Überwachungsergebnisse „von Hand“ auszuwerten und auf diese zu reagieren. Sondern dies liegt ebenso daran, dass auch unsere Handlungen – und damit auch die Gegenstände der Überwachung – mehr und mehr technisiert sind. Wir benutzen technische Artefakte gerade für aufwendige, komplexe Handlungen (Kommunikation, Mobilität) – und diese sind von besonderem Überwachungsinteresse. Diese technischen Artefakte bekommen mehr und mehr systemischen Charakter. Sie sind in ihrem Funktionieren also auf andere Artefakte ausdrücklich angewiesen. Daher lassen sie sich systembedingt nicht nur problemlos anzapfen (=überwachen), sondern auch problemlos blockieren bzw. sperren oder (mglw. verdeckt) aktivieren (=kontrollieren). Das entsprechende Phänomen habe ich TT-

Überwachung genannt: Überwachen kann man, aus Bequemlichkeits- und Praktikabilitätserwägungen heraus, mit technisch hochgerüsteten Mitteln genau diejenigen Handlungsvollzüge besonders gut, die in hohem Maße technisiert sind. In diesen Handlungen, genauer: in den zu ihrer Ausführung eingesetzten Mitteln, finden sich genau die richtigen Ansatzpunkte für eine technisierte Überwachung und Kontrolle. Dies betrifft derzeit schon Telefone, Personal Computer, Autos, Unterhaltungselektronik, mehr und mehr auch den Haushalt („smart home") und andere Bereiche, die die „Smartisierung" erfasst, d.h. in denen unsere Mittel elektronisch gesteuert und miteinander vernetzt werden.

4. Biometrische Überwachung

Was sind nun die Besonderheiten biometrischer Überwachung, und wie lässt sich diese zu anderen Überwachungsarten in Bezeihung setzen? Biometrische Überwachung, wie sie gegenwärtig diskutiert wird, ist ganz offenbar eine Art technisierter Überwachung. Doch was für eine? Die Werkzeug-Maschine-System-Unterscheidung hilft an dieser Stelle nicht weiter. Ich möchte vorschlagen, zwei Arten technisierter Überwachung zu unterscheiden, und zwar nach dem genauen Gegenstand der Überwachung. Oben wurde gesagt, dies seien Ereignisse. Diese Ereignisse lassen sich nun danach unterscheiden, ob sie technisch oder natürlich markiert sind. Die Überwachung technisch markierter Prozesse (t-Überwachung) kann also von der Biometrie als technisierter Überwachung natürlich markierter Prozesse (n-Überwachung) unterschieden werden. Wie wir gleich sehen werden, ist auch das noch etwas zu einfach. Zunächst möchte ich jedoch diese „Markierungen" näher erläutern. Betrachten wir als Beispiel einen Türsteher: Macht der Türsteher eine Gesichtskontrolle, würde er einen Vorgang, den Zugang nämlich, anhand einer natürlichen Markierung überwachen. Lässt sich der Türsteher hingegen eine Einladung oder eine Eintrittskarte zeigen, würde er einen Vorgang anhand einer technischen Markierung überwachen. Auch das Öffnen eines Schlosses mit einem bestimmten Schlüssel wäre ein technisch markierter Prozess: In beiden Fällen sind es keine natürlichen Merkmale von Personen, sondern technische, auf die die Aufmerksamkeit gelegt wird: der passende Schlüssel, die gültige Eintrittskarte.

Biometrische Überwachung nun ziele, so wurde gesagt, auf n-markierte Prozesse. Es wurde auch gesagt, dass Biometrie in der Regel biometrische Erkennung meint (zumindest im Überwachungs- und Kontrollkontext). Eine technisierte biometrische Erkennung nun aber kann sich nicht allein auf n-markierte Prozesse richten. Oben wurde erklärt, dass die

Erkennung von Personen durch den Vergleich natürlicher Merkmale (n-Markierung) mit Inhalten einer Datenbank (der „Gallery“) geschieht, ja: geschehen muss, um funktionieren zu können. Der überwachte Prozess ist also *immer auch t-markiert*. Erst die Kombination beider Markierungen, die Passung, leistet das Gewünschte. Ein biometrisches System arbeitet hier genauso, wie es auch der Beamte tun würde, der bei der Einreise eine Passkontrolle vornimmt: Sowohl natürliche (Gesicht) als auch technische Merkmale (Pass mit Passfoto) zusammen markieren den Prozess, der überwacht werden soll, d.h. das Passieren der Grenze. Biometrische Überwachung richtet sich also im Kern auf tn-markierte Prozesse.

5. Technisierungsgrade

Die Technisierung der Überwachung kann, um das Bisherige zusammenzufassen, sich in drei Dimensionen vollziehen. Sie kann sich auf die *Überwachungsmittel* beziehen, auf die *Markierung* des zu überwachenden Ereignisses und auf die einbettende Ereigniskette, d.h. die *Handlung* des Überwachten. In jeder dieser drei Dimensionen ist sie eine Frage des Grades. Die folgende Tabelle verdeutlicht das am Beispiel der Überwachung des Verhaltens an einer roten Verkehrsampel.

	Überwachungsmittel	**Markierung**	**Überwachte Handlung**
Niedriger Technisierungs-grad	Polizist beobachtet den Verkehr und wertet aus	Mensch x läuft/fährt über Rot	Laufen zu Fuß
Mittlerer Technisierungs-grad	Blitzer fotografiert und Polizist wertet aus.	Jemand mit einem Fahrrad der Marke a fährt über Rot	Fahrradfahren
Hoher Technisierungs-grad	Blitzer fotografiert und Computer wertet aus (erkennt ggf. Nummernschild, verschickt Bußgeldbescheid)	Auto y fährt über Rot, Jemand mit dem Handy z läuft über Rot	Autofahren

Man beachte, dass der Vorgang des Bei-Rot-die-Straße-Überquerens an sich schon eine technische Markierung enthält, die durch das „Bei Rot“ angezeigt wird, nämlich das Rotlicht der Ampel. Möglich wird das dadurch, dass die überwachte Handlung selbst in einem

technisierten *Handlungskontext* vorgestellt wird, nämlich als eine Handlung an einer Verkehrsampel. Notwendig ist dies aber nicht, man könnte die obenstehende Tabelle auch angesichts der Überwachung des Einhaltens der Vorfahrtregeln entwickeln.

Typisch für die Biometrie nun scheint mir ein hoher Grad der Technisierung der Überwachungsmittel, des Handlungskontexts sowie der Markierung des zu überwachenden Ereignisses – das gleichzeitig t- wie n-markiert wird, aber damit eben auch t-markiert – zu sein. Die überwachte Handlung hingegen ist typischerweise nicht in gleichem Maße technisiert. Allerdings gibt es eine wichtige Ausnahme, auf die ich gleich noch zu sprechen komme, nämlich die Zugangskontrolle. Zunächst aber ergibt sich folgendes Bild: Während mithilfe der Technisierung der Überwachungsmittel allein (oben T-Überwachung genannt, bzw. dann, wenn auch die Handlung technisiert ist, TT-Überwachung) das *Was*, *Wie*, *Wann* usw. des fraglichen Ereignisses genau bestimmen kann, muss das *Wer* prinzipbedingt offen bleiben. Genau die Bestimmung des *Wer* leistet die Biometrie – und nur die Biometrie, so scheint es, denn nur sie erlaubt es, n-Markierungen zu verwenden.

6. Perspektiven

Genau die Bestimmung des *Wer* leistet also die Biometrie – doch wirklich nur die Biometrie? Und wohin führt biometrische Überwachung? Ich möchte abschließend dafür argumentieren, dass die Biometrie in zentralen Bereichen der *Wer*-Bestimmung Konkurrenz bekommt. Und ich möchte dafür argumentieren, dass der biometrischen Überwachung eine verstärkende Funktion zukommen könnte auf dem Weg von einer technisierten Überwachung zu einer technisierten Kontrolle.

Tatsächlich dürfte in sicherheitskritischen Bereichen die n-Markierung ein prinzipieller Vorteil sein (obwohl auch biometrische Systeme nicht unfehlbar sind bzw. sich gezielt täuschen lassen, siehe Kramer 2009 und Starbug 2004/2007). Doch wird es in vielen Bereichen gar nicht um solche vergleichsweise hohen Standards gehen, genauer: immer dann nicht, wenn sich die Überwachung (wie in allen Big-Brother-Szenarien) nicht ausschließlich auf einzelne Personen richtet, denen eine hohe kriminelle Energie unterstellt werden kann. In solchen Bereichen zumindest eröffnet sich zur Bestimmung des *Wer* auch eine andere, möglicherweise elegantere Möglichkeit der technisierten Überwachung ohne Biometrie: Im Zuge der Individualisierung und Kennzeichnung einzelner Gegenstände (bis hin zur Auszeichnung auch noch der passiven Gegenstände mit RFID-Funketiketten) ist eine

Situation, in der der Einsatz oder der Besitz bestimmter technischer Artefakte normalerweise eineindeutig an bestimmte Personen gebunden ist, keine Zukunftsmusik mehr. Nicht allein die Kombination bestimmter Artefakte oder technisierter Handlungen kennzeichnet dann die Person (auch das schon funktioniert manchmal recht gut, siehe die Rasterfahndung), sondern mehr und mehr auch die Kombination bestimmter personalisierter Artefakte (mit einer auslesbaren Seriennummer, MAC-Adresse, IMEI, Rufnummer, DSL-Portadresse usw. usw.). Dann lässt sich auch das *Wer* mit hinreichend guter Trefferquote allein über solche anhand des Besitzes oder des Einsatzes dieser Artefakte möglichen *massiven t-Markierungen* ausmachen. Vorsätzlich lassen sich diese Zuordnungen natürlich noch immer leichter verändern, als sich biologische Merkmale verändern lassen, und damit Identitäten fingieren oder verschleiern. Zumindest in nicht sicherheitskritischen Bereichen jedoch werden, so meine These, tn-markierende mit massiv t-markierenden Überwachungen konkurrieren.

Steigt die Technisierung der Überwachungsmittel sowie des Handlungskontextes (wie bei der Biometrie) und auch die Technisierung der zu überwachenden Handlungen, ist eine Verlängerung der technisierten Überwachung hinein in eine technisierte Kontrolle sehr naheliegend. Wenn es jedoch in der Logik der technisierten Überwachung liegt, zu technisierter Kontrolle fortzuschreiten, dann gilt das für die biometrische Überwachung erst recht. Dies nun aber nicht so sehr, weil nur die massenhafte Identifikation von Personen zuließe: Denn dass das auch über massive t-Markierungen möglich ist, wurde gerade ausgeführt. Der Grund ist vielmehr, dass die Biometrie typischerweise bereits jetzt in beiden Kontexten propagiert wird, also gewissermaßen in beiden Kontexten zuhause ist: Dem der Überwachung sowie dem der Kontrolle. Schon jetzt werden Fingerabdruckscanner in vielen Laptops verkauft, sind es vielfach Zugangs*kontrollen*, in genau dem oben ausgeführten Sinne der Gewährung oder der Verweigerung einer Handlungsausführung, die die intendierten Anwendungen der Biometrie ausmachen. Die Biometrie könnte also ein Katalysator sein der Entwicklung einer technisierten Überwachung, die mit technisierter Kontrolle Hand in Hand geht – und zugleich zu einem Brennpunkt entsprechender Debatten darüber werden, in welchem Maße so etwas wünschenswert ist.

Literatur

BSI - Bundesamt für Sicherheit in der Informationstechnik (o.J.): Biometrie – Übersicht. http://www.bsi.bund.de/fachthem/biometrie/index.htm vom 7.6.09

Gottschalk-Mazouz, N. (2008): „Die Spezifik technisierter Überwachung: Überlegungen zu Überwachung und Macht aus technikphilosophischer Sicht“. In: Gaycken, S.; Kurz, C. (Hg.): 1984.exe - Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, Bielefeld: Transcript, S. 209-230.

Hubig, Ch.; Jelden, E. (1995): „Werkzeuge, Maschinen und Systeme: Leben in der Technik.“ In: DIFF (Hg.): *Funkkolleg Technik: Einschätzen - Beurteilen - Bewerten. Studienbrief 1 (STE 1)*. Weinheim: Beltz Quadriga, S. 4-38.

Hubig, Ch. (2006): *Die Kunst des Möglichen, Bd. I: Technikphilosophie als Reflexion der Medialität*. Bielefeld: Transcript.

Kramer, A. (2009): „Unsichtbare Augen. Gesichtserkennung zu Hause, im Web und in der Öffentlichkeit“. In: *c't*, S. 82-87

Starbug (2004/2007): Hacking biometric systems“. In: Datenschleuder Nr. 84 (2004), online unter http://chaosradio.ccc.de/media/ds/ds084.pdf vom 7.6.09; vgl. auch seinen Vortrag auf der HITB in Malaysia (2007), http://video.google.com/videoplay?docid=-6545371437568517262