Manu Luksch, Mukul Patel

Faceless: Die Jagd nach Datenschatten

Seltsamer als jede Fiktion

Ferngesteuerte unbemannte Luftfahrzeuge überfliegen die Stadt auf der Suche nach unsozialem Verhalten. Sprechende Kameras rufen (mit Kinderstimmen) Menschen, die Abfälle auf die Straßen werfen, zur Ordnung. Bildern aus Videoüberwachungsanlagen werden biometrische Daten entnommen, um Passanten über ihr Gesicht oder ihren Gang zu identifizieren. Die Überwachungskameras einer Wohnanlage versorgen den lokalen Kabelkanal mit Bildern und ermöglichen den Bewohnern, sich selbst zu kontrollieren.
Dies sind keine Szenen aus dem Science-Fiction-Film, der Thema dieses Textes ist, sondern Techniken, die heute in Merseyside, Middlesborough, Newham und Shoreditch (GB) zum Einsatz kommen.

Plakat in London

Großbritannien ist heute führend, was die Dichtheit und Raffinesse der Überwachungstechnologien anbelangt. Mit einer geschätzten Anzahl von 4,2 Millionen CCTV-Kameras sind die Einwohner Großbritanniens die meist beobachteten der Welt. *(A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network2,* September, 2006, S. 19. Zu beziehen über http://www.ico.gov.uk). Viele Londoner Busse sind im Inneren mit fünf oder mehr Kameras bestückt, weitere sind außen angebracht, wobei eine die Autos aufnimmt, die die Busspur benützen.
Doch die Bilder der Überwachungskameras sind nur eine der vielen Datenspuren, die wir – freiwillig oder unfreiwillig – hinterlassen. Unsere Autofahrten werden mittels ANPR-Systemen aufgezeichnet, dank der *Location awareness* der Endgeräte (wie etwa Mobiltelefone) werden unsere Bewegungen registriert, die Spuren unserer Online-Aktivitäten von Internetdienstanbietern aufgezeichnet, unsere Gespräche von Echelon abgehört, Einkaufsgewohnheiten per Kundenkarten überwacht, individuelle Einkäufe über RFID-Kennungen *(Radio Frequency Identification,* Identifizierung über Radiowellen) und unsere Ernährungsgewohnheiten mit den Fluggastdaten erfasst. Unsere digitalen Alter Egos sind mehrdimensional, wachsam und vergessen nie etwas.
Diese Datenspuren werden zunehmend in global vernetzten Datenbanken gehortet und verwaltet. Man muss nicht unbedingt eine totalitäre Verschwörung hinter dieser Datenakkumulation vermuten – die Auswertung von Daten ist sowohl ein Erfordernis der Markteffizienz als auch der bürokratischen Rationalität. Über die „Überwachungsgesellschaft" und die „kontrollierte Gesellschaft" wurde bereits viel geschrieben, und es ist nicht unsere Absicht, in diesem Rahmen, eine allgemeine Kritik von Datensammlung, -vorratsspeicherung und -analyse zu leisten. Doch dürfen wir nicht die Augen davor verschließen, dass im Namen von Effizienz und Rationalität – und natürlich der Sicherheit – eine ständige wachsende Datenmenge zwischen den Hütern scheinbar nicht vernetzter Aufzeichnungen wie Krankengeschichten, Einkaufsgewohnheiten und Grenzübertritten ausgetauscht wird. Es gibt gesetzliche Rahmenbedingungen zum Schutz der Privatheit, die Datentransfers auf die zugehörigen Parteien beschränken. Es sind diese Gesetze und insbesondere das britische Datenschutzgesetz (DPA, 1998), die der Films *Faceless* durch seine Machart untersucht.

Vom Gesetz zum Manifest

Ich möchte gemäß DPA 1998 *sämtliche Videobilder meiner Person, die von Ihrer Videoüberwachungsanlage aufgezeichnet wurden, beantragen. Ich war am [Datum] um [Zeit] in [Ort] anwesend.*
(Aus dem für Faceless *verwendeten Vordruck „Antrag eines Betroffenen um Zugriff auf Videodaten")*

Unter dem Namen „ambientTV.NET" betrieb Manu Luksch mehrere Jahre lang eine Reihe von Workshops zur Visualisierung von Datenspuren, um diese in dramatisierter Weise erfahrbar zu machen und „jene zu beobachten, die uns beobachten". Diese Experimente, in denen die Grenze zwischen Öffentlichkeit und Privatheit im Alltagsleben nach 9/11 eingehend untersucht wurde, liefen unter dem Titel *The Spy School*. Im Jahr 2002 wurde in *The Spy School* ein Experiment durchgeführt, um die Wirksamkeit des *UK Data Protection Act* in Bezug auf CCTV-Bilddaten zu testen.

Der Data Protection Act 1998 *versucht, eine Balance zwischen den Rechten des Einzelnen und den mitunter konkurrierenden Interessen jener herzustellen, die legitime Gründe haben, personenbezogene Daten zu verwenden.*
Der DPA gesteht Einzelpersonen gewisse Rechte hinsichtlich der über sie gesammelten Daten zu. Er erlegt jenen, die Daten verarbeiten (den verantwortlichen Stellen) Verpflichtungen auf, während er jenen, deren Datenprofil erstellt wird (Betroffenen) Rechte zugesteht. Personenbezogene Informationen umfassen sowohl Fakten als auch Meinungen über Einzelpersonen.
(Der Gesetzesauszug zum DPA ist über das UK Information Commissioner's Office *(ICO) zu beziehen, www.ico.gov.uk.)*

Der DPA (1984) wurde ursprünglich ausgearbeitet, um den Zugang zu computerisierten personenbezogenen Daten, wie etwa medizinischen und buchhalterischen Aufzeichnungen, zu ermöglichen und zu regulieren. Durch eine spätere EU-Richtlinie wurden der Datenschutz und der Aufgabenbereich des DPA (1998) auf Aufzeichnungen von Videoüberwachungsanlagen ausgedehnt. Abgesehen vom DPA müssen Betreiber von Videoüberwachungsanlagen weitere Gesetze erfüllen, die sich auf die Menschenrechte, das Recht auf Privatheit und kriminalpolizeiliche Ermittlungen, wie sie im *CCTV Code of Practice (www.ico.gov.uk)* festgelegt sind, beziehen.
Als die ersten Anträge für Zugriff auf Videodaten insofern erfolgreich waren, als CCTV-Aufzeichnungen für *The Spy School* freigegeben wurden, stellte sich die Frage, wie stabil die gesetzlichen Rahmenbedingungen denn waren. Das *Manifest für CCTV-Filmemacher* wurde verfasst, demzufolge lediglich die Verwendung von Aufzeichnungen gestattet ist, die mithilfe des DPA erlangt wurden. Das Gesetz sollte mit den Mitteln der Kunst überprüft werden.

Ein gesetzliches Readymade

Undeutliche Schreckgespenster einer Bedrohung, die über zeitkodierte Überwachungskameras festgehalten wurden, rechtfertigen ein umfassendes Netz voyeuristischer Kameralinsen. Ein Netz teilnahmsloser Beobachtungsgeräte, die jede Straße, jedes Gebäude abtasten, um die Möglichkeit einer Vergangenheit, die freie Wahl, etwas zu vergessen, auszuschalten. Glanzpunkte, besondere Augenblicke kann es nicht mehr geben: Eine diskrete Tyrannei des „Jetzt" ist im Entstehen. „Realzeit" in ihrer pedantischsten Ausprägung.
Sinclair, Ian: *Lights out for the territory*, Granta, London 1998, S. 91

Faceless ist ein CCTV-Sciencefiction-Märchen, das in London, der Stadt mit der weltweit größten Dichte an Überwachungskameras, spielt. Der Film wurde nach den Vorgaben des Manifests gedreht – die Bilder stammen aus bestehenden CCTV-Systemen und wurden eingeholt, indem die Regisseurin/Protagonistin ihre Rechte als „überwachte Person" gemäß DPA wahrnahm.

Begreiflicherweise ist die Protagonistin in jedem Bild präsent. Durch die gesetzlichen Auflagen zum Schutz der Privatheit sind die CCTV-Betreiber dazu verpflichtet, dafür zu sorgen, dass keine andere Person in den Aufzeichnungen identifizierbar ist – im Allgemeinen erfüllen sie diese Anforderung, indem sie deren Gesichter unkenntlich machen. Dies erklärt die „gesichtslose" Welt des Films. Das Drehbuch von *Faceless* lässt sich somit auf die gesetzlichen Vorschriften für Bilder aus Videoüberwachungsanlagen zurückführen.

EchtZeit bestimmt das Leben aller Bewohner.
Arbeiten, ruhen, essen, heiraten – jede Handlung passiert im Takt der EchtZeit.
Und jede Handlung hinterlässt eine Spur – einen Fußabdruck am Strand des Daten-Meeres.
Faceless, 2007

Der Film spielt in einer geradezu unheimlich vertrauten Stadt, in der ein neu eingeführter Echtzeitkalender Vergangenheit und Zukunft abschafft, wodurch die Bürger von Schuld, Bedauern, und Zukunftsangst befreit sind. Ohne Gedächtnis oder Erwartung verblassten die Gesichtszüge und wurde die Bevölkerung sprichwörtlich gesichtslos. Eine Zeit unvorstellbaren Glücks beginnt – bis eine Frau ihr Gesicht wiedererlangt ...
Es gab kein Drehbuch im herkömmlichen Sinn: Der Plot entwickelte sich während des vierjährigen Prozesses der Bilderlangung. Szenen wurden zwar für bestimmte Orte geplant, doch waren die Aufzeichnungen aus der Videoüberwachung nicht immer erhältlich, weshalb die Geschichte ständig umgeschrieben werden musste.


Standbild aus *Faceless,* 2007

Faceless beschreibt das CCTV-Bild als Beispiel für ein rechtliches Readymade *(objet trouvé).* Das Medium, im Sinne eines „Rohmaterials, das Kunst wird", ist nicht einfach als Video oder fixiertes Licht adäquat zu beschreiben. Genauer gesagt, besteht das Medium aus Bildern, die kontingent unter bestimmten gesellschaftlichen und gesetzlichen Bedingungen existieren – im Wesentlichen aus Bildern mit einem rechtlichen Überbau. Der Film *Faceless* hinterfragt die Gesetze, die die Videoüberwachung der Gesellschaft regeln, sowie die Kommunikationscodes, die ihre Umsetzung bestimmen, und ist sowohl durch seine eine Entstehungsweise als auch durch sein Plot eine Form von Kritik.

Die Einforderung des Datenprofils

Da der DPA über einen langen Zeitraum hinweg angewendet und seine Auswirkungen beobachtet wurden, konnten Veränderungen des Gesetzes, seine Stärken und Schwächen im Detail aufgezeigt werden.

Ich kann bestätigen, dass es keine Aufzeichnungen von Ihnen für diesen Zeitpunkt gibt, unser Aufzeichnungssystem war zu dieser Zeit nicht in Betrieb. (11/2003)

Viele Datenanfragen wurden negativ beantwortet, weil entweder die betroffene Überwachungskamera oder das Aufnahmegerät oder das gesamte CCTV-System nicht funktionstüchtig war. Dies kommt einer illegalen Verwendung der Videoüberwachungsanlage gleich: Das Gesetz schreibt vor, dass Betreiber dem DPA Folge zu leisten heben, indem sie dafür sorgen, dass [...] die Geräte funktionieren.
(CCTV Systems and the Data Protection Act 1998, zu beziehen über http://www.ico.gov.uk)

Mehrfache, widersprüchliche Zeitstempel

In einigen Fällen bemerkten die Betreiber erst als ein Antrag gestellt wurde, dass das System nicht funktioniert. Im folgenden Fall war das CCTV-System erst zwei Jahre vor der Anfrage installiert worden.

Nach Erhalt Ihres Schreibens [...] und der erforderlichen Gebühr von 10 £ habe ich eine Firma zur Bearbeitung dieser Bänder gesucht, um die Privatheit anderer Personen, die der Freigabe nicht zustimmten, zu schützen. [...] Man teilte mir mit, [...] dass alle Bänder leer wären. [...A]ls der Techniker beigezogen wurde, bestätigte er, dass das Gerät seit seiner Installation nicht in Betrieb war.
Wir bedauern, dass wir in dieser Angelegenheit nichts für Sie tun können und ersuchen Sie um Nachsicht für die Unannehmlichkeiten, die Sie hatten. (11/2003)

Technische Ausfälle dieser Größenordnung waren gang und gäbe. Auch grobes menschliches Versagen wurde bereitwillig eingestanden:

> *Wie ich Ihnen in meinem vorangegangenen Schreiben mitteilte, haben wir beantragt, das Videoband zu entnehmen, damit es nicht gelöscht wird. Bedauerlicherweise wurde diesem Ansuchen nicht Folge geleistet und das Band wurde gemäß der bei [Name unkenntlich gemacht] üblichen Bandspeicherungsvorgabe gelöscht. Ich ersuche um Nachsicht und versichere Ihnen, dass Schritte unternommen wurden, um in Zukunft derartige Fehler zu vermeiden. (10/2003)*

Einige Antworten, wie etwa die folgende, kann man nur als mysteriös bezeichnen (Datenanfrage nach einstündigem Aufenthalt vor mehreren Kameras, die an einem Zugabteil angebracht waren).

Wir haben alle relevanten Bänder sorgfältig geprüft und versichern Ihnen, dass wir über keine Bilder von Ihnen verfügen. (06/2005)

Ist eine solche Verleugnung von Tatsachen möglicherweise nur ein Vorwand, um die kostspieligen Auflagen des DPA nicht erfüllen zu müssen? Viele ältere Kameras liefern derartig schlechte Bilder, dass kein einziges Gesicht erkennbar ist. Auch in solchen Fällen erfüllt der CCTV-Betreiber seine gesetzmässig verankerten Verpflichtungen nicht.

> *Sie werden bemerken, dass die Gesichter von Ihnen und Ihrem Kollegen in dem Video ziemlich undeutlich sind. Auf dem Bild, das Sie uns schickten, tragen Sie jedoch einen ähnlichen Pelzmantel, sodass wir Sie hauptsächlich durch diesen Pelzmantel und Ihre Ortsangabe identifizieren konnten.*

Daten, die auf Basis so vager Angaben ermittelt werden, dürften ebenfalls nicht freigegeben werden.
Die Verpflichtung, die Privatsphäre abgebildeter Dritter zu schützen, stiftete große Verwirrung. Das führte mehrmals dazu, dass Betreiber sich der Pflicht, Bildinformation zugänglich zu machen, enthoben glaubten.

Der Rotakin-Test, der von der Home Office Police Scientific Development Branch (GB) entwickelt wurde, misst die Effizienz einer Überwachungskamera.

> *[…W]ir können Ihnen die angeforderten Bilder nicht aushändigen, da ansonsten Informationen über und Bilder von anderen Personen, die auf der Videokassette identifizierbar sind, preisgegeben würden. Es ist uns leider nicht möglich, deren Zustimmung zur Herausgabe der Bilder einzuholen. Außerdem ist uns unmöglich, die anderen Bildinformationen herauszulöschen. Ich verweise auf den Abschnitt 7 des* Data Protection Act 1998 *und insbesondere auf Abschnitt 7 (4) (11/2003).*

Obwohl in dem Abschnitt betont wird, dass dies

> *nicht so auszulegen sei, dass es den Betreiber von der Verpflichtung entbindet, soviel der angesuchten Information wie möglich weiterzuvermitteln, ohne dabei die Identität von Dritten, sei es namentlich oder durch andere indentifizierbare Besonderheiten preiszugeben.*

Im Fall von Video ist die Anonymisierung Dritter ein kostspieliges, aufwändiges Verfahren – eine weitverbreitete Methode besteht darin, jeden Kopf durch ein schwarzes Oval abzudecken.
Es darf nur die gesetzlich vorgeschriebene Höchstsumme von £10 pro Anfrage verrechnet werden, obwohl das nicht alle zu wissen schienen:

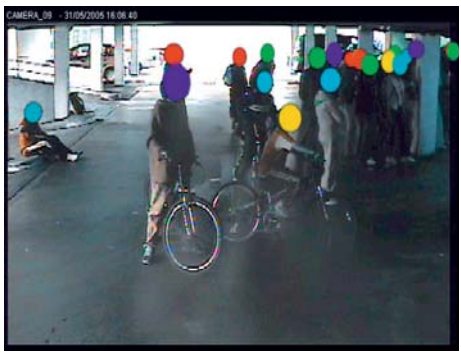
> *Wir gingen davon aus, dass die Kosten für die Nachbearbeitung des Videos von der ansuchenden Person übernommen werden, wobei wir diesen Punkt natürlich noch überprüfen werden. In der Zwischenzeit übermitteln wir Ihnen das Videoband mit den besten Grüßen von [Firmenname unkenntlich gemacht] – und zwar gebührenfrei. (07/2002)*

Die visuell provokanten und symbolisch aufgeladenen, unkenntlich gemachten Köpfe garantieren nicht unbedingt Anonymität. Das Ausschwärzen eines Gesichts kann unzureichend sein, wenn die Drittperson demjenigen, der die Bilder anfordert, bekannt ist. Nur ein CCTV-Betreiber hat die richtige Massnahme zum Schutz der Privatheit Dritter angewendet und die elegante Lösung gefunden den Antragsteller mit einer Negativmaske zu versehen („Schlüssellochmaske"), die alles ausser den erkennbaren Betroffenen abdeckte. (Es handelt sich dabei um ein vom Betreiber ohne Kommentar übermitteltes zweites Band, nachdem das erste völlig unbearbeitet ausgehändigt worden war.)

Ein CCTV-Betreiber entdeckte eine opportune Gesetzeslücke im DPA:

> *Ich sollte darauf hinweisen, dass wir uns – gemäß Abschnitt 8(2) des Data Protection Act – das Recht vorbehalten, Ihnen keine Kopien der angeforderten Daten zu übermitteln, wenn dies einen „unverhältnismäßigen Aufwand" impliziert. (12/2004)*

Was gilt als „unverhältnismäßiger Aufwand"? Alle Rekorde diesbezüglich schlug eine Institution, deren Vorgangsweise fast als barock bezeichnet werden kann – hunderte von relevanten Einzelbildern der Zeitrafferaufnahmen wurden auf Papier ausgedruckt und die Köpfe der Drittpersonen waren allem Anschein nach mit Nagelscheren ausgeschnitten worden.
Zwei Dokumente waren (zufällig?) zwischen die Ausdrucke gerutscht – das eine war ein Brief einer jungen Angestelltengehilfin, die ihre Kündigung einreichte (besteht womöglich ein Zusammenhang mit dem Job, Köpfe auszuschneiden?), und das andere eine ironische Notiz:



Standbild aus *Faceless*, 2007

> *Und die erfreuliche Nachricht – ich lege die Gebühr von £ 10 bei, damit sie auf das Konto Verschiedenes überwiesen werden kann (Sicherheitschef, interne Kommunikation 09/2003).*

Ab 2004 wurde das Verfahren, Bilder einzufordern, erheblich schwieriger.

> *Aus Ihrem Brief geht hervor, dass Sie die Bestimmungen des* Data Protection Act *kennen, daher bin ich sicher, dass Sie auch über die Richtlinien des jüngsten Entscheids des Berufungsgerichts im Fall* Durant *versus* Financial Services Authority *informiert sind. Meiner Ansicht nach fällt das von Ihnen verlangte Filmmaterial nicht unter „persönliche Daten", weshalb wir [Name unkennlich gemacht] Ihnen das angeforderte Filmmaterial nicht aushändigen werden. (12/2004)*

Im britischen Rechtssystem, das auf dem Gewohnheitsrecht basiert, haben Urteile Präzedenzcharakter. Die Entscheidung im Fall Durant versus Financial Service Authority (Finanzdienstleistungsbehörde; 2003) hat den Begriff „personenbezogene Daten" neu definiert; seither hat ein Betroffener nicht mehr das Recht, Kopien der Aufzeichnungen zu erhalten, nur weil er auf den Originalaufnahmen zu sehen ist. Dieses Recht hat er nur, wenn Informationen „biografischer Art" preisgegeben werden.

> *Nach sorgfältiger Erwägung der Angelegenheit glauben wir nicht, dass die Informationen, über die wir verfügen, die nötige Relevanz für Sie haben. Demgemäß glauben wir nicht, dass wir verpflichtet sind, Ihnen entsprechend des* Data Protection Act 1998 *eine Kopie auszuhändigen. Insbesondere möchten wir anmerken, dass das Video keine in irgendeiner Weise aussagekräftigen biografischen Details von Ihnen enthält. (11/2004)*

Weiters liegt seit der Einführung von Schwenks und Zoomfunktionen keine ausreichende Begründung für eine Datenanforderung vor, wenn man mit einer statischen Kamera etwa inmitten einer Menschenmenge gefilmt wurde.

> *[D]as Information Commissioner's Office bezeugte, dass es sich in diesem Fall nicht um personenbezogene Daten handelt, da das System eingerichtet wurde, um ein Gebiet und nicht eine Einzelperson zu überwachen. (09/2005)*

Während die Sensibilität der Öffentlichkeit in Bezug auf Datenrechte ansteigt, wird die Durchsetzung derselben immer schwieriger:

> *Ich verweise auf den Text „CCTV Systems and the Data Protection Act 1998 (DPA) Guidance Note on when the Act applies". Diesem Dokument zufolge fällt unser Videoüberwachungssystem nicht länger unter den DPA, [weil] wir:*
> - *nur einige Kameras haben;*
> - *diese nicht fernbedienen können;*
> - *nur auf Video aufnehmen, was zufällig in das Blickfeld der Kamera kommt;*
> - *die Aufnahmen lediglich der Polizei zur Untersuchung von Vorfällen auf unserem Gelände aushändigen. (05/2004)*

Auch die Zeitspanne der Datenvorratsspeicherung (die von den verantwortlichen Stellen selbst definiert wird) ist für den CCTV-Filmemacher oft ein Unsicherheitsfaktor:

> *Besten Dank für Ihr an unser Geschäft in Newcastle adressiertes Schreiben vom 9. November, das an mich weitergeleitet wurde. Bedauerlicherweise erhielt ich den Brief durch eine Verzögerung auf dem Postweg erst diese Woche. [...] Es befanden sich keine der von Ihnen angeforderten Bilder auf den Videobändern, die Anlass gegeben hätten, die Videobänder über den üblichen Speicherungszeitraum hinaus aufzubewahren, weshalb das Filmmaterial der Videoüberwachungsaufnahmen vom 28. Oktober und 2. November nicht mehr verfügbar ist. (12/2004)*

Inmitten dieser Litanei an Ausreden wegen nicht funktionierender technischer Ausstattung, gelöschter Bänder, verlorener Briefe oder reinen Ausflüchten brachte ein CCTV-Betreiber eine vernünftige Rechtfertigung hervor, warum er keine Bilder liefern konnte:

> *Wir können Ihnen nicht mitteilen, ob wir im [unkennlich gemacht] Bilder von Ihnen aufnahmen. Die Bänder für den gewünschten Zeitraum wurden bereits vor Erhalt Ihrer Anfrage der Polizei übergeben, um deren Untersuchungen verschiedener Aktivitäten am [unkennlich gemacht] während des Karnevals zu unterstützen. (10/2003)*

Im Schatten des Schattens

Man diskutiert über Effizienz, Kosten-Nutzen-Rechnung, Qualität der Ausführung, politische Legitimität und kulturelle Auswirkungen der CCTV-Systeme in Großbritannien. Während Videoüberwachung bei der Lösung einiger Fälle, die grosse Beachtung in den Medien fanden, eine wesentliche Rolle spielten (z. B. 1999 beim Fall des Londoner Nagelbombers oder 1993 im Mordfall von James Bulgur), erwiesen sie sich in anderen Fällen als seltsam nutzlos (z.B. 2005 als Jean Charles de Menezes von der Polizei ermordet wurde). Die eifrigsten Verfechter der Videoüberwachungn scheinen bereits ihren Glauben an dieses Allheilzweckmittel verloren zu haben. In den 1990er Jahren investierte das britische Innenministerium 78 % des Präventivbudgets gegen Kriminalität in CCTV. In einem Evaluationsbericht aus dem Jahr 2005 kam dieselbe Stelle zu dem Schluss, dass

> *die bewerteten CCTV-Modelle wenig Auswirkung auf die Kriminalitätsrate hatten.*
> (Gill, M. und Spriggs, A.: *Assessing the impact of CCTV,* Home Office Research, Development and Statistics Directorate, London 2005, S. 60–61)

Standbild aus *Faceless,* 2007

Die öffentliche Wahrnehmung sieht anders aus. Überwiegend ist die Öffentlichkeit positiv eingestellt, obwohl in jüngerer Zeit Bedenken über Zweckentfremdung laut wurden (ausgelöst beispielsweise durch die Enthüllung, dass die Kameras, die in London die Bezahlung der Innenstadtmaut überwachen, auch außerhalb der gebührenpflichtigen Zeit eingeschaltet bleiben). Das Vertrauen in die Technologie ist zwar nach wie vor hoch, könnte aber schwinden, sollten die tatsächlichen Umstände des täglichen Betriebs bekannter werden.
Physische Körper hinterlassen Datenspuren: Schatten der Anwesenheit, der Gespräche, der Bewegung. Vernetzte Datenbanken verdichten diese Spuren zu einem „Datenkörper", dessen Verhalten und Risiko Hauptgegenstand von Analysen sind (seitens der Wirtschaft und der Regierung). Die Sicherstellung eines „Datenkörpers" ist angeblich notwendig, um den menschlichen Körper zu schützen (entweder präventiv oder als forensisches Hilfsmittel). Wenn Ersteres nicht überzeugend gewährleistet werden kann, warum sollte man daran glauben, dass Letzteres funktioniert?
Das panoptische System ist (noch) nicht komplett. Es stellt sich aber die dringende Frage: Kann der einseitige Blick jemals als Grundlage eines Sicherheitskonzeptes dienen, das vorgibt, die Betroffenen zu bevollmächtigen, sie zur Mitverantwortlung und Teilnahme aufzufordern?

Aus dem Englischen von Martina Bauer

Der vollständige Text des DPA (1998) ist zu beziehen über *www.opsi.gov.uk/ACTS/acts1998/19980029.htm*