Die Überwachungsgesellschaft existiert bereits

Im Juni 2006 beauftragte der britische Datenschutzbeauftragte Richard Thomas das Surveillance Studies Network mit der Erstellung eines Berichts zu der Problematik des Überwachens. Das Dokument wurde im November 2006 auf der Londoner Datenschutzkonferenz vorgestellt. Es handelt sich also um ein offizielles Dokument. Umso bemerkenswerter sind die alarmierenden Schlussfolgerungen zu denen die Studie gekommen ist. forum zitiert im Folgenden einige Auszüge aus der Studie.

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

Die Überwachung wächst im Einklang mit dem modernen Zeitalter. Wenn wir die Überwachungsgesellschaft als Produkt der Moderne erkennen, lassen sich gleich zwei Fallen vermeiden: Erstens gehört Überwachung nicht zu den üblen Machenschaften fragwürdiger Bösewichter und zweitens erwächst Überwachung nicht ausschließlich aus neu erfundenen Technologien (ganz Paranoide glauben natürlich, dass diese beiden Gedankengänge zusammengehören). Trotzdem: Auch wenn man die Überwachung ins rechte Licht rückt, bedeutet das noch lange nicht, dass am Ende alles gut wird. Wir müssen die Kernfragen der Überwachung auch weiterhin sorgfältig identifizieren und im Auge behalten. Überwachung ist ein zweischneidiges Schwert – wir dürfen ihre Vorteile nicht außer Acht lassen. Doch groß angelegte Systeme bergen Risiken und Gefahren in sich, und Macht korrumptiert – oder verzerrt zumindest die Ansichten der Mächtigen. Groß angelegte Technologie-Infrastrukturen neigen auch zu großen Problemen. Ein versehentlicher oder falscher Tastendruck kann leicht Chaos verbreiten. Denken wir doch nur an das Online-Verhalten von 20 Millionen ganz normalen Bürgern, das AOL im August 2006 zu „Forschungszwecken“ freigab. Obwohl angeblich von allen Identifikationsmerkmalen befreit, konnten die Suchanfragen in Sekundenschnelle mit Namen in Verbindung gebracht werden.¹ Ebenso wichtig sind Korruption und verzerrte Machtansprüche. Auch hier muss man nicht auf einen boshafte Tyrannen zurückgreifen, der sich der Datenbanken mit Sozialhilfeangaben oder medizinischen Daten bemächtigt. Machtmissbrauch gibt es auch bei Politikern, die sich auf das sogenannte öffentliche Wohl (wie z. B. den Sieg über einen Kriegsgegner) berufen, um un- oder gar außergewöhnliche Taktiken durchzusetzen. Im Zweiten Weltkrieg wurden japanischstämmige Amerikaner in den USA über den – normalerweise illegalen – Einsatz von Volkszählungsdaten ermittelt und inhaftiert. In jüngster Vergangenheit wurden viele muslimische Amerikaner unter Zuhilfenahme von Flugverbotslisten als reiseuntauglich eingestuft oder anderweitig in Rassenprofile aufgenommen – Praktiken, die in einem

anderen Zusammenhang eindeutig als unfair eingestuft worden wären.² In einer globalisierten Hightech-Welt gibt es ausreichend Beispiele für die unbeabsichtigten Konsequenzen gut gemeinter Maßnahmen und Richtlinien. So hieß es z. B., Konzerne könnten nur wettbewerbsfähig bleiben, wenn sie „ihre Kunden gut kennen“, ihre Werbung entsprechend ausrichten und sogar ihre Fabriken und Geschäfte an den entsprechenden Orten ansiedeln. Den Geschäftsführer eines Ladens, der nur die kreditwürdigsten Kunden anziehen möchte und daher Kreditprüfungen über Experian vornimmt, hält ja auch niemand für unaufrichtig. Im Streben nach höheren Gewinnen ist das einfach sinnvoll. Ergebnis – und damit unbeabsichtigte Konsequenz – dieser Datenerfassung zur Schaffung eines profitablen Kundenstamms ist jedoch, dass bestimmte Gesellschaftsgruppen aufgrund ihrer Zahlungsfähigkeit eine Sonderbehandlung erfahren und andere links liegen gelassen werden.³ Besonders schwer wiegt die Tatsache, dass all diese Überwachungsverfahren und -methoden eine Welt schaffen, in der uns niemand mehr vertraut. Überwachung fördert Misstrauen.⁴

Arbeitgeber installieren Tastenanschlagsanzeiger in Firmenc Computern oder Routenkontrollgeräte in Dienstfahrzeugen und geben damit unumwunden zu, dass sie ihren Mitarbeitern nicht trauen. Der Sozialbeamte, der auf Sozialhilfebetrug untersucht oder nach Hinweisen für einen „Ehemann im Hause“ forscht, gibt damit zu, dass er seinen Empfängern nicht traut. Und auch Eltern, die die Aktivitäten ihrer Teenager per Webcam oder GPSSystem verfolgen, erklären damit offen, dass sie ihnen nicht trauen. Man mag einwenden, dass es sich doch um reine Vorsichtsmaßnahmen handelt. Aber wie weit darf dieses Verhalten gehen? Unsere gesellschaftlichen Beziehungen basieren auf Vertrauen und wenn wir dieses Fundament untergraben, kommt das einem langsamen gesellschaftlichen Selbstmord gleich.

Der Gesamttext der Studie ist verfügbar unter:
www.privacyconference2006.co.uk/files/report_ger.pdf

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

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

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

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