VIDEOÜBERWACHUNG

Dietmar Kammerer

Seit den von Edward Snowden ausgelösten Enthüllungen über datengestützte, vernetzte und automatisierte Überwachung wirken die Kameraaugen auf öffentlichen Straßen und Plätzen wie ein Relikt aus dem späten 20. Jahrhundert: ein bildgebendes Kontrollinstrument, dessen letzte Legitimation darin besteht, Hollywood-Thrillern eine zum Klischee geronnene blaustichige Pixel-Ästhetik zu verpassen. Überprüft man die Berichterstattung der vergangenen Jahre, stößt man deutlich häufiger auf die Rede von Big Data und sozialen Netzwerken, von Smartphones und E-Mail-Verschlüsselung als von Kameras, Monitoren und den Bildern, die sie erzeugen. Angesichts des schieren Ausmaßes, mit dem westliche Geheimdienste die globale elektronische Kommunikation anzapfen, mitprotokollieren, in riesigen Datenspeichern ablegen und durch eine Armada von Analysten und Algorithmen auswerten lassen, haben die grauen Kamerakästen an Betonwänden einen Teil ihres Schreckens (und ihrer Faszination) verloren.

Zudem eignet die visuelle Kultur sich die Ästhetik und Logik der Überwachung an. Es gibt keinen Ort im bewohnten Teil der Welt, der nicht zu jeder Uhrzeit durch Kameras beobachtet würde: Smartphones, Webcams, Dashcams, Bodycams, Kameras an Drohnen und in Satelliten, an Häuserwänden, auf Laternenpfosten, in Bussen, Zügen und Straßenbahnen, an Straßenrändern, am Haus des Nachbarn, in der Shopping Mall, im Kinderzimmer, im Sportstudio, im Kino, im Schwimmbad, im Hörsaal, in der Bibliothek, im Restaurant, auf Berggipfeln, am Strand: Die Welt ist Bild geworden. All das hat

zur Gewöhnung geführt. Seltsame Vertauschung: Die Fähigkeit, mühelos Bilder produzieren und jeden beliebigen Ort, jedes Ding, jede Person sofort sichtbar machen zu können (einst das Privileg der Macht), gehört nun >uns allen<, während das einst als demokratische Institution gefeierte Internet >von denen< besetzt worden ist, ohne dass jemand es bemerkt hätte. Unsichtbare Daten und im Geheimen operierende Algorithmen bilden das neue Panoptikum.

Das war vorauszusehen. In Großbritannien, seit mehr als zwanzig Jahren Vorreiter der flächendeckenden und ungebremsten Installation von Videokameras im öffentlichen Raum, ist auch unter den Hardlinern der Sicherheitspolitik der hartnäckige Optimismus der Einsicht gewichen, dass es nicht ausreicht, an jeder verfügbaren Straßenecke ein elektronisches Auge aufzustellen, um Verbrechen zu verhindern. 1994 startete die britische konservative Regierung, mit der Rückendeckung wissenschaftlicher Gutachten und der öffentlichen Meinung, ein Förderprogramm, das die Installation von Videoüberwachung oder Closed Circuit Television (CCTV) in Städten und Gemeinden finanziell unterstützte. Der Andrang auf die Millionen in den Fördertöpfen war derart groß, dass das Programm in den kommenden Jahren, auch unter der Labour-Regierung Tony Blairs, mehrfach neu aufgelegt und der Kreis möglicher Empfänger erweitert wurde. Im Land von George Orwell galten Videokameras auf einmal als Wundermittel der Verbrechensbekämpfung. Schätzungen zufolge wurden in den 1990er Jahren drei Viertel des Budgets zur Kriminalprävention ausschließlich für CCTV-Systeme ausgegeben, Betriebs- und Wartungskosten nicht eingerechnet.

Die Zahl der Kameras im öffentlichen Raum beträgt nach aktuellen Schätzungen zwischen vier und sechs Millionen, etwa 20 Kameras pro Quadratkilometer oder eine Kamera auf 14 Einwohner. Insgesamt sollen zwischen einer und vier Milliarden Pfund in die Technik investiert oder, besser gesagt, versenkt und verschenkt worden sein. Mehrere von der Regierung in Auftrag gegebene Studien, die den Nutzen und Vorteil von Videoüberwachung belegen sollten, kamen zum gegenteiligen Ergebnis, dass die Kriminalitätsrate von den Kameraaugen im Großen und Ganzen unbeeinflusst bleibt: Eine Verringerung von lediglich drei bis vier Prozent konnten Statistiker und Kriminologen auf CCTV zurückführen. Gravierender noch: Videoüberwachung trug lediglich dazu bei, in etwas stärkerem Maße Sachbeschädigungen (Graffiti), Autodiebstähle oder Autoaufbrüche zu verhindern, sie war aber ohne Einfluss bei Gewalt gegen Personen, bei Prügeleien, Raubüberfällen oder Mord. Ein interner Bericht der Londoner Polizei zog 2009 die Bilanz, dass auf jeden gelösten Kriminalfall 1000 Kameras kommen.

Angesichts solcher Zahlen räumen mittlerweile auch ranghohe britische Polizisten ein, dass Videoüberwachung aus Sicht der Kriminalprävention ein »völliges Fiasko« darstelle und die Öffentlichkeit »in die Irre geführt« worden sei, was die Effektivität der optischen Überwachung betreffe. Hauptproblem: Während

Unsummen dafür eingesetzt worden sind, Anzahl und Dichte der Kameras zu erhöhen, wurde kein Gedanke darauf verwendet, wie die dadurch anfallenden Bilderfluten ausgewertet werden könnten. Aller Rhetorik von High-Tech zum Trotz verfügen nur wenige britische Gerichte über Abspielgeräte für Beweisvideos. Polizisten weigern sich, Bilder aus privaten Überwachungskameras auszuwerten, weil ihnen schlicht die Ressourcen dafür fehlen. Viele Mitte der 1990er Jahre aufgestellte Kameras nehmen noch auf Magnetband auf, das von minderer Qualität und nur aufwendig zu archivieren oder auszuwerten ist.

Als die BBC im vergangenen Jahr über ein mögliches »End of the CCTV Era« spekulierte, geschah dies nicht wegen der schieren Ineffizienz der Technik, sondern weil den klammen Gemeinden und Städten allmählich das Geld ausgeht, die Unzahl an Kameras und Sicherheitszentralen weiterhin zu betreiben. Die Regierung hat den Fokus ohnehin auf die Erfassung und Kontrolle elektronischer Kommunikation verschoben und bereitet ein neues Überwachungsgesetz vor, das Polizei, Geheimdiensten (GCHQ) und anderen staatlichen Institutionen (Pensionsbehörden!) weitreichende Befugnisse einräumen soll. Die Investigatory Powers Bill sieht unter anderem vor, dass private Datenbanken ohne richterlichen Vorbehalt durchsucht und ausgewertet, private Telefone oder Computer auch ohne direkten Verdacht gegen die Person gehackt sowie globale Unterseekabel angezapft werden dürfen (letzteres ist bereits gängige Praxis, nur bislang ohne ausdrückliche gesetzliche Erlaubnis).

Schwierig für die Kameras, da noch mitzuhalten. Die Sicherheitsindustrie, die ihre Produkte weiterhin verkaufen möchte, setzt wie immer auf technische Aufrüstung und blumige Versprechungen in Werbebroschüren. Dabei sollen die Kameras nicht nur digital, hochauflösend und irgendwie ›smart‹ werden, sie sollen vor allem nicht länger nur isolierte Sicherheitsfunktionen übernehmen. Die Videoüberwachung der Zukunft ist eine flexible und multifunktionale Infrastruktur: Teil eines umfassenden Netzwerks, das aus weiteren Sensoren, aus Datenbanken, Computern, Algorithmen und menschlichen Akteuren besteht. Ein Anbieter von Straßenbeleuchtung wirbt für eine neue Generation von Laternen, die neben den obligatorischen Videokameras Sensoren für Erdbeben, chemische Waffen, Umgebungstemperatur und Helligkeit, Luftqualität und weitere Umweltdaten enthalten. Ein Hersteller digitaler Kameras will die bildgebenden Chips mit einer Software-Plattform ausstatten, die es erlaubt, verschiedene Programme (gleichsam Apps) aufzuspielen und parallel auszuführen. Jeder Akteur, der sich am Netzwerk der Kameras beteiligt, könnte dieses dann für seine eigenen Zwecke programmieren – Ladenbesitzer könnten die Kundenbewegungen in Echtzeit analysieren, während zur selben Zeit die Sicherheitsbehörden ein Programm zur Gesichtserkennung ausführen. Hohe Auflösung, Multifunktionalität, Vernetzung, ›intelligente‹ automatisierte Bilderkennung: Das sind die Stichworte, dank denen Videokameras Sicherheitsbehörden, Unternehmen und besorgten Privatleuten weiterhin als attraktive Waren erscheinen sollen.

Allerdings ist die biometrische Erkennung von Individuen in der Praxis noch weit davon entfernt, zuverlässig zu funktionieren. Dass Videokameras künftig jeden Einzelnen von uns auf der Straße erkennen können, gehört zu den hartnäckigsten Gerüchten. Die Realität der Biometrie sieht anders aus. Ein groß angelegter Feldversuch des Bundeskriminalamtes (BKA) am Mainzer Hauptbahnhof vor einigen Jahren, der als weltweit erstes Pilotprojekt die Leistungsfähigkeit von Gesichtserkennungs-Software unter halbwegs realistischen Bedingungen überprüfte, brachte ernüchternde Ergebnisse. Selbst unter optimalen Lichtbedingungen wurde nur etwas mehr als die Hälfte der Personen richtig erkannt, nachts fiel die Quote auf magere zehn Prozent. Ein Problem waren die zahlreichen, hell erleuchteten Werbetafeln am Bahnhof, welche die empfindliche Optik der Kameras störten. Das BKA musste einräumen, dass die Technik noch nicht einsatzfähig sei (freilich konnte so auch festgestellt werden, wie die öffentliche Architektur künftig gestaltet sein muss, um optimale Bedingungen für den Einsatz von Überwachungstechnik zu bieten).

Interessanterweise kommen in der Praxis der Ermittler keine Super-Algorithmen, sondern menschliche ›Super-Recognizer‹ zum Einsatz, die durch eine nicht näher begründete ›Gabe‹ in der Lage sein sollen, individuelle Gesichter mit absoluter Sicherheit zu erinnern und innerhalb großer Menschenmengen wieder aufzufinden. Scotland Yard hat schon vor einigen Jahren eine Spezialeinheit derart inselbegabter Gesichtserkenner aufgestellt, einige davon unterstützten jüngst die Kölner Polizei bei der Fahndung nach Verdächtigen aus der Silvesternacht 2015.

Dass in Köln der Hauptbahnhof und sein Vorplatz in den Blick gerieten, ist kein Zufall. Videoüberwachung findet vor allem an Orten der Mobilität statt. Von den (offiziell) 14.765 Kameras, die in Berlin den öffentlichen Raum einsehen, filmen 13.643 im Nahverkehr, also in Bahnhöfen, Zügen, Bussen und Straßenbahnen. An ausgewählten U-Bahnhöfen hat die Berliner Polizei die Möglichkeit, live auf Kameras und Bilder zuzugreifen. Auf Bundesebene setzten sich die Verkehrsminister der Länder auf ihrer Frühjahrskonferenz 2016 für die »flächendeckende, tageszeitunabhängige Videoaufzeichung in öffentlichen Verkehrsmitteln« ein. Erklärtes Ziel ist die Schaffung einer »einheitlichen Sicherheitsphilosophie im öffentlichen Personennahverkehr« – und das nicht nur, weil die Räume des Fern- wie Nahverkehrs bekanntermaßen ein bevorzugtes Ziel von Terroristen, Antänzern, Taschendieben und Drogenhändlern darstellen, sondern weil sich die Architekturen des ÖPNV in besonderem Maße für die optische Überwachung eignen. Anders als unter freiem Himmel sind die Lichtverhältnisse dort weitgehend konstant. Die Rolltreppen, Gänge und Schleusen der U- und S-Bahnen kanalisieren die Menschenströme, geben ihnen eine Richtung. Das erzeugt Übersichtlichkeit, erleichtert es, Personen zu erkennen und über mehrere Kameras zu verfolgen (›multi-camera tracking‹). Sicherheitsingenieure haben einen eigenen Namen für solche Räume, die Menschen

anordnen: ›facetraps‹, Gesichtsfallen. In diesen Architekturen ist die Bandbreite erwarteter Handlungen (im Vergleich zu einem öffentlichen Ort, etwa einem Park) stark eingeschränkt. Als Normalverhalten gilt: ankommen, auf den nächsten Zug warten, einsteigen. Alles andere fällt dagegen in einem Maße auf, dass selbst Algorithmen die Abweichung erkennen können.

Nicht die individuelle Identifizierung (das übernehmen die ›Super-Recognizers‹), sondern die typenhafte Mustererkennung wird an bilderkennende Rechner delegiert (›video analytics‹). Bestimmt man eine unerwünschte Handlung oder ein Ereignis allgemein genug, kann dieses automatisch erkannt und menschlichen Beobachtern zur weiteren Prüfung gemeldet werden. Typisch: Koffer, die zu lange im Bildbereich bleiben, ohne bewegt zu werden (Verdacht auf Bombenattentat). Einzelne Personen, die sich gegen den allgemeinen Strom der Passanten bewegen (Verdacht auf den Beginn einer Panik). Personen, die am Bahnsteig lange Zeit sehr nahe am Gleisbett stehen, ohne in einen Zug einzusteigen (Verdacht auf Suizidversuch). Personen, die die Hände heben (Verdacht auf Raubüberfall). In London – erneut ist Großbritannien Vorreiter – sind an ausgewählten U-Bahn-Stationen und an touristischen Orten Systeme im Einsatz, die u.a. ›Herumlungern‹, die Gefahr einer Blockade oder Stauung von Passagieren, das Eindringen unbefugter Personen in geschlossene Bereiche oder vergessene (und verdächtige) Gepäckstücke erkennen und melden sollen. Zugleich kann das Anwachsen und Abnehmen von Passagierströmen gezählt und analysiert werden (›automated crowd management‹). Ein von der Bundesregierung finanziertes Forschungsprojekt verspricht, durch die visuelle Analyse von Mimik, Körperhaltung, Gang die Absichten von Personen in Echtzeit vorhersagen zu können: ob jemand aggressiv wird, ob ein medizinischer Notfall oder eine andere »interventionsbedürftige Situation« vorliegt.

Man stelle sich vor, solche Systeme zur Bildanalyse würden auf das große Netzwerk der Bilder losgelassen: auf alle Bilddateien, die in der Cloud, in sozialen Netzwerken oder in den Bildarchiven der staatlichen Sicherheitsbehörden liegen. Auf freiwilliger Basis geschieht das teilweise bereits jetzt legal: Bei Katastrophen oder terroristischen Attentaten, wie dem Anschlag auf den Bostoner Marathon, wird die Bevölkerung aufgerufen, ihr privates Bildmaterial zur Auswertung an die Ermittlungsbehörden zu senden. Darum gerät in der Gegenwart jede private Filmaufnahme einer Großveranstaltung potenziell zum Dokument einer forensischen Ermittlung, zum Baustein sicherheitspolitischen Handelns. Geheimdienste mit uneingeschränktem Zugriff auf die Bilddatenbanken der Online-Speicher müssten (oder müssen) nicht einmal um Erlaubnis fragen. ◆