Auszug aus **Context XXI**
http://contextxxi.org/von-kleinen-und-grossen-brudern.html

erstellt am: 28. März 2024
Datum dieses Beitrags: Juni 2000

Von kleinen und großen Brüdern

Überwachung in der Informationsgesellschaft

Die polizeistaatliche Kontrolle der BürgerInnen wird sowohl in Österreich als auch in der restlichen EU immer mehr verschärft.

CORNELIA MOSER

Neue Informations- und Kommunikationstechnologien werden zumeist als Mittel zur Schaffung einer grenzenlosen Wissensgesellschaft propagiert. Sie sind jedoch nicht nur dazu geeignet, abstrakte Sachverhalte zu erfassen und für die Allgemeinheit bereitzustellen oder als kommunikative Vernetzungsformen die Plattform für potentiell freie und gleiche Diskurse zu liefern. Die technischen Grundlagen der modernen Informationsgesellschaft bieten darüber hinaus die Möglichkeit, in den unterschiedlichsten Zusammenhängen personenbezogene Informationen zu erfassen, zu speichern, weiterzugeben und zu verwerten.

Schauplatz 1: Monaco ist eine sichere Stadt.

Schon in der Anfahrt erfassen Überwachungskameras den Ankommenden, der über die elektronischen Augen an allen wichtigen Punkten der Stadt jederzeit im Bild bleibt. Gesteuert wird dieses ausgefeilte System über die zentrale polizeiliche Leitstelle, die über die schwenkbaren Kameras potentielle Rechtsbrecher — wie zum Beispiel Fahrradfahrer in der Fußgängerzone — entdecken und ein Sicherheitsorgan zur Maßregelung des Missetäters entsenden kann. Dunkelheit ist kein Problem für die Infrarotkameras zur Küstenüberwachung, und auch ungewöhnliche nächtliche Geräusche können mittels eines Abhör- und Geräuschanalysesystems jederzeit ausgemacht werden.

Schauplatz 2: Das Unternehmen macht ausgezeichnete Gewinne.

Maximale Kontrolle über die Effizienz und Produktivität der MitarbeiterInnen erreichen Tourismusunternehmen in den USA durch den Einsatz des Computers als Aufseher über die telefonische Kundenberatung. Mittels Steuersignal in den Sprechgarnituren der Angestellten wird jede Sekunde kontrolliert, ob gesprochen wird oder nicht. Die computergenerierten Auswertungsprotokolle der Zahl und Länge der Verkaufsgespräche sowie der Verkaufserfolge werden täglich oder wöchentlich kontrolliert und verglichen.

Schauplatz 3: Ich habe mein Kind immer im Auge.

Ebenfalls in den USA boomt der Verkauf von „Nannycams“, die die elektronische Überwachung des Kinderzimmers samt Kind und Kindermädchen ermöglichen. Mittels Koppelung an einen PC kann auch über einen weit entfernten Arbeitsplatz die häusliche Sphäre im Blickfeld bleiben.

Alle drei Beispiele haben als gemeinsamen Nenner die Nutzung moderner Kommunikationstechnologien und verweisen auf das, was spätestens seit George Orwells literarischer Negativ-Utopie „1984“ in liberalen westlichen Demokratien als abschreckende Zukunftsvision der totalen Überwachungsgesellschaft gesehen wird. Wenn auch der „Große Bruder“ in nächster Zeit nicht über die Hintertüre der neuen schönen Informationsgesellschaft Einzug halten wird, so zeigt doch der Blick auf die Einsatzmöglichkeiten neuer Technologien das Wesen und Wirken der vielen „kleinen Brüder“, die hier am Werk sind. In jedem der Fälle werden technische Hilfsmittel eingesetzt, um ehemals unzugängliche — private — Informationen zu erheben, Schlußfolgerungen zu ziehen und einseitig Handlungsoptionen zu entwickeln.

Die Entwicklung der unterschiedlichsten Überwachungstechnologien ist vor allem auf die Forschungstätigkeiten für den militärischen Einsatz und für die Erfordernisse der Spionageabwehr zurückzuführen, die nach dem 2. Weltkrieg weiter vorangetrieben wurde. Die Technologien zur Erfassung, Speicherung und Verarbeitung von personenbezogenen Informationen sind seither laufend weiterentwickelt worden und finden sich seit den achtziger Jahren verstärkt auch in zivilen Bereichen. Viele der Einsatzformen von Überwachungstechnologien zielten und zielen nicht explizit auf die Erfassung intimer Daten ab. Die Verwendung erfolgt dezentral und ist keineswegs flächendeckend. In den neunziger Jahren hat jedoch die Entwicklung der Technologien des Erfassens, Sammelns, Speicherns und Verwertens von personenbezogenen Informationen eine neue Dynamik entwickelt, die vermehrt in Hinblick auf ihre sozialen und politischen Konsequenzen diskutiert werden muß. Die qualitativen Verschiebungen durch Überwachungstechnologien ergeben sich vor allem durch die Verschränkung der direkten Informationserfassung mit gleichzeitiger Verarbeitung und Weitergabe der Informationen, die erst durch die Möglichkeit-

en der Konvertierung unterschiedlicher Datenformen — Bild, Ton und Text — sowie durch die Vernetzung dezentraler Quellen verwirklicht werden. So erfassen Stroboskopkameras auch in großen Menschenmassen einzelne Personen und liefern innerhalb von Sekunden hunderte Einzelbilder. Neben der reinen Einzelbilderfassung kann das Personenbild über CCTV (Closed Circuit Television)-Technologie mit anderen Bild-Datenbanken abgeglichen werden. Eindeutige Identifizierungsysteme wie Irisscans oder DNA-Proben werden verstärkt zur zweifelsfreien Personenfeststellung herangezogen und immer mehr personenbezogene Informationen aus unterschiedlichsten Bereichen werden über große Informationsverbundsysteme speicher- und abfragbar. Damit zeichnen sich neue Formen der sozialen Kontrolle ab, die zunehmend intensiver und extensiver wirken, und die von den jeweils Betroffenen mmer weniger bemerkt oder kontrolliert werden können. Inwieweit elektronische Überwachung den Anspruch erfüllt, „im Dienste des Menschen“ zu stehen, bleibt eine Frage des Zusammenhangs. Handelt es sich um Einsatzgebiete mit unterschiedlichen Interessen und eingeschränkten Handlungsspielräumen auf Seiten der Überwachten, dann erweist sich Überwachung als eine Verstärkung des Machtungleichgewichts zugunsten desjenigen, von dem elektronische Überwachung ausgeht.

Im modernen Panopticum

Aus theoretischer Sicht wird in Anlehnung an Michel Foucaults „Überwachen und Strafen“ unter dem Stichwort des panoptischen Blickes vermehrt die normierende Wirkung elektronischer Überwachung diskutiert. Foucaults Beschreibung von Machtgefügen anhand des Panopticums beinhaltet zwei zentrale Aspekte von Überwachung: Zum einen den direkten personenbezogenen — asymmetrischen — Informationsfluß, wobei der Betroffene gesehen wird „... ohne selbst zu sehen, er ist Objekt einer Information, niemals Subjekt einer Kommunikation“ (Foucault 1995: 257); zum anderen die Sammlung von Informationen, die es in der Summe erst ermöglichen, Kategorien zu bilden, daraus Abweichungen zu erkennen und entsprechend zu sanktionieren. Die Qualität des Panopticums zur Analyse moderner elektronischer Überwachung besticht vor allem in Hinblick auf den Einsatz von Kamerasystemen im öffentlichen und privaten Bereich, in der der kontrollierende Blick der Linse Regelverstösse seltener werden läßt und dadurch tatsächlich „normend, normierend, normalisierend“ (Foucault 1995: 236) wirkt.

Vielfach wird davon ausgegangen, daß das Schrekkensszenario des „Großen Bruders“ ausgedient hat, und daß das Bedrohungspotential für individuelle Privatsphären nicht durch staatliche Überwachungsaktivitäten entsteht, sondern sich vielmehr aus den vielen dezentralen Kontroll- und Überwachungsformen privater Unternehmen ergibt. Das ist richtig, allerdings sollten die staatlichen Aktivitäten in diesem Bereich nicht unterschätzt werden. Die Zuwächse an Sammlungen personenbezogener Daten rühren in erster Linie von den Aktivitäten der Privatwirtschaft her, aber auch der Staat nutzt neue Formen der Informationserfassung und verfeinert die vorhandenen Instrumentarien, die im Zuge verwaltungsstaatlicher und polizeilicher Aufgaben Verwendung finden.

Die Erhebung von personenbezogenen Informationen — seien es Bilder, Bewegungen im öffentlichen Raum, Gespräche mit dritten oder Informationen über Konsum- und Sozialverhalten — schafft Wissen über Bevölkerungskreise und einzelne Personen. Sie ermöglicht Kontrolle und etwaige Sanktionierung regelwidrigen Verhaltens einzelner Personen. Parallel zum Kontrollzuwachs auf Seiten der Überwacher verstärkt sich der Kontrollverlust auf Seiten der Überwachten, deren Bestimmungsgewalt darüber, mit wem sie wann, wie, wo und zu welchen Bedingungen Informationen über sich selbst mit Dritten teilen, sinkt. Der selbstgewählten Entgrenzung des Privaten steht die fremdbestimmte Entgrenzung mittels Überwachungstechnologien gegenüber, und nicht ohne Grund wird die Kehrseite der Informationsgesellschaft auch als „das Ende der Privatheit“(Whitacker 1999) thematisiert, in der „der Mensch unter ständigem Verdacht“ (Leuthardt 1996) steht und sich „im Visier der Datenjäger“ (Reischl 1998) wiederfindet.

Das Recht auf Privatheit

Der Anspruch auf die Unverletzbarkeit der Person und eine ihr zuzurechnende individuelle Sphäre wurde zunächst als ein Abwehrrecht gegenüber Dritten — „the right to be let alone“ — formuliert, um später als Selbstbestimmungsrecht fixiert zu werden. Selbstbestimmung versteht sich dabei vor allem als Kontrollrecht, durch welches die Entscheidungshoheit über Grenzüberschreitungen ins Private dem/der Einzelnen überlassen wird. Als Gegenpart zur öffentlich-staatlichen Gewalt muß es daher in liberalen Demokratien private Räume geben, die als individuelle Ansprüche festgelegt werden und dem Prinzip der — wie immer gearteten — Ausgewogenheit zwischen kollektiven und individuellen Interessen folgen. Ihre Legitimation zieht diese Fassung von individueller Privatsphäre aus der Betonung des demokratischen Wertes von Privatheit. Selbstbestimmung über die eigene Privatsphäre und über angestrebte Kommunikationsprozesse wird dadurch zur Voraussetzung für soziales und politisches Handeln und damit zur Basis für alle Bürgerrechte schlechthin.

Die Ausdehnung der jeweiligen Privatsphäre orientiert sich aber auch am jeweiligen Umfeld und nicht zuletzt an kollektiven Interessen, vor denen das Ausmaß an Privatheit im Zweifelsfall neu abgesteckt wird. In der rechtlichen Fassung als Anspruch auf Achtung des Privat- und Familienlebens wird dieser Vorbehalt bereits formuliert. Privatheit steht dabei im Spannungsfeld zu allgemeinen Werten der Sicherheit, Gesundheit, Moral und auch zu den Anrechten anderer Einzelpersonen auf Freiheit und Sicherheit.

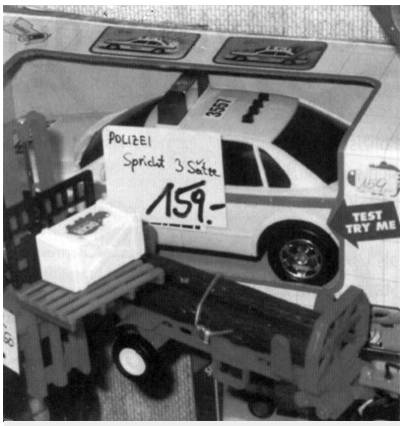


Das Grundrecht auf Privatsphäre wurde in den siebziger Jahren in den meisten Ländern um die Datenschutzgesetzgebung erweitert, die staatlichen Eingriff-

en auf personenbezogene Daten Schranken setzen sollte. Darin wurde auch der Anspruch auf Geheimhaltung persönlicher Daten formuliert, den moderne Verfechter von Privatheit als Recht auf informationelle Selbstbestimmung für BürgerInnen und KonsumentInnen verankert sehen möchten. Dieser geforderte Paradigmenwechsel zeichnet sich angesichts der laufenden Entwicklungen nicht ab. Im Gegenteil: Elektronische Überwachung gibt staatlichen Stellen die Möglichkeit, eine größere Menge privater — personenbezogener — Informationen besser zu sammeln, zu speichern und zu verknüpfen. Überwachung durch den Staat bedeutet zwar nicht eine absolute Veröffentlichung privater Informationen im Sinne allgemeiner Zugänglichkeit, denn dies wird durch das Geheimhaltungsgebot grundsätzlich verhindert. Überwachung in der Beziehung Staat — Privat führt vielmehr zu neuen „intimen“, quasi privaten Beziehungen, die sich durch asymmetrische Transparenz auszeichnen, wobei die überwachende Stelle über die Macht oder die Ermächtigung sowie die Mittel verfügt, Informationen zu generieren.

Überwachen und Strafen in Österreich ...

In Österreich ist diese Entwicklung seit einigen Jahren zu beobachten, wobei der tatsächliche flächendeckende Einsatz angesichts der vorhandenen Ressourcen zwar derzeit wenig wahrscheinlich scheint, die legistischen Voraussetzungen jedoch geschaffen und laufend weiter ausgebaut werden. Bereits vor der Einführung der besonderen Ermittlungsverfahren „Lauschangriff“ und „Rasterfahndung“ 1997 waren eine Vielzahl von Einsatzmöglichkeiten technischer Überwachungsverfahren durch entsprechende rechtliche Regelungen gedeckt. Telefonüberwachungen sind seit Jahren gang und gäbe und auf der Basis der entsprechenden gesetzlichen Bestimmungen nach richterlicher Genehmigung möglich und auch die Strafprozeßordnung bot bereits vor 1997 eine Reihe von Instrumenten, um in der Strafverfolgung technische Hilfsmittel einzusetzen. Mit dem Sicherheitspolizeigesetz 1991 wurden erstmals auch für den präventiven sicherheitspolizeilichen (inklusive staatspolizeilichen) Einsatz Regelungen für die Inanspruchnahme akustischer und optischer Geräte und den Umgang mit personenbezogenen Daten getroffen. Ausgenommen waren bis dahin nur der große Lausch- und Spähangriff als akustische oder optische Überwachung von privaten Räumen und die negative automationsgestützte Rasterfahndung, bei der nicht nach bestimmten bekannten Personen gesucht wird, sondern nach dem Prinzip der Wahrscheinlichkeit Personengruppen nach bestimmten Kriterien vom Tatverdacht ausgeschlossen werden. Im Rahmen der Aufrechterhaltung der öffentlichen Ordnung wurde überdies die optische Überwachung des öffentlichen Raums durch Kameras geregelt, die immer dann auf einer rechtlichen Basis steht, wenn mit Menschenansammlungen und möglichen daraus resultierenden Gefahren zu rechnen ist. Dabei kann seither sowohl auf reine Übertragungs- als auch auf Aufzeichnungsgeräte zurückgegriffen werden.



„Test Try Me“

Die befristete Einführung von „Lauschangriff“ und „Rasterfahndung“ 1997 stellt die bislang letzte große Maßnahme im Bereich der polizeilichen Befugniserweiterung unter Nutzung technischer Hilfsmittel dar. Beide Überwachungsformen sind sowohl in Hinblick auf die Eingriffsmöglichkeiten polizeilicher Gewalt in die Intimsphäre als auch auf die Verwischung strafrechtlich relevanter Tatbestände und konkreter Verdachtsmomente umstrittene Methoden. Als Entscheidung zwischen kollektiver Sicherheit und individueller Freiheit formuliert, konnte sich jedoch die Argumentation der BefürworterInnen, die die besondere Gefährlichkeit „Organisierte Kriminalität“ für den Staat und seine BürgerInnen hervorhoben, durchsetzen. Den Bedenken der GegnerInnen wurde durch bestimmte Auflagen und die Einführung einer übergeordneten Kontrolle Rechnung getragen, die diesen Methoden, private Räume mittels Kameras und/oder Mikrofone zu überwachen sowie staatliche und private Datenbanken nach mutmaßlichen Straftätern im Bereich der „Organisierten Kriminalität“ zu durchsuchen, Grenzen setzen. Es ist davon auszugehen, daß beide Instrumente in das Dauerrecht übernommen werden, obwohl die Frage, inwieweit die Aktivitäten krimineller Organisationen in Österreich tatsächlich jene oft konstatierte letale Bedrohung für den Rechtsstaat darstellen, keineswegs eindeutig mit Ja beantwortet werden kann.

... und in der EU

Die stärksten Impulse in Richtung des Ausbaus polizeilicher Überwachungsinstrumentarien gehen heute jedoch nicht mehr nur von einzelnen nationalen „law & order“-Regierungen aus. Im Zuge des europäischen Integrationsprozesses erweisen sich die Hüter der Inneren Sicherheit als besonders zielstrebig. Im Rahmen des dritten Pfeilers der EU, der Sicherheitsunion, werden nicht nur grenzüberschreitende Abhöraktionen ohne nationale Kontrollmöglichkeiten — derzeit noch heftig umstritten — angestrebt, sondern es zeichnet sich auch ein weiterer Ausbau der EU-weiten Informationssysteme ab. Das kriminalpolizeiliche Schengener Informationssystem (SIS) oder auch The European Computer System (TECS) von Europol entwickeln sich zu mächtigen Datensammlungen, deren Aufnahmekriterien und Inhalte weitgehend unkontrolliert bleiben. Einen weiteren Schritt hin in Richtung der Nutzung elektronischer Überwachungsverfahren wird die Verabschiedung der Eurodac-Konvention darstellen, wonach EU-weit die Fingerabdrücke von Asylsuchenden registriert werden, womit schnell und relativ treffsicher der Status von Personen ermittelt und „unerwünschte“ Menschen „beamtshandelt“ werden können. Den gut vernetzten Innenministerien Europas stehen dabei in ihren Bestrebungen keine vergleichbaren Kräfte gegenüber, die die Rechte auf Privatspähre ähnlich vehement forden würden wie es bei den Anwälten

der informationellen Aufrüstung im Rahmen der Polizeiapparate zu beobachten ist.

Die Technik macht's möglich: Im Visier polizeilicher Ermittlungen sind im Zeitalter elektronischer Überwachung weitaus mehr Menschen. Zum einen alle Personen „ohne Ansehen der Person" im Falle der kategorialen Ermittlungen („Verdächtig sind alle männlichen Porschefahrer, die ihre Duftbäume über ein Versandhaus beziehen ..."), zum anderen alle, die heimlicher, direkter Überwachung ausgesetzt sind: Tatverdächtige, ihre Familien, Freunde und Bekannten. Das Prinzip, wonach ein Vergehen und konkrete Verdachtsmomente vorliegen müssen, damit eine polizeiliche Ermittlung beginnen kann, löst sich mit der Intensivierung präventiver Beobachtungsmaßnahmen zunehmend auf. Betroffen davon sind grundsätzlich alle, die „anders" und damit unvermeidbar „verdächtig" sind. Die technologische Entwicklung und ihre legistische Instrumentalisierung etablieren damit in ihrer Intensität und Extensität qualitativ neue Dimensionen, Normenbefolgung zu überwachen. Unweigerlich wird es damit schwieriger, sich den Staat vom Leibe zu halten.

Der politische Wille geht nicht erst seit der blau-schwarzen Regierungsbildung in Richtung Ausbau präventiv orientierter polizeilicher Befugnisse. Technische Hilfsmittel durften dabei bisher nicht fehlen und werden auch in Zukunft eingefordert werden. Der Mangel an qualifiziertem Personal und geringe finanzielle Mittel bleiben die neuen (alten) Grenzen, die die Eingriffsmöglichkeiten öffentlich-staatlicher Gewalt in private Sphären mildern. Ein schwacher Trost.

Literatur:

- Foucault, Michel (1995): *Überwachen und Strafen: Die Geburt des Gefängnisses.* Frankfurt/-Main
- Leuthardt, Beat (1996): *Leben Online. Von der Chipkarte bis zum Europol-Netz: Der Mensch unter ständigem Verdacht.* Hamburg
- Reischl, Gerald (1998): *Im Visier der Datenjäger.* Wien
- Whitaker, Reg (1999): *Das Ende der Privatheit.* München

Aktuelle Informtionen:

- www.ad.or.at
- www.telepolis.de
- www.quintessenz.at

Cornelia Moser: Cornelia Moser ist Politikwissenschaftlerin in Wien und hat ihre Diplomarbeit zum Thema „Privates in Öffentlicher Hand. Elektronische Überwachung vor dem Hintergrund von Lauschangriff und Rasterfahndung" geschrieben.

Lizenz dieses Beitrags
Copyright
© Copyright liegt beim Autor / bei der Autorin des Artikels