Der gläserne Bürger und der vorsorgliche Staat: Zum Verhältnis von Überwachung und Sicherheit in der Informationsgesellschaft

Ralf Bendrath (Bremen)

Zusammenfassung

Das Sicherheitsparadigma des Präventionsstaates im „Kampf gegen den Terror“ unterscheidet sich in zweierlei Hinsicht von dem des Gefahrenabwehrstaates im Kalten Krieg. In zeitlicher Hinsicht geht es nicht mehr um die Abwehr gegenwärtiger Bedrohungen, sondern um die Vorbeugung zukünftiger Risiken. Auf der Akteursebene sind die Träger dieser Risiken nicht mehr Staaten, sondern Individuen. Damit gelten nun alle als potenziell verdächtig. Hier spielt der Computer eine entscheidende Rolle, indem er die alten Überwachungstechniken des Aufzeichnens und Verbreitens von Informationen durch die Möglichkeit des automatischen Entscheidens ergänzt. Aus „Überwachen und Strafen“ wird damit „Überwachen und Sortieren“, aus individuellen Bewertungen wird massenhafte digitale Diskriminierung auf der Basis von vernetzten Datenbanken und in Algorithmen gegossenen Vorurteilen. Mit diesem Verfahren sind jenseits juristischer und politischer Schwierigkeiten drei strukturelle Probleme verbunden: das Problem der Modellbildung, das Problem der Probabilistik und das Problem der Definitionsmacht. Dennoch scheint der Trend zum weiteren Ausbau der Überwachungsinfrastrukturen nicht aufzuhören. Mögliche Erklärungen, aber auch Hinweise auf weiteren Forschungsbedarf, liefern dafür jeweils auf unterschiedlichen Ebenen die Gesellschaftsdiagnose, die Techniksoziologie und die politische Ökonomie. In normativer Hinsicht geht es hier letztlich auch um die Sicherheitsvorsorge der Bürger gegenüber dem Staat und damit um die Frage: Wie können wir unsere technischen Infrastrukturen so aufbauen, dass unfähige und unredliche Machthaber damit keinen großen Schaden anrichten können?

1 Privatheit und Technologie im Wandel

Im Jahr 1890 erschien im Harvard Law Journal ein Artikel unter dem Titel „The Right to Privacy“ (Warren/Brandeis 1890). Er gilt bis heute als juristischer Gründungsakt für den Schutz der Privatsphäre.[1] Geschrieben haben ihn zwei angesehene Juristen aus Boston, der Anwalt Samuel Warren und der spätere Verfassungsrichter Louis Brandeis. Wie kamen sie dazu, diesen Artikel zu schreiben? Den Anstoß gaben zwei technische Entwicklungen.

Kurz zuvor hatte die Eastman Dry Plate Company unter dem Produktnamen „Kodak“ die ersten Handkameras mit Rollenfilm und relativ leistungsstarken Objektiven auf den Markt gebracht. Während Kameras vorher umständlich aufgebaut werden mussten und eine lange Belichtungszeit hatten, erlaubten diese neuen Geräte erstmals so etwas wie Schnappschüsse.

[1] Für eine konkurrierende Begründung siehe aktuell Richards / Solove (2007).

Das wiederum führte zu einem Problem für die gesellschaftliche Elite, zu der Warren und Brandeis damals in Boston gehörten. Ein findiger Reporter schoss mit einer solchen Kamera nämlich heimlich Fotos von der Hochzeit der Tochter von Samuel Warren (Prosser 1960).

Die andere Entwicklung war die Entstehung der modernen Tageszeitungen. 1812 war die Schnellpresse erfunden worden, 1845 die Rotationsmaschine, und 1884 kam die Linotype-Setzmaschine auf den Markt. Anzahl und Auflagenstärke der Tageszeitungen stiegen daher gegen Ende des 19. Jahrhunderts rasant an. Dieses neue Massenmedium sorgte für die schnelle und großflächige Verbreitung von Informationen – und auch von Fotos. Also erschienen die Fotos von der Hochzeit von Samuel Warrens Tochter in den Zeitungen in Boston.

Das hatte zwei Effekte: Aus den Mitgliedern der abgeschotteten gesellschaftlicher Elite wurden einerseits, wie man heute sagen würde, „Promis“. Zum anderen waren Warren und Brandeis gar nicht erfreut über diese Entwicklung, und als Reaktion entwickelten sie die oben erwähnte juristische Fundierung von Privatheit und Privatsphäre. Aus dieser Tradition wurden im Laufe der Zeit dann Konzepte wie „Datenschutz“ und das „Recht auf Informationelle Selbstbestimmung“ hergeleitet (Mayer-Schönberger 1996).

Dieser kurze Abriss der Geschichte des Rechtes auf Privatheit und Datenschutz zeigt bereits zweierlei: Erstens: Privatheit und Technologie waren schon immer eng verwoben, nicht erst seit der Erfindung von Computern und Datennetzen. Zweitens: Schon die 1890 verwendeten Geräte illustrieren sehr treffend den Kern der technischen Bedrohungen für die Privatsphäre. Die Kamera steht für die Mittel des Beobachtens und Aufzeichnens, während die Druckerpresse die Mittel des Transports, der Verbreitung und der Veröffentlichung symbolisiert. Wie sieht es heute aus, mehr als einhundert Jahre später, mit Computern, Internet und einer Durchdringung von Alltag und Berufsleben mit Informationstechnologie? Man könnte sagen, dass die Eastman-Kodak-Kamera von Handy-Kameras abgelöst wurde, während die Druckerpresse ihre Rolle an das Internet und Dienste wie Flickr und Youtube abgeben musste. Die Mittel des Aufzeichnens und Überwachens sind ebenso moderner geworden wie die Mittel der Verbreitung, aber im Kern gibt es nichts Neues. Oder?

Es ist *eine* Technologie dazu gekommen, die Warren und Brandeis noch nicht vorhersehen konnten: Der Computer als symbolverarbeitende Maschine, die automatisch Entscheidungen fällen kann. Er ermöglicht neben dem Aufzeichnen und dem Verbreiten nun auch das automatische Sortieren von Informationen. Und genau hier findet sich die direkte Verbindung zum zweiten Thema dieses Beitrages, zur Sicherheit.

Einige Beispiele aus der Sicherheitspolitik der jüngeren Vergangenheit dürften genügen, um das Ausmaß an technischen Veränderungen in der Politik der inneren Sicherheit oder des transgouvernementalen „Kampfes gegen den Terror“ zu illustrieren (als Überlick vgl. ICAMS 2006).

- Mit der Vorratsdatenspeicherung wird ab 2008 für alle Bewohner der EU monatelang gespeichert, mit wem sie wann und wo telefoniert haben, wann sie unter welcher IP-Adresse im Netz waren und wem sie wann eine Mail geschickt haben.

- EU-weit werden demnächst allen Bürgern für ihre Reisepässe die Fingerabdrücke abgenommen.
- In Großbritannien werden in der nationalen Gen-Datenbank die DNA-Profile von 2,5 Millionen Menschen aufbewahrt - auch von Unschuldigen, sofern sie irgendwann einmal einer Straftat verdächtig waren. Regierung und Polizei arbeiten seit längerem an Plänen, von allen Bürgern DNA-Proben zu entnehmen.
- In den USA werden über fünfzig Datensätze von Flugpassagieren vor dem Betreten des Flugzeugs mit Datenbanken von FBI, Heimatschutz und Geheimdiensten abgeglichen. Daraus wird eine Art Terrorismus-Rating in drei Stufen errechnet. Wer ein grünes Lämpchen kriegt, darf an Bord, bei wem gelb aufleuchtet, der wird von Beamten der Flugsicherheit vernommen, und wer rot bekommt, darf nicht an Bord. Die Berechnungsgrundlage für diese Bewertungen ist geheim.
- Ebenfalls in den USA hat der militärische Abhörgeheimdienst NSA seit 2001 die Telefonverbindungen von Millionen von Amerikanern mitprotokolliert. Diese Maßnahme verstieß zwar offen gegen den *Foreign Intelligence Surveillance Act*, soll aber nun nachträglich legalisiert werden.
- Am Mainzer Hauptbahnhof lief bis Juli 2007 ein Pilotprojekt, bei dem Überwachungskameras mittels biometrischer Verfahren die Gesichter von Passanten erkennen und diese identifizieren sollen. Anderswo existieren bereits Prototypen von Kamerasystemen, die aufgrund von Bewegungsmustern der überwachten Personen gewalttätiges Verhalten detektieren sollen. In Großbritannien und den Niederlanden sind einige Überwachungskameras bereits mit Mikrofonen ausgestattet. Die dahinter liegende Audioauswertungs-Software erkennt, ob sich in den aufgenommenen Stimmen Aggression oder Ärger ankündigen, und alarmiert dann von selber die Polizei (Roth 2006).

Jenseits der oberflächlichen technischen Grundlagen dieser Überwachungsmaßnahmen haben diese Beispiele gemeinsam, dass sie Ausdruck eines Paradigmenwechsels in der Sicherheitspolitik sind. In ihnen dient nämlich die Sammlung und Verarbeitung von Daten nicht mehr der Verfolgung von bereits begangenen Straftaten oder der Abwehr unmittelbar bevorstehenden Gefahren, sondern der *Prävention von Risiken* – des Risikos von terroristischen Anschlägen, aber auch des Risikos von Straßenkriminalität und anderen Vergehen. Damit verbunden ist ein grundsätzlicher Wandel im Verhältnis zwischen Staat und Bürger. Der Staat der inneren Sicherheit transformiert sich vom Gefahrenabwehrstaat zum vorsorglichen Staat oder Präventionsstaat. Möglich wird dies gerade durch die massive Nutzung des Computers als Entscheidungsmaschine.

2 Der vorsorgliche Staat in historischer Perspektive

Vor der Entstehung des neuzeitlichen Staates existierte „Sicherheit“ als politischer Begriff überhaupt nicht. Seit seiner Etablierung durch Thomas Hobbes im 17. Jahrhundert ist seine Bedeutung ständig erweitert worden. Ein Grund dafür liegt im Verschwinden des mittelalterlich-religiösen Heilsversprechens, als der Mensch im Zuge der Aufklärung entdeckte, dass er seine Zukunft selbst gestalten kann und muss. Die Unwägbarkeiten des

Lebens waren plötzlich kein gottgegebenes Schicksal mehr, sondern ein Problem aktiv herzustellender, geplanter Zukunft. An die Stelle der religiösen *Gewissheit* der Erlösung im Jenseits trat die moderne Idee der *Sicherheit* in einer diesseitigen, innerweltlichen Zukunft. Nichts anderes ist Sicherheit: Verfügung über die Zukunft. Die Zukunft ist aber naturgemäß offen und nicht vorherbestimmt. Damit steht sie im Dauerkonflikt mit der Idee der "Sicherheit" und mit der Aufgabe der Sicherheitspolitik. "Sicherheit" ist damit ein inhärent expansiver Begriff. Wenn man mit ihm operiert, finden sich immer wieder neue Unsicherheiten (Kaufmann 1973).

"Sicherheit" kann ganz allgemein verstanden werden als die Abwesenheit von Unsicherheit (Wolfers 1962). Entscheidend ist dann die Definition der Unsicherheit. "Sicherheitspolitik betreibt, wer die Bedrohung definiert" (Daase 1993: 45). Und hier zeigt sich: Nicht mehr *Bedrohungen oder Gefahren,* sondern *Risiken* prägen heute das sicherheitspolitische Denken. Ich will das mit einem kleinen Umweg in die internationale Sicherheitspolitik deutlich machen, wo diese Diskussion am klarsten und offensten geführt wird.

Das klassische Bedrohungsdreieck besteht aus drei Elementen: Einem Akteur (A) mit einer feindlichen Intention (I) und einem Potenzial (P), um diese böse Absicht auch umzusetzen. Erst wenn alle Ecken vorhanden sind, kann von einer Bedrohung geredet werden. Der Akteur (A) Großbritannien etwa ist durchaus eine starke Militärmacht, verfügt also über ein gefährliches Potenzial (P). Warum wird das in Deutschland nicht als Bedrohung angesehen? Was fehlt - ganz einfach - ist die feindliche Absicht (I). In Zeiten des Ost-West-Konflikts war die Lage hier noch klar: Es gab einen Akteur (die Sowjetunion) mit einer feindlichen Intention (der Abschaffung des Kapitalismus) und einem gefährlichen Potenzial aus Atomwaffen mit Interkontinentalraketen, strategischen U-Booten und so weiter. Es bestand also in der Wahrnehmung der Sicherheitspolitiker eine klare Bedrohungslage.[2]

Mit dem Irak unter Saddam Hussein stellte sich aus Sicht der US-Regierung vor der Invasion 2003 das Problem anders dar. Die Logik ging ungefähr wie folgt: Der Akteur (A) Saddam Hussein hat feindliche Absichten (I). Er mag im Moment noch keine Fähigkeiten (P) haben, die den USA gefährlich werden könnten - die Inspekteure haben ja trotz jahrelanger Suche weder einsatzfähige Massenvernichtungswaffen noch Langstreckenraketen gefunden. Selbst wenn er sie hätte, könnte man unter dem alten Bedrohungsparadigma die klassische Abschreckungspolitik betreiben, die gegen die Sowjetunion immerhin jahrzehntelang funktioniert hat. Aber, so die Logik des Risikoparadigmas, das wäre zu riskant. Man weiß ja nicht, was er dann macht. Ist er wirklich so rational wie die Abschreckung es erfordert? Gibt er - entgegen allen Geheimdienstanalysen - vielleicht doch schmutzige Bomben an Terroristen weiter? Daher, so die Bush-Regierung, musste man *vorbeugend* handeln und den Irak *präventiv* angreifen. Nur so ist vollständige Sicherheit gewährleistet.

Die so genannte Bush-Doktrin und der Irak-Krieg 2003 waren aber nicht in ihrer theoretischen Konzeption neu, sondern lediglich in der Radikalität der Ausführung (Bendrath 2003). Die Zentrierung der sicherheitspolitischen Strategie um den Begriff des Risikos wurde

---

[2] Das Bedrohungsparadigma war allerdings schon seit der Ölkrise der 1970er Jahre unter Druck geraten und durch das Konzept „Sicherheit vor Verwundbarkeit" ergänzt worden, vgl. Daase (1991).

schon 1991 im „neuen strategischen Konzept“ der NATO festgeschrieben, die Vorarbeiten liefen bereits seit Sommer 1990. Auch die Bundeswehr ist diesem Trend gefolgt: “Risiko” ist einer der Kernbegriffe in den Grundlagenpapieren, die seit der deutschen Wiedervereinigung erstellt wurden, seien es Rühes “Verteidigungspolitische Richtlinien” von 1992 oder der Bericht der Weizsäcker-Kommission von 2000. Das letzte Weißbuch von 2006 konstatiert:

> „Unsere Sicherheitspolitik steht heute vor neuen und zunehmend komplexeren Herausforderungen. Grenzüberschreitende Risiken sowie inner- und zwischenstaatliche Konflikte fordern Deutschland auf neue Weise. Deshalb gilt es, Risiken und Bedrohungen für unsere Sicherheit vorzubeugen und ihnen rechtzeitig dort zu begegnen, wo sie entstehen“ (BMVg 2006: 19).

Diese Strategie der vorbeugenden Risikobekämpfung zeigt sich besonders deutlich im Kampf gegen den Terrorismus seit dem 11. September 2001.

Mit der Umstellung der sicherheitspolitischen Großstrategie von der Gefahrenabwehr auf die Risikobekämpfung ist es allerdings nicht getan. Hinzu kommt der Wandel in der Akteurskonzeption – weg von Staaten, hin zu Individuen oder transnationalen Gruppen. Bei einem “Schurkenstaat” wie dem Irak unter Saddam Hussein war das Bedrohungsdreieck nämlich zumindest teilweise noch vorhanden: Man hatte einen benennbaren Akteur mit einer feindlichen Intention. Was aber macht man, wenn man schon den feindlichen Akteur gar nicht mehr kennt, sondern nur das Risiko vermutet, dass irgendwo in der Welt unfreundlich gesinnte Zeitgenossen herumlaufen, die möglicherweise in der Zukunft eine Gefahr werden könnten?[3] Hier, mit der Sicherheit vor nichtstaatlichen Akteuren, konvergieren äußere und innere Sicherheit.

Auch in Theorie und Praxis der Inneren Sicherheit finden wir den gleichen Trend. Es geht nicht mehr nur um die Strafverfolgung nach begangener Tat oder um die Abwehr konkreter, unmittelbar bevorstehender Gefahren, was die klassischen polizeilichen Aufgaben sind. Es geht zunehmend auch um Gefahren*vorsorge* oder Risikovorbeugung. Bereits seit 1989 kann in Deutschland in “Vorbeugehaft” genommen werden, wer lediglich im Verdacht steht, wiederholt schweren Landfriedensbruch begangen zu haben und von dem vermutet wird, dass er solches in Zukunft wieder tun werde. Das niedersächsische Polizeirecht erlaubt seit 1995 den “vorbeugenden Gewahrsam” von bis zu vier Tagen bei der vagen Annahme, dass jemand “eine Straftat begehen oder zu ihrer Begehung beitragen könnte”. Aus Repression wird so Prävention (Bendrath 1997).

Wie gesagt, Sicherheit ist Verfügung über die Zukunft. Nicht die Abwehr einer konkreten Gefahr steht laut der herrschenden Doktrin heute als Sicherheitsaufgabe an, sondern es gilt zu verhindern, dass aus Risiken in Zukunft Bedrohungen werden, die dann in noch weiterer Zukunft zu einem Schaden führen könnten. Die Unsicherheitswahrnehmung und damit die Herstellung von Sicherheit verlagern sich damit immer weiter in die Zukunft. Dies entspricht ebenfalls einem allgemeinen Trend der Moderne:

---

[3] Diesem Problem hat der damalige US-Verteidigungsminister Donald Rumsfeld (2002) mit der Rede von den „unknown unknowns“ zum geflügelten Wort verholfen.

> "The extrapolated or narrative future has replaced the historical past (which has receded behind museum-piece layers of simulation) as our most fundamental and decisive reference" (Shapiro 1997).

3 Die Rolle der Informationstechnologie

Die Prognose der Zukunft benötigt – wir kennen das von der Wettervorhersage – große Datenmengen und leistungsfähige Computer. Die Bekämpfung von Sicherheitsrisiken produziert entsprechend einen immensen Informationsbedarf. Natürlich waren Geheimdienstinformationen und andere Daten über die Interna des Kreml schon zu Zeiten des Bedrohungsparadigmas wichtig. Heute geht der Datenhunger aber weit darüber hinaus, weil man nicht mehr weiß, wo man nach gefährlichen Akteuren suchen muss. Prinzipiell verdächtig sind daher erst einmal alle. Also müssen über alle Daten gesammelt werden, um abschätzen zu können, ob jemand ein Sicherheitsrisiko darstellt. Gleichzeitig hat man mit moderner EDV die Technologie an der Hand, die solche Abschätzungen vermeintlich erlaubt.[4]

Wie läuft ein solcher Prozess ab, in dem beispielsweise entschieden wird, ob man ein Flugzeug betreten darf? Er besteht im Wesentlichen aus drei Elementen: Als *erstes* gibt es Daten über eine große Menge von Personen, etwa Flugpassagiere. Man weiß, von wo nach wo sie fliegen, was sie essen, ihre Kreditkartennummer, ihre Anschrift und Telefonnummer, aus anderen Quellen noch ihren Beruf oder ihr Studienfach, mit wem sie telefonisch und per Internet in Kontakt sind, ob sie bereits auffällig waren, welche Bücher sie in Bibliotheken ausleihen, was sie kaufen, und so weiter. Diese Daten fallen heute routinemäßig allerorten an, und seit den Sicherheitsgesetzen der letzten Jahre dürfen sie – natürlich mit nationalen Variationen – auch von staatlichen Stellen zum Zwecke der Terrorbekämpfung genutzt werden. Hier finden wir übrigens den Schritt von der Überwachungsgesellschaft zum Überwachungsstaat. Die meisten dieser Daten werden von privaten Unternehmen zu rein wirtschaftlichen Zwecken gesammelt, der gläserne Kunde ist eben ein besseres Marketingobjekt. Der Staat kann sich aber mittlerweile unter den Vorzeichen des Kampfes gegen den Terrorismus (oder die Kinderpornografie – die Begründungen sind hier oft austauschbar) recht einfach Zugang zu diesen Daten verschaffen (Haggerty/Ericson 2000). Damit wird der gläserne Kunde zum gläsernen Bürger.

Zum *Zweiten* hat man ein Modell, das aus einer Reihe von Indikatoren besteht, und das Annahmen darüber macht, bei welchen Werten in welchen Kombinationen von Indikatoren jemand ein Sicherheitsrisiko darstellt – also etwa ein potenzieller Selbstmordattentäter ist. Die Indikatoren können dabei etwa das Reiseverhalten, die Herkunft, die Religion, der Studiengang oder die Email-Kontakte der jeweiligen Person sein.

Mit diesem Modell wird *drittens* die große Menge an Daten über die betroffenen Bürger – also hier die Flugpassagiere – abgeglichen. Und genau hier besteht der entscheidende Schritt von der Bedrohung der Privatsphäre, wie sie Samuel Warren und Louis Brandeis 1890 gesehen haben, zu den heutigen Überwachungssystemen. Nicht nur die Aufzeichnung und

---

[4] Ich sage bewusst vermeintlich, darauf werde ich noch zurückkommen.

Verbreitung von Informationen über Menschen wird durch die Technologie in großem Umfang möglich, sondern auch das automatische Vergleichen und Sortieren dieser Informationen – und damit der Menschen, die sie betreffen. Der kanadische Soziologe David Lyon hat daher Überwachung als „soziales Sortieren“ oder „digitale Diskriminierung“ bezeichnet (Lyon 2003). Mit Bezug auf Foucault könnte man sagen: Aus „Überwachen und Strafen“ wird „Überwachen und Sortieren“.

Der gleiche Dreischritt von

- Daten über Personen sammeln,
- diese Daten mit einem Modell abgleichen,
- über Einstufung einzelner Person in eine Kategorie entscheiden

findet sich in allen möglichen gesellschaftlichen Bereichen. Das Verfahren wenden auch Unternehmen an, wenn sie abschätzen wollen, ob ihre Kunden an bestimmten Produkten interessiert sein könnten oder ob man bei ihnen eine Rechnung schickt oder Vorkasse verlangt. Hier sind es in der Regel Daten über das Einkommen, die Zahlungsmoral, den Lebensstil sowie Hobbies und andere Interessen. Die Modellbildung und automatische Sortierung entscheidet hier, welche Werbepost man im Briefkasten findet, ob man aufgrund der Schufa-Auskunft höhere Kreditzinsen zahlen muss als andere, oder ob man sehr lange im Callcenter einer Firma in der Warteschleife hängt. Ist Ihnen das schon mal passiert? Dann haben sie wahrscheinlich Ihre Rufnummernübermittlung nicht ausgeschaltet, und der Computer im Callcenter hat entweder erkannt, dass sie ein zu knauseriger Kunde sind oder dass sie in einem Umfeld wohnen, das nicht zur gefragtesten Zielgruppe der angerufenen Firma passt. Mit ein wenig Pech kann man aufgrund solcher computerbasierten Abschätzungen aber auch in Guantanamo oder zumindest im Verhörraum eines amerikanischen Flughafens landen.

Die Logik ist im Bereich staatlicher Terrorabwehr die gleiche wie im Bereich des Customer Relationship Management. Es ist die Logik der Sicherheit, und das heißt heute eben: der Risikovorsorge. Staatliche Einrichtungen wollen Anschläge verhindern, Unternehmen wollen Kostenfaktoren vermeiden, Banken wollen Kreditrisiken minimieren – und alle wollen mittels Prognosen die Verfügung über die Zukunft erreichen. Im Kern werden hier jeweils automatische Entscheidungen über einzelne Menschen gefällt auf der Basis von Annahmen über Personengruppen – Terroristen oder ordentliche Bürger, ungewollte oder begehrte Kunden. Mit diesem Verfahren sind – jenseits oberflächlicher juristischer und politischer Schwierigkeiten – drei strukturelle Probleme verbunden, die man als Problem der Modellbildung, als Problem der Probabilistik und als Problem der Definitionsmacht bezeichnen kann.

Zum Problem der Modellbildung: Was bei Werbesendungen oder Amazon-Kaufempfehlungen noch funktionieren mag, nämlich halbwegs interessierte Kunden anzusprechen, ist bei der Terrorismusbekämpfung hochproblematisch. Direktwerbefirmen können Daten über Millionen realer Käufer auswerten, um darauf ihre Annahmen über Trefferquoten zu stützen. Im Vergleich dazu ist aber die Anzahl der bekannten Terroristen einfach zu klein. Man kann damit keine validen statistischen Modelle erstellen, auf deren Basis man halbwegs seriöse, auf realen Wahrscheinlichkeiten abgestützte Prognosen abgeben

könnte. Was aus Sicht der Sicherheitsbehörden einen Terroristen auszeichnet, ist daher lediglich eine rudimentäre und oft hochproblematische Vermutung. Dadurch, dass diese Vermutung in Computerroutinen übersetzt wird, wird sie aber nun verdinglicht. Dem Computer werden die Normen und Vorurteile der Sicherheitspolitik eingeschrieben, und weil am Ende Zahlen oder Bewertungen auf dem Bildschirm erscheinen, erzeugt er die Illusion von Berechenbarkeit und damit von Sicherheit.

Zum Problem der Probabilistik: Selbst wenn die Datenbasis für saubere statistische Annahmen groß genug ist, ist ein realer Mensch etwas anderes als eine statistische Annahme. Nur weil man in einem Viertel mit geringem Einkommen lebt, muss man als individueller Mensch noch lange nicht wenig Geld haben. Und weil man kein Schweinefleisch isst und ein naturwissenschaftliches Fach studiert, ist man noch lange kein Terrorist. Es mag zwar eine gewisse Wahrscheinlichkeit bestehen, dass die Prognose zutrifft, aber mehr eben nicht. Das Problem ist: Während eine gewisse Streuung über die Zielgruppe hinaus bei Werbesendungen noch leicht zu verkraften ist, haben fehlerhafte Einschätzungen im repressiven Bereich staatlicher Sicherheitspolitik für die Betroffenen unmittelbar negative Konsequenzen. Hier sprechen die vielen *False Positives* der amerikanischen Flugverbotslisten Bände. Von dieser Art automatisch generierter Fehlprognose sind bereits einige Kongressabgeordnete und Senatoren betroffen gewesen (Schneier 2006).

Die Probleme der Modellbildung und der Probabilistik liegen auf der Ebene der Effektivität. Damit bewegen sie sich noch innerhalb der instrumentellen Rationalität der Sicherheitspolitik. In der Regel wird darauf mit noch mehr Datensammelei und verfeinerten Algorithmen reagiert. Dies scheint ein genereller Trend moderner Sicherheitspolitik zu sein: Während die Glücksgöttin Fortuna bei Macchiavelli, dem ersten Sicherheitstheoretiker der Neuzeit, noch systematisch berücksichtigt war, wird sie heute durch vermeintliche Berechenbarkeit und rationale Modelle der Risikoanalysten ersetzt. In der Militärpolitik wird ganz ähnlich auf die Clausewitzsche Friktion des Krieges, die in seinen Worten „den Krieg dem Kartenspiel am nächsten stellt“ (Clausewitz 1957: 32), heute mit chaostheoretischen Computersimulationen geantwortet (Watts 1996). Die zugrunde liegende Logik der Berechenbarkeit wird nicht aufgegeben.

Zum Problem der Definitionsmacht: Dieses Problem betrifft nicht die Effektivität der Sortierer und ihrer Algorithmen, sondern die informationelle Selbstbestimmung und letztlich die Menschenwürde der Betroffenen. Die Computermodelle der präventiven Sicherheit zeichnen sich nicht nur dadurch aus, dass sie die Menschen aufgrund automatischer Vergleiche in bestimmte Schubladen sortieren – wie im Märchen nach dem Motto „Die Guten ins Töpfchen, die Schlechten ins Kröpfchen“. Um diese Entscheidung fällen zu können, muss noch vorher bestimmt werden, nach welchen Kriterien dies geschehen soll. Die Modelle reduzieren daher bereits vorher jedes Individuum auf einen Satz von Daten. Wie die Datenfelder heißen und welche Werte sie annehmen können, ist dabei von den Sicherheitsapparaten oder den Unternehmen definiert. Man kann zwar teilweise durch Korrektur der Daten dafür sorgen, dass man in die richtige Schublade sortiert wird – aber die Schubladen und ihre Indikatoren selber erstellen andere. Das gleiche zeigt sich in ganz banalen Auswahlmenüs bei der Kundenregistrierung auf vielen Webseiten. Man darf zwar häufig angeben, ob man männlichen oder weiblichen Geschlechts ist, aber Zwischentöne oder

Antworten wie „ich weiß noch nicht“ sind nicht zugelassen (Nakamura 2002). Speziell in der Definitionsmacht darüber, was ein potenzieller Terrorist und damit ein Sicherheitsrisiko ist, zeigt sich der Kern des präventiven Sicherheitsstaats. Hier äußert sich die Souveränität des modernen Staates:

„Jede Benennungshandlung teilt die Welt in zwei Teile. (…) Unabänderlich ist eine solche Einschließung / Ausschließung ein Gewaltakt, der an der Welt verübt wird, und bedarf der Unterstützung durch ein bestimmtes Ausmaß an Zwang“ (Bauman 1995: 15). Daher „ist alles, was sich selbst definiert oder der machtgestützten Definition entzieht, subversiv“ (Bauman 1995: 21). Intoleranz „ist daher die natürliche Neigung der modernen Praxis“ (ebda.). Nicht umsonst heißt die Leitidee des New Yorker Polizeimodells „Zero Tolerance“.

Die verdinglichte Klassifizierung von Menschen durch den Computer ist also verdinglichte Souveränität und der typisch moderne Versuch, Eindeutigkeit und damit Sicherheit herzustellen. Nach höchstrichterlicher Rechtsprechung aus Karlsruhe ebenso wie laut der EU-Datenschutzrichtlinie verstößt es gegen die Menschenwürde, wenn eine Entscheidung mit negativen Konsequenzen für den Betroffenen allein durch eine Maschine gefällt wird (BVerfG 1983; EU 1995). Getan wird es dennoch.

4 Warum geht es immer weiter? Erklärungsansätze und Forschungsbedarf

Ich fasse zusammen: Sicherheit ist eine moderne Idee, deren Kern die Verfügung über die Zukunft ist. In den letzten Jahrzehnten haben sich die Definition der Unsicherheit und damit auch das handlungsleitende Paradigma der Sicherheitspolitik verschoben. Statt Bedrohungsabwehr geht es nun um Risikoprävention. Die Informationstechnologie macht es möglich. Sie erlaubt das großflächige, datenbankgestützte Entscheiden darüber, ob Menschen als wahrscheinliche Gefährder gelten. Aus Überwachen und Strafen wird Überwachen und Sortieren. Dabei gibt es jedoch sowohl massive Effektivitätsprobleme als auch schwere ethische Probleme.

Es stellt sich also die Frage: Warum geht diese Entwicklung dennoch immer weiter? Trotz einiger bremsender Urteile der Verfassungsgerichte und eines in letzter Zeit wieder wachsenden politischen Widerstandes gegen die Politik der inneren Sicherheit ist ja keine grundlegende Wende abzusehen. Ich will dafür drei mögliche Erklärungen anbieten, die aus verschiedenen Traditionen der Sozialwissenschaften stammen. Gleichzeitig werde ich jeweils skizzenhaft mögliche weitere Forschungsfelder daraus ableiten:

Zunächst die würdige Tradition der *Gesellschaftsdiagnose*. Ulrich Beck hat in seiner „Risikogesellschaft“ (Beck 1986) schon vor mehr als zwanzig Jahren auf diesen Trend hin zur Risikopolitik hingewiesen, sich leider aber kaum um „harte“ Sicherheitspolitik gekümmert. Ältere Texte von Herbert Marcuse (1994 [1967]) bis Jürgen Habermas (1969) haben bereits viel früher die instrumentelle Rationalität der technisch-naturwissenschaftlichen Welt analysiert und kritisiert. Die Verdinglichung der Herrschaft des Menschen über die Natur durch Technologie schlägt damit um in eine technische – also wiederum verdinglichte – Herrschaft des Menschen über den Menschen. Auch Arnold Gehlen hat diese These vertreten: Der Mensch wird vom *Homo Faber* zum *Homo Fabricatus*, sobald die Maschinenrationalität wieder auf Menschen angewandt wird (vgl. Habermas 1969: 82). Die Logik des präventiven

Sicherheitsstaates funktioniert in dieser Lesart etwa so: Das Sicherheitsparadigma macht die Bevölkerung zu Objekten der Sicherheitspolitik, und die Informationstechnologie macht das maschinengestützte Sortieren der Menschen als Herrschaftsobjekte möglich und rationalisiert es. Ob diese Beherrschung des Menschen durch die menschengemachte Technik selber noch beherrschbar ist, ob durch die gesamte Gesellschaft oder auch nur durch die Herren, blieb in dieser Debatte immer umstritten. Josef Weizenbaum (1977) hat etwa bezweifelt, dass so komplexe Systeme wie Computer noch rational auch nur im Sinne der Herren, also hier im Sinne einer präventiven Sicherheitslogik, kontrolliert werden können, während Ulrich Beck (1994) die Errichtung neuer politischer Institutionen fordert, die über die Wahl der Technik entscheiden sollen.

Bislang unterbelichtet ist hier, dass es innerhalb der instrumentellen Logik der technisch-wissenschaftlich-positivistischen Rationalität Varianz geben kann. Früher wurden Schädel vermessen, um die kriminogenen Prädispositionen von Individuen zu erschließen; gestern waren es Daten über ihre Lebensumstände; in Zeiten von Web 2.0 sind es ihre im Netz abgebildeten Sozialbeziehungen; morgen ist es die DNA? Wenn man diese Veränderungen im Vermessen und Sortieren der Menschen in den historischen Kontext einordnet, könnte man auch funktionalistisch antworten: Stärker individualisierte und hochmobile Gesellschaften benötigen notwendig Systeme, die den Bürgern, Behörden und Unternehmen verlässliche Interaktionen unter Bedingungen von Fremdheit ermöglichen – man kennt sich eben nicht mehr wie auf dem Dorf. Die technische Risikoabschätzung ersetzt also den sozialen Vertrauensvorschuss. Zu erklären wäre hier wiederum, welche *spezifischen* Elemente dieses Vertrauen jeweils erzeugen sollen.

Etwas konkreter und näher dran an den konkreten Techniken und maschinellen Systemen wäre eine Erklärung aus der Perspektive der *Techniksoziologie*. Mit ihr kann man die Überwachungsapparate als „großtechnische Systeme“ verstehen. Großtechnische Systeme sind komplexe Verknüpfungen von Normen, Praktiken und Technologien, die zu einem Gesamtsystem integriert sind (Vgl. Weingart 1989, Bechmann/Rammert 1992, Schneider 2001). Sie zeichnen sich durch zwei Eigenschaften aus: Die Tendenz zur Innovation, also die Unmöglichkeit des technischen Stillstandes, und die Tendenz zur Expansion, also das Bestreben, ihre Umwelt nach der eigenen Logik zu strukturieren (Weingart 1989). Der letzte Punkt verweist auf die inzwischen unter Verfassungsjuristen kursierende These, dass wir uns auf dem Weg in einen Polizeistaat befinden. Dessen Logik ist die gleiche: Zivile gesellschaftliche Bereiche wie Telekommunikation oder Verkehrsinfrastrukturen werden nach der Logik der Strafverfolgung und Risikovorsorge strukturiert. Dieses findet sich z.B. bei der Vorratsdatenspeicherung von Kommunikationsdaten, an der die Provider selber kein originäres Interesse haben und daher per Gesetz gezwungen werden sollen, aber auch bei dem Trend, urbane Architekturen so zu gestalten, dass es für Überwachungskameras keine toten Winkel mehr gibt.

An dieser Stelle wäre zu untersuchen, unter welchen Umständen spezifische sozio-technische Leitideen (Dierckes/Hoffmann/Marz 1992) sich gegen andere durchsetzen. Dies wird besonders dann relevant, wenn relativ offene großtechnische Systeme ins Visier konkurrierender Visionen geraten. Konkret: Woran liegt es, ob das Internet als „terroristisches Ausbildungscamp“ definiert wird, das kontrolliert und überwacht werden muss, oder es als

offener Kommunikationsraum, neue Öffentlichkeit und begünstigender und wünschbarer Teil der offenen Gesellschaft verstanden wird? Neben der aktuellen Diskurshoheit werden hier auch noch andere Variablen eine Rolle spielen, etwa die konkrete technische Struktur, das Vorhandensein von Regelungen begünstigenden „Flaschenhälsen“ oder die sicherheitspolitische Tradition des jeweiligen Landes.

Die dritte Perspektive wäre die der *politischen Ökonomie*. Sie knüpft hierbei an frühere Forschungen zum militärisch-industriellen Komplex an (Albrecht 1980, Hennes 2003). Die These wäre, dass man heute auch einen überwachungs-industriellen Komplex findet, der ein demokratisch kaum noch zu kontrollierendes Konglomerat aus Sicherheitspolitik und Sicherheitstechnologiewirtschaft bildet (ACLU 2004). Bislang kursieren in der (noch nicht akademischen) Debatte um den überwachungs-industriellen Komplex verschiedene Interpretationen: Im Marktmodell agiert die Sicherheits- und Überwachungsindustrie als Anbieter und die sicherheitspolitische Bürokratie als Nachfrager. Die Sicherheitsindustrie bietet immer wieder neue Technologien an, die dann von den Staaten gekauft werden. Zu fragen wäre hier, wann welche Ansätze sich am „Markt“ durchsetzen. Die Technologie kann nämlich im Sinne einer anderen Erklärung genauso als Lösung auf der Suche nach einem Problem (Cohen/March/Olsen 1972) angesehen werden. Die Beschaffung durch staatliche Stellen wäre entsprechend eine vermeintliche Problemlösung, bei der beide Seiten gewinnen: Die Firmen haben Aufträge, die Politiker „tun etwas“, und zusammen kann man noch den nationalen Forschungsstandort stärken und sich dabei gegenseitig feiern. Die Verbindung zwischen Unternehmen und Bürokratien ist allerdings in Teilbereichen mittlerweile so eng, dass man sie je nach Geschmack oder Publikum als „epistemische Gemeinschaft“ (Haas 1992), korporatistisches Arrangement oder einfach Filz bezeichnen kann.[5] Künftige Forschung in diesem Bereich hätte die Aufgabe, das Konzept des überwachungs-industriellen Komplexes weiter zu spezifizieren und theoretisch einzubetten, so dass spezifische Entscheidungen für konkrete Überwachungsprojekte erklärt werden können.

Dieser kurze Durchgang durch verschiedene Erklärungsmuster für den immer weiteren Ausbau der Apparate der Risikoprävention und damit des Sortierens und Klassifizierens von Menschen soll nur als Denkanstoß dienen. Welche von diesen drei Perspektiven die richtigere ist, vermag ich hier nicht beantworten, und für eine systematische Evaluation wäre viel mehr vergleichende empirische Forschung in diesem Politikfeld nötig.

5 Die normative Seite

Zum Abschluss möchte ich noch kurz auf das Verhältnis Staat-Bürger eingehen. Oft hört man die These, wer nichts zu verbergen hat, hätte auch nichts zu befürchten.

---

[5] Bekannt und auch öffentlich kritisiert wurde z.B. die Tätigkeit des früheren Bundesinnenministers Otto Schily für die Firmen „Safe ID Solutions“ und „Byometric Solutions“, die biometrische Ausweistechnologien und -datenbanken anbieten (Krempl 2006). Aber auch auf den ersten Blick unverdächtige EU-Forschungsverbünde zur Sicherheitstechnologie und andere Netzwerke an der Schnittstelle zwischen Sicherheitsunternehmen und Sicherheitspolitik sind in der Regel durch Einladungspolitiken, Habitus und auf vielfache andere Arten recht abgeschottet gegen Kritiker der präventiven Sicherheitspolitik (Bendrath 2006). Sie werden höchstens aus Akzeptanzgründen eingebunden.

Dem wären eine normative Setzung und zwei Fragen entgegenzuhalten. Die normative Setzung ist natürlich die Tatsache, dass das Recht auf Privatheit ein universelles Menschenrecht darstellt[6] und insofern geschützt werden muss, unabhängig von der immer schwankenden gesellschaftlichen Akzeptanz. Dieses rein normative Argument ist allerdings oft nicht leicht zu vermitteln. Daher wären zwei Fragen zu stellen, die den impliziten empirischen Annahmen der „nichts zu verbergen"-These auf den Grund gehen (Lohmann 2006).

Erstens: Hat man wirklich nichts zu befürchten? Diese Behauptung setzt ein enormes Vertrauen in die staatlichen und privaten Akteure voraus, die unsere Daten speichern, verwalten und auswerten. Gerade der Staat ist ja in jeder Hinsicht ein Risiko: Er ist ein mächtiger Akteur, der mit dem Gewaltmonopol über ein bedrohliches Potenzial verfügt. Die Frage ist dann: Welche Intentionen hat er? Die Geschichte zeigt ja zumindest immer wieder, dass diese über die Zeit nicht immer stabil sind, und dass zunächst „harmlose" Daten plötzlich für schwerste Menschenrechtsverletzungen genutzt wurden.[7]

Privatheit und Datenschutz sind damit auch Sicherheitsvorsorge der Bürger gegenüber dem übermächtigen Staat. Hier gilt es die Regel der bewussten Beschränkung des Missbrauchs- und Schadenspotenzials politischer Institutionen auch auf technische Infrastrukturen anzuwenden. Aus der Maxime "Wie können wir unsere politischen Einrichtungen so aufbauen, dass auch unfähige und unredliche Machthaber keinen großen Schaden anrichten können?" (Popper 1984, zit. nach Watzlawick 1997: 105) würde dann "Wie können wir unsere technischen Infrastrukturen so aufbauen, dass unfähige und unredliche Machthaber damit keinen großen Schaden anrichten können?"

Die zweite Frage ist: Hat der Staat eigentlich etwas zu verbergen? Er hält generell einen großen Teil seiner Informationen und deren Beschaffung geheim – nicht umsonst heißen die zuständigen Einrichtungen *Geheim*dienste. Er legt aber auch die technischen Sortiermechanismen nicht offen, aufgrund derer seine Bürger in Schubladen sortiert und als Risiken abgeschätzt werden.[8] Firmen machen das übrigens auch nicht: Die Algorithmen der Schufa zur Bewertung der Kreditwürdigkeit sind nicht veröffentlicht, genauso wenig wie die Methoden, nach denen Google seinen Kunden Werbung einblendet. Der Unterschied zwischen Firmen und dem Staat ist aber wie bereits erwähnt das Gewaltmonopol des letzteren. Wenn die Definitionsmacht und die Sortierung von Menschen wichtiger Teil staatlicher Souveränitätsausübung sind, dann sollten auch diejenigen Mitspracherechte bei den Parametern und Algorithmen bekommen, denen der Staat seine Souveränität verdankt – die Bürger.

---

[6] Vgl. die Allgemeine Erklärung der Menschenrechte, die Europäische Erklärung der Menschenrechte sowie das vom Bundesverfassungsgericht aus der Menschenwürde (Art. 1 GG) abgeleitete Grundrecht auf „informationelle Selbtbestimmung" (BVerfG 1983).

[7] Für eine Reihe drastischer Beispiele der Rolle von Bevölkerungsregistern im Kontext von Genoziden vgl. Selzer / Anderson (2001).

[8] Als Beispiel aus Deutschland: „Terrorverdächtigen" Ausländern wird vielfach das Arbeitslosengeld gesperrt, ohne dass sie erfahren, welches die Gründe für diesen Verdacht sind (Nowak 2005).

Was also tun, um die staatliche Macht gegenüber den Bürgern einzuhegen und zu begrenzen? Die Forderung nach dem „gläsernen Staat“ ist sicherlich berechtigt, wird aber nicht reichen. Natürlich kann man auch immer wieder die mangelnde Effektivität der Überwachungssysteme kritisieren oder versuchen, den Filz zwischen Sicherheitsindustrie und Sicherheitsbürokratie aufzudecken. Die Opposition gibt sich ja hier mehr oder weniger redliche Mühe. Im Kern, so scheint mir, ginge es aber um eine Abkehr von der Sicherheitslogik. Denn die Idee der Sicherheit ist der Antriebsmotor für das weitere Wachstum der Überwachungssysteme, und je höher erstere auf der öffentlichen Agenda steht, desto schneller werden letztere ausgebaut. Paul Watzlawick (1997) hat anhand der Hexen in Macbeth und ihrer Strategie sehr schön herausgearbeitet, wie Sicherheit ein trügerisches Gefühl ist. Am Ende führt nämlich die Illusion der Sicherheit zum Tod des Helden. Ich möchte daher mit Shakespeare schließen:

> „Dem Tod und Schicksal sprech' er Hohn,
> Nicht Gnad' und Furcht soll ihn bedrohn;
> Denn, wie ihr wisst, war Sicherheit
> Des Menschen Erbfeind jederzeit.“[9]

6 Literatur

ACLU [American Civil Liberties Union], 2004, The Surveillance-Industrial Complex, New York: ACLU. Online verfügbar: http://www.aclu.org/FilesPDFs/surveillance_report.pdf (Stand: 29.9.2007).

Albrecht, Ulrich, 1980, Militärisch-Industrieller Komplex (MIK), in: Wichard Woyke (Hg.): Handwörterbuch Internationale Politik, Opladen: Leske+Budrich.

Bauman, Zygmunt, 1995, Moderne und Ambivalenz. Das Ende der Eindeutigkeit. Frankfurt: Fischer.

Bechmann, Gotthard und *Volker Schneider*, 1992, „Großtechnische Systeme, Risiko und gesellschaftliche Steuerung“, Technik und Gesellschaft. Jahrbuch 6, Frankfurt a.M.: Campus.

Beck, Ulrich, 1986, Risikogesellschaft. Auf dem Weg in eine andere Moderne, Frankfurt/M.: Suhrkamp.

Bendrath, Ralf, 1997, Von „Freiheit stirbt mit Sicherheit“ zu „keine Freiheit ohne Sicherheit“? Über die Umwertung des Staates und das „Grundrecht auf Sicherheit“, antimilitarismus information, 27: 12, 11-20, auch erschienen als Online-Publikation in telepolis, 15.6.1998, http://www.heise.de/tp/deutsch/inhalt/co/3246/1.html (Stand: 30.7.2007).

Bendrath, Ralf, 2003, Vorbeugende Risikobekämpfung in der inneren und äußeren Sicherheit. Anmerkungen zum Neuigkeitswert der Bush-Doktrin, in: Dividuum 1:1. Online verfügbar: http://userpage.fu-berlin.de/~bendrath/Bendrath-Dividuum.rtf (Stand: 30.6.2007).

[9] William Shakespeare: Macbeth, III/5, Übersetzung: Dorothea Thieck, zit. nach Watzlawick (1997: 8).

Bendrath, Ralf, 2006, The European way: “Surveillance while protecting privacy”, Online-Publikation: http://bendrath.blogspot.com/2006/10/european-way-surveillance-while.html (Stand: 25.9.2007).

BMVg [Bundesministerium der Verteidigung], 2006, Weißbuch zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr, Berlin, Online verfügbar: http://www.weissbuch.de (Stand: 30.7.2007).

BVerfG [Bundesverfassungsgericht], 1983, BVerfGE 65, 1 – Volkszählung. Urteil des Ersten Senats vom 15. Dezember 1983. Online verfügbar: http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm (Stand: 30.7.2007).

Clausewitz, Carl von, 1957 [1834]: Vom Kriege, eingeleitet von Ernst Engelberg und Otto Korfes, Berlin (DDR): Ministerium für Nationale Verteidigung.

Cohen, Michael; James G. March, und *Johan P. Olsen*, 1972, A Garbage Can Model of Organizational Choice; In: Administrative Science Quarterly 17:1, 1-25.

Daase, Christopher, 1991, Bedrohung, Verwundbarkeit und Risiko in der „Neuen Weltordnung“. Zum Paradigmenwechsel in der Sicherheitspolitik, in: antimilitarismus information, : 21: 7, 13-21.

Daase, Christopher, 1993, Sicherheitspolitik und Vergesellschaftung. Ideen zur theoretischen Orientierung der Sicherheitspolitischen Forschung, in: Christopher Daase, Susanne Feske, Bernhard Moltmann, Claudia Schmidt (Hg.): Regionalisierung der Sicherheitspolitik. Tendenzen in den internationalen Beziehungen nach dem Ost-West-Konflikt, Baden-Baden: Nomos.

Dierkes, Meinolf, Ute Hoffmann und *Lutz Marz*, 1992, Leitbild und Technik. Zur Entstehung und Steuerung technischer Innovationen, Berlin: edition sigma 1992.

EU [Europäische Union], 1995, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 24. Oktober. Online verfügbar: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm (Stand: 17.9.2007)

Haas, Peter M., 1992, Banning Chlorofluorocarabons. Epistemic Community Efforts to Protect Stratospheric Ozone, in: International Organization 46:1,187-224.

Habermas, Jürgen, 1969, Technik und Wissenschaft als „Ideologie“, Frankfurt a.M.: Suhrkamp.

Haggerty, Kevin D. und *Richard V. Ericson, Kevin D.*, 2000, The surveillant assemblage, British Journal of Sociology 51: 4, 605–622.

Hennes, Michael, 2003, Der neue Militärisch-Industrielle Komplex in den USA, in: Aus Politik und Zeitgeschichte, Nr. 46. Online verfügbar: http://www.bpb.de/publikationen/U6A0BW (Stand: 17.9.2007).

ICAMS [International Campaign Against Mass Surveillance], 2005, The Emergence of a Global Infrastructure for Mass Registration and Surveillance, Online-Publikation: http://www.i-cams.org/ICAMS1.pdf (Stand: 17.9.2007).

Kaufmann, Franz-Xaver, 1973, Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften, Stuttgart: Ferdinand Enke.

Krempl, Stefan, 2006, Ex-Innenminister Schily berät künftig Biometrie-Firmen, heise news, 10.8. Online-Publikation: http://heise.de/newsticker/meldung/76682 (Stand: 25.9.2007).

Lohmann, Michael, 2006, „Wer nichts zu verbergen hat, hat auch nichts zu befürchten“, in: telepolis, 27.9., Online-Publikation: http://www.telepolis.de/r4/artikel/23/23625/1.html (Stand: 30.7.2007).

Lyon, David (Hg.), 2003, Surveillance as Social Sorting. Privacy, Risk, and Digital Discrimination, London / New York: Routledge.

Mayer-Schönberger, Viktor, 1998, Generational Development of Data Protection in Europe, S. 219-241, in: *Philip E. Agre* und *Marc Rotenberg* (Hg.), Technology and Privacy: The New Landscape, Cambridge/Mass: MIT Press.

Marcuse, Herbert, 1994 [1967], Der eindimensionale Mensch. Studien zur Ideologie der fotgeschrittenen Industriegesellschaft, München: Deutscher Taschenbuch Verlag.

Nakamura, Lisa, 2002, Cybertypes. Race, Ethnicity, and Identity on the Internet, New York: Routledge.

Nowak, Peter, 2005, Kafka in Europa, Telepolis, 26.12.2005, Online-Publikation: http://www.telepolis.de/r4/artikel/21/21658/1.html (Stand: 30.7.2007).

Popper, Karl R., 1984, Woran glaubt der Westen, in: Auf der Suche nach einer besseren Welt, München: Piper.

Prosser, William L., 1960, Privacy, California Law Review 48:3, 383-423.

Richards, Neil M. und *Daniel J. Solove*, 2007, Privacy's Other Path: Recovering the Law of Confidentiality. Georgetown Law Journal. Online verfügbar: http://ssrn.com/abstract=969495 (Stand: 30.6.2007).

Roth, Wolf-Dieter, 2006, "Bitte nicht so laut, sonst wacht die Kamera auf!", Telepolis, 28.11.2006, Online-Publikation, http://www.heise.de/tp/r4/artikel/24/24088/1.html (Stand: 25.9.2007).

Rumsfeld, Donald H., 2002, Transforming the Military, in: Foreign Affairs 81:3, 20-32.
Shapiro, Alan, 1997, The Star trekking of Physics, in: Ctheory, Article 52, Online-Publikation: http://www.ctheory.net/articles.aspx?id=95 (Stand: 30.7.2007).

Seltzer, William und *Margo Anderson*, 2001, The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses, in: Social Research, Nr. 2, 481-513. Online verfügbar: http://www.findarticles.com/p/articles/mi_m2267/is_2_68/ai_77187772 (Stand: 30.7.2007).

Schneider, Volker, 2001, Die Transformation der Telekommunikation. Vom Staatsmonopol zum globalen Markt (1800-2000), Frankfurt a.M.: Campus.

Schneier, Bruce, 2006, Automated Targeting System, Online-Publikation: http://www.schneier.com/blog/archives/2006/12/automated_targe.html (Stand 30.7.2007).

Watzlawick, Paul, 1997, Vom Schlechten des Guten oder Hekates Lösungen, München: dtv.

Warren, Samuel D. und *Louis D. Brandeis*, 1890, The Right to Privacy, Harvard Law Review 4: 5, 193-220.

Watts, Barry D., 1996, Clausewitzian Friction and Future War, Washington D.C.: National Defense University Press.

Weingart, Peter, 1989, ”Großtechnische Systeme” - ein Paradigma der Verknüpfung von Technikentwicklung und sozialem Wandel? in: ders. (Hg.), Technik als sozialer Prozess, Frankfurt/M.: Suhrkamp, 174-196.

Weizenbaum , Joseph, 1977, Die Macht der Computer und die Ohnmacht der Vernunft Frankfurt a.M.: Suhrkamp.

Wolfers, Arnold, 1962, Discord and Collaboration: Essays on International Politics, Baltimore: The Johns Hopkins Press.

Zum Autor

Ralf Bendrath, Dipl.Pol., ist wissenschaftlicher Mitarbeiter am Sonderforschungsbereich „Staatlichkeit im Wandel“ an der Universität Bremen und beschäftigt sich vor allem mit Internet-Governance, Datenschutz und Legitimationsfragen internationaler Politik. Er ist „hard blogging scientist“ bei http://bendrath.blogspot.com und http://www.netzpolitik.org.

Der Beitrag basiert auf einem Vortrag, den der Autor am 28.6.2007 im Rahmen der Ringvorlesung „Sicherheit“ des Forum Siegen gehalten hat.

Bitte diesen Artikel wie folgt zitieren:

Bendrath, Ralf (2007): Der „gläserne Bürger“ und der vorsorgliche Staat. Zum Verhältnis von Überwachung und Sicherheit in der Informationsgesellschaft. In: kommunikation@gesellschaft, Jg. 8, Beitrag 7. Online-Publikation: http://www.soz.uni-frankfurt.de/K.G/B7_2007_Bendrath