Peter Schaar

Peter Schaar, geboren 1954 in Berlin, studierte Volkswirtschaftslehre an der Freien Universität Berlin und den Universitäten Frankfurt am Main und Hamburg und ist seit fast 20 Jahren in verschiedenen Funktionen im Bereich des Datenschutzes tätig. Seit Ende 2003 ist er Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Neben zahlreichen Zeitschriften- und Buchbeiträgen sind von ihm die Bücher „Datenschutz im Internet“ (2002) und „Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft“ (2007) erschienen.

Kontakt Peter Schaar
Der Bundesbeauftragte für den
Datenschutz und die Informationsfreiheit
Husarenstraße 30
53117 Bonn
Deutschland

Technisch ist eine Totalüberwachung schon heute möglich

Adelbert Reif im Gespräch mit dem Datenschutzexperten Peter Schaar

Computer, Internet, ISDN- und Mobiltelefonie, RFID-Chips, Videokameras, Drohnen, Biometrie und weitere, in den letzten Jahren immer mehr verfeinerte Informationstechniken stehen heute den staatlichen Organen zur Überwachung jedes einzelnen Bürgers zur Verfügung. Eine Folge davon ist, dass die staatliche Datensammelwut immer extremere Ausmaße angenommen hat: „Großer Lauschangriff", Zusammenarbeit von Geheimdiensten und Polizei, Vorratsdatenspeicherung, Scoring lauten einige der Stichworte, die das Ausforschungsbestreben des Staates – und zum Teil auch der Wirtschaft – charakterisieren. In seinem kürzlich erschienenen Buch „Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft" (C. Bertelsmann Verlag, München) schildert der Datenschutzexperte Peter Schaar die brisante, den Kern unserer Demokratie bedrohende Entwicklung. Schaar plädiert für eine globale Ethik im Informationszeitalter, die auf Verantwortung statt auf Kontrolle setzt.

conturen: Herr Schaar, an einer Stelle seines berühmten Buches „Die Welt von Gestern" hat Stefan Zweig den Schutz der Privatsphäre und damit die Integrität der Persönlichkeit in den europäischen Gesellschaften vor dem Ersten Weltkrieg verglichen mit ihrer danach folgenden Preisgabe unter den diktatorischen und totalitären Regimen. Inzwischen hat diese Preisgabe längst Orwell'sche Dimensionen angenommen. Leben wir bereits in einem Überwachungsstaat?

Intensität nimmt zu

Schaar: Der zentrale Unterschied zur Entwicklung in den 30er-Jahren des letzten Jahrhunderts besteht darin, dass die Technik heute eine unvergleichlich intensivere Überwachung ermöglicht. Die Überwachungstechniken zeichnen sich durch eine enorme Vielfältigkeit aus. Dabei geht es zum einen um die „offene Überwachung", beispielsweise mit Videokameras, wobei der Trend zu immer kleineren bis hin zu versteckten, das heißt mehr oder weniger unsichtbaren Videokameras geht. Zum anderen haben wir ein ganzes Spektrum von unsichtbaren elektronischen Überwachungsmöglichkeiten.

Kritische Alltagsregistrierung

Für besonders kritisch halte ich die so genannte „Alltagsregistrierung", die stattfindet ohne expliziten Überwachungszweck, aber mit der Möglichkeit, die dabei entstehenden Daten zur Profilbildung des einzelnen zu nutzen. Dabei handelt es sich um jene Da-

Die Datenverarbeitung ist allgegenwärtig

ten, die anfallen, wenn man das Handy anschaltet, ein Telefonat führt oder das Internet benützt. Schon heute spricht man von „ubiquitous Computing“, also von einer allgegenwärtigen Datenverarbeitung. Wenn ein Staat sich dieser Mittel bedient – und die modernen Staaten bedienen sich fast alle in zunehmendem Maße aller drei Überwachungsansätze –, dann kommt man einer Rundumüberwachung immer näher. Technisch ist eine Totalüberwachung schon heute möglich. Glücklicherweise leben wir in einem demokratischen Staat, in dem diese Totalüberwachung noch nicht ausgeübt wird und in dem eben – noch – nicht alle Daten miteinander verknüpft werden.

conturen: Milliarden von Informationen über Hunderte Millionen von Menschen werden heute Stunde für Stunde, Tag für Tag kreuz und quer in der Welt übermittelt. Worin besteht bei einer solchen kaum vorstellbaren Menge von Daten der Nutzen der erlangten Informationen?

Suchmaschinen demonstrieren rasendes Tempo der Datensuche

Schaar: Das Argument, dass die Verarbeitungskapazitäten selbst nicht ausreichen würden, um diese anfallende Datenmenge auszuwerten, gilt im Zeitalter von Google & Co. nicht mehr. Bedenken Sie, welche unglaublichen Informationsmengen in Sekundenschnelle ausgewertet werden, wenn Sie eine Anfrage an eine moderne Suchmaschine richten. Und natürlich werden diese Techniken auch von immer mehr Unternehmen, vor allem aber von staatlichen Stellen genutzt, um vergleichbar große Informationsmengen auszuwerten.

Der Mensch als Schwachstelle bei der Auswertung

Was den Sinn des Ganzen betrifft, habe ich häufig das Gefühl, dass diejenigen, die die menschliche Intelligenz aufbringen müssten, um Informationen auszuwerten, den Engpassfaktor darstellen. Berichte über die Terroranschläge von 2001 in New York und Washington und ihre Vorbereitung dokumentieren: Die Informationen waren vorhanden, sie wurden aber nicht als relevant erkannt. Und darin liegt das zentrale Problem. Die heutige Vorstellung zielt dahin, auf Vorrat alle möglichen Informationen zu sammeln, auszuwerten und zwar über unverdächtiges Verhalten, um abweichendes Verhalten zu erkennen. Die Erkenntnis abweichenden Verhaltens bedeutet aber noch nicht die tatsächliche Identifizierung des Verdächtigen oder Gefährlichen. Stattdessen sieht sich eine Vielzahl von Personen, die in diesem Raster hängen bleibt, einem verstärkten Rechtfertigungszwang ausgesetzt, ohne dass damit wirklich mehr Sicherheit verbunden wäre, weil man die wirklichen Gefährder eben meistens nicht erkennt, weil sie sich gerade nicht „abweichend“ verhalten.

Zunehmender Zwang zur Rechtfertigung ohne Gewinn an Sicherheit

conturen: Lässt sich denn mit der staatlicherseits betriebenen Informations- und Datensammelwut eine entschieden gewollte, gezielte terroristische Attacke verhindern?

Ein Bündel von Maßnahmen

Schaar: Das ist ganz schwer zu sagen. Ich glaube nicht, dass man allein aufgrund der Auswertung von unglaublichen Datenmengen im vorhinein feststellen kann, wo etwas passieren wird und wer die Täter sein werden. Dazu bedarf es nach wie vor ganz gezielter polizeilicher, kriminalistischer, vielleicht auch nachrichtendienstlicher Maßnahmen, die sich gegen bestimmte Personen oder

Gruppen richten. Dagegen erhebe ich als Datenschützer auch keine Einwände. Denn ich bin selbst daran interessiert, dass unsere Behörden in die Lage versetzt werden, grausame Anschläge möglichst zu verhindern. Tatsächlich wurde aber der Blick sozusagen umgedreht. Die Idee, das normale Verhalten zu überwachen, um das abweichende frühzeitig zu erkennen, bedingt, dass unser aller Verhalten möglichst umfassend registriert wird.

Normales Verhalten wird umfassend registriert

Ganz massiv sieht man das in den USA, wo eine ganze Reihe von Maßnahmen in dieser Richtung eingeführt wurde. Wer in die USA einreisen möchte, dessen Verhalten, Kreditkartendaten, E-Mail- und Telefondaten werden exzessiv registriert und ausgewertet. Außerdem wurden die Regeln zur Internet- und Telefonüberwachung in den USA insbesondere bei Auslandsbezug kürzlich erheblich gelockert, so dass es auch hier keines individuellen Verdachts mehr bedarf, um eine Überwachungsmaßnahme anzuordnen. Mit diesem generellen Präventionsansatz gibt es praktisch keine Räume mehr, die nicht überwacht werden müssen, weil ja derjenige, der Böses plant, solche überwachungsfreien Räume nutzen könnte. In der Konsequenz hätten wir dann durchaus gefährliche Tendenzen in Richtung auf einen „Überwachungsstaat", in dem die Privatsphäre immer weiter eingeschränkt wird.

Negatives Vorbild USA

Einschränkung der Privatsphäre

conturen: Auf welche hauptsächlichen „Ziele" konzentriert sich das Interesse der staatlichen Informations- und Datenspeicherung gegenwärtig?

Schaar: Hier muss man unterscheiden zwischen der offiziellen Begründung und der Realität. Nehmen wir zum Beispiel den „Kontodatenabruf". Er wurde in Deutschland im Jahr 2002 unmittelbar nach den Anschlägen vom September 2001 eingeführt mit der Begründung, es ginge um die Aufdeckung der Terrorismusfinanzierung. Mit diesem Argument konnte man durchsetzen, dass die deutschen Banken bestimmte Informationen über ihre Kunden und deren Konten in eine Datenbank einspeisen müssen, aus der diese Daten dann von Behörden abgerufen werden können. Zugleich wurde ausdrücklich erklärt, dass die Finanzbehörden keinen Zugang zu diesen Daten bekommen würden. Heute hat nicht nur jedes deutsche Finanzamt Zugang zu diesen Daten, sondern auch die Sozialbehörden, die Bundesagentur für Arbeit, die Bafögstellen und eine Vielzahl weiterer Behörden darf inzwischen auf diese Daten zugreifen. Ich wage die Vermutung, dass die Zugriffe zur Terrorismusbekämpfung weit unter einem Prozent ausmachen. Die zur angeblichen Terrorismusbekämpfung eingeführte Maßnahme wird also in der Realität zu ganz anderen Zwecken eingesetzt. Das führt zu einer großen Skepsis gegenüber allen Versprechungen des Staates, geforderte neue noch weiter gehende Befugnisse seien ausschließlich zur Terrorismusbekämpfung erforderlich. Die Erfahrung zeigt ja, dass solche Befugnisse häufig im Laufe der Zeit eben nicht bloß zu diesem Zweck eingesetzt werden.

Nur eine Minderheit der Datenabfragen dient der Terrorbekämpfung

conturen: In Ihrem Buch verweisen Sie auf die Gefahr, dass die ungeheure Menge der auf Vorrat zu speichernden Daten weitere

Begehrlichkeiten wecken wird. Rechnen Sie mit einer Steigerung des Informations- und Datensammelns?

Schaar: Das Sammeln ist ja eine natürliche menschliche Verhaltensweise. Und es ist uns allen nicht fremd ist, etwas als nützlich oder scheinbar nützlich Erkanntes verbessern, erweitern, ausbauen zu wollen. Nehmen wir die Speicherung der IP-Nummern, also der Internetadressen auf Vorrat: Wirklich aussagekräftig werden diese Daten erst, wenn der Staat auch weiß, welche Seite der Internetnutzer aufgerufen hat. Der nächste Schritt wäre also, auch diese Information über das eigentliche Nutzungsverhalten zu speichern. Das ist zwar noch nicht realisiert, aber ich bin mir sicher, dass Forderungen nach der Ausweitung der Vorratsspeicherung bald kommen werden, zumal wenn die Anbieter von Internetinhalten dazu übergehen, wie das beispielsweise in Deutschland gesetzlich verpflichtend ist, diese detaillierten Nutzungsdaten, also darüber, wer welche Internetseite aufgerufen oder welche Suchanfrage gestellt hat, zu löschen.

Nutzungsverhalten wird in Zukunft möglicherweise bis ins Detail registriert

Ich unterstelle weder den Innenministern noch den Chefs der Nachrichtendienste oder einem Polizeipräsidenten, dass sie Tag und Nacht überlegen, wie sie die Rechte der Bürger abbauen oder einschränken können. Das ist nicht der Ansatz. Als Verantwortungsträger liegt ihnen vor allem daran, ihre Aufgabe besser zu erfüllen. Von daher gibt es niemanden, den wir als „Big Brother", als „Großen Vordenker", als „Symbol des Schlechten" im Sinne der Orwell-Analogie bezeichnen könnten. Vielmehr haben wir es mit Entwicklungen zu tun, die – einzeln betrachtet – sogar manches Argument für sich haben, in ihrer Gesamtheit aber zu untragbaren Konsequenzen führen.

Den „Big Brother" gibt es nicht

conturen: „RFID-Technik für Ausweispapiere und Geldscheine", „Flugpassagiere im Visier der EU", „Zentrale Schülerdatenbank", „Weitergabe von Finanzdaten an die USA", „Forschung will Anti-Terrortechnologien stärken", „Verstärkte Videoüberwachung in den Städten", „Drohnen über Problemvierteln" – Zeitungsüberschriften wie diese beleuchten die bereits bestehende Bandbreite der Datenerfassung...

Schaar: Aus diesen Schlagzeilen wird nicht nur der staatliche Anteil an diesen Überwachungs- und Kontrollmaßnahmen unserer Gesellschaft erkennbar, sondern auch der Anteil privater Stellen. Zugrunde liegt diesen Maßnahmen die Vorstellung, man könne mit Überwachung tatsächlich Risiken vorbeugen oder bekämpfen. Dabei führt schon ein kurzes Nachdenken zu dem Ergebnis, dass die Dinge so einfach nicht liegen. Ein gutes Beispiel dafür bietet die Videoüberwachung. Von London heißt es, es sei die am besten videoüberwachte Metropole der Welt. Und trotzdem steht London nach wie vor einem unglaublich intensiven Kriminalitätsproblem gegenüber. Die Gefahr, überfallen oder vergewaltigt zu werden, ist in London wesentlich größer als in jeder anderen europäischen und sogar nordamerikanischen Großstadt.

Nicht nur der Staat kontrolliert, das tun auch private Stellen

Werfen wir einen Blick auf unsere eigenen U- oder S-Bahnhöfe. Auf ihnen gibt es schon seit langem kein Dienstpersonal mehr. Stattdessen sind an allen möglichen Punkten Videokameras instal-

Videokameras ersetzen Wachpersonal

liert. Wenn man tatsächlich auf einem dieser Bahnhöfe Opfer einer Straftat wird oder auch nur Hilfe benötigt, weil man gestürzt ist und sich aus eigener Kraft nicht erheben kann – dann wird man auf diese Hilfe womöglich vergeblich warten, weil die von den Überwachungskameras gelieferten Bilder zum großen Teil gar nicht ausgewertet werden, sondern nur auf Videobänder laufen und bisweilen hat eine Überwachungskraft 30 Monitore zu beobachten. Was hier geschaffen wurde, ist ganz überwiegend eine Scheinsicherheit und sie wird überdies bezahlt mit einem Verlust an Freiheit.

Bei kriminellen Delikten oder Unglücksfällen wenig Chancen auf Hilfe

conturen: Dass auch die Wirtschaft ein starkes Interesse an immer mehr Daten an den Tag legt, ist bekannt. Wie weit verzweigt sind diese Interessen nach Ihren Beobachtungen?

Schaar: Überwachung ist ein Thema im Verhältnis Unternehmer – Mitarbeiter ebenso wie im Verhältnis Unternehmer – Kunden. Was das Verhältnis Unternehmer – Mitarbeiter anbelangt, so haben wir es im Prinzip mit einem Machtgefälle zu tun. Der Arbeitgeber verfügt über die Arbeitsmittel und kann im Rahmen von Vorstellungsgesprächen Fragen stellen, die unstatthaft sind. An diesem Punkt fängt es im Grunde schon an. Denn auch durch gesetzliche Maßnahmen lässt sich nicht verhindern, dass ein Arbeitgeber oder Arbeitsvermittler über einen Stellenbewerber im Internet recherchiert, was dieser einmal irgendwo geäußert hat, welche politischen Auffassungen er tatsächlich oder vermeintlich vertritt, oder ob irgendwelche diskreditierenden Bilder oder abschätzige Bemerkungen von ihm vorhanden sind. So dürfte jeder gut beraten sein, bei seinen Äußerungen im Netz Vorsicht walten zu lassen.

Überwachung am Arbeitsplatz und durch Arbeitgeber

Was das normale Arbeitsleben betrifft, kann die Nutzung von technischen Systemen – sei es die elektronische Registrierkasse oder der PC, an dem Texte produziert oder Buchungsvorgänge abgewickelt werden – heute sehr viel stärker überwacht werden, als das in der Vergangenheit der Fall war. Wenn früher ein Mitarbeiter in ein paar „ruhigen Minuten“ während der Arbeitszeit die Zeitung las, hatte das für gewöhnlich keine Folgen, surft er heute im Internet, hinterlässt das Spuren und der Arbeitgeber könnte diese auswerten, was er auch häufig genug tut. E-Mails, die an die dienstliche Mail-Adresse gerichtet sind, können gegebenenfalls parallel an den Chef weitergeleitet werden. Auch solche Fälle gibt es. In den USA ist das, wie ich gehört habe, sogar sehr verbreitet. Ich sehe deshalb die Notwendigkeit eines besonderen gesetzlichen Schutzes gegen eine ausufernde Überwachung im Arbeitsleben und trete für ein Arbeitnehmerdatenschutzgesetz ein.

Nutzung technischer Systeme ist heute viel leichter kontrollierbar als früher

Für ein Arbeitnehmerdatenschutzgesetz

conturen: Sie nannten vorhin auch das Verhältnis Unternehmer – Kunden: Welches Ausmaß hat die Auskundschaftung von Kundendaten angenommen?

Schaar: Da haben wir es mit zwei Arten von Interessen zu tun. Das eine Interesse ist darauf gerichtet, Kunden an sich zu binden. Das setzt voraus, deren individuelle Neigungen und Verhältnisse so gut wie möglich zu kennen, damit man den Einzelnen sehr individuell mit Werbung versorgen oder als Kunden an sich binden kann. Die zweite Interessendimension der Wirtschaft besteht in der Risiko-

Kunden unter der Lupe

Vermeidung von Risiken birgt das Risiko der Stigmatisierung

vermeidung. Und dieses Interesse ist besonders problematisch, weil dabei der Einzelne im Hinblick auf sein tatsächliches Verhalten, aber auch hinsichtlich seiner Zugehörigkeit zu einer beliebigen statistischen Risikogruppe bewertet wird.

Ein typisches Beispiel ist die Kreditwürdigkeitsprüfung, wie sie in den Vereinigten Staaten schon vor mehr als 50 Jahren gehandhabt wurde. Damals kennzeichnete man die verschiedenen Wohngebiete in Städten mit unterschiedlichen Farben. Das schlechteste Rating hatten die rot umrandeten Bezirke. Deshalb nannte man diese Methode auch „Redlining“: Wer in einem solchen Bezirk wohnte, der konnte sich gleich die Mühe sparen, einen Kredit zu beantragen. Denn er hatte keine Chance, ihn zu bekommen. Das führte dazu, dass jeder, der es sich auch nur einigermaßen leisten konnte, diesen Stadtteil verließ. Noch heute kann man in vielen amerikanischen Städten die katastrophalen Folgen dieser sozialen Brandmarkung feststellen. Die moderne Form des dieses „Redlining“ ist das Scoring, bei dem es ebenfalls darum geht, bestimmte Merkmale zu listen und zu entschlüsseln. Dazu kann gehören, wie häufig jemand umzieht, seine Kontoverbindung ändert oder seinen Arbeitsplatz wechselt. Für sich genommen, sagt jede dieser Informationen nichts über die Kreditwürdigkeit aus. Wird aber ein statistischer Zusammenhang vermutet, kann dies dazu führen, dass der einzelne mehr Zinsen zahlen muss oder schlimmstenfalls überhaupt keinen Kreditvertrag, Mietvertrag oder Handyvertrag mehr bekommt. Aus meiner Sicht bedeutet das eine neue soziale Diskriminierung. Auch das beliebte Argument, man habe ja nichts zu verbergen, weil man sich nichts habe zuschulden kommen lassen, gilt schon angesichts solcher abstrakten Risikobetrachtungen nicht, weil man ja kaum Einfluss auf die Bewertung ausüben kann.

Katastrophale Folgen sozialer Brandmarkung

Betroffene können Bewertung der Daten kaum beeinflussen

conturen: Wenn wir nun Europa in den Blick nehmen: Hält die Informations- und Datensammelwut in den einzelnen Ländern der EU ungefähr den gleichen Stand?

Schaar: Es liegen nur wenige internationale Vergleichsstudien vor. Was die Überwachung des öffentlichen Raums anbelangt, nimmt Großbritannien einen Spitzenplatz ein. Bei der Speicherung von Telekommunikationsdaten stehen Staaten wie Italien und auch die skandinavischen Länder weit vorn. In Skandinavien haben wir auch – und dies schon geradezu traditionell – eine wesentlich stärkere Registrierung sämtlicher steuerrelevanter Informationen als anderswo. Aber solche Vergleiche sind immer mit Vorsicht zu genießen.

Schwierige Vergleichbarkeit bei europäischen Staaten

conturen: In welchen Bereichen der Datenerfassung wird eine globale Vernetzung angestrebt?

Schaar: Ich sehe zwei Bereiche, in denen eine solche globale Vernetzung zunehmend stattfindet. Zum einen entstehen immer mehr Informationen bei der elektronischen Kommunikation und die Datenströme über das Internet wachsen von Tag zu Tag. Sowohl staatliche Stellen als auch Unternehmen tauschen auf diesem Weg auch persönliche Informationen aus. Unsere Daten rasen in Sekundenbruchteilen um den Globus und es ist für den Einzelnen zu-

Immer mehr Datenströme im Internet

nehmend schwierig herauszufinden, welche Stelle gerade seine Daten verarbeitet und ob dies in Europa, den USA oder in Indien geschieht.

Globale Datenauswertung ist möglich

Das zweite Feld internationaler Vernetzung staatlicher Sicherheitsbehörden sind die so genannten biometrischen Angaben. Für besonders sensibel halte ich hier insbesondere die Fingerabdrücke. Wenn ich in die USA einreise, muss ich derzeit noch zwei Fingerabdrücke abgeben, in Zukunft werden es zehn sein, die über viele Jahre gespeichert bleiben und mit allen möglichen Datenbanken abgeglichen werden. Japan hat jüngst angekündigt, dass es ebenso verfahren will. Im Irak werden die US-Truppen mit tausenden mobilen Fingearabdruckscannern ausgerüstet und die Soldaten erfassen die Fingerabdrücke möglichst vieler Iraker. Diese Daten werden dann mit amerikanischen Datenbanken abgeglichen. Dem Fingerabdruck kommt zunehmende Bedeutung zu und es entstehen globale Fingerabdruckdatenbanken.

Problematische Sammlung biometrischer Angaben

conturen: Was kommt an neuen technischen Überwachungssystemen in nächster Zeit alles auf uns zu?

Schaar: Die Zukunft hat auf diesem Gebiet schon längst begonnen. Wir haben die schon angesprochenen RFIDs, „Radio Frequency Identification“, das heißt Funkchips. Diese Funkchips werden immer billiger und können in alle möglichen Gegenstände eingebaut werden: in Kleidung, Verpackung, Gegenstände des täglichen Gebrauchs. Sie ermöglichen es, jeden Gegenstand, jedes Tier oder auch jede Person zu identifizieren. Wenn diese Technologie kombiniert wird mit anderen Techniken, zum Beispiel mit der Satellitenortung, dann geht die Entwicklung in einen für den Persönlichkeitsschutz sehr kritischen Bereich. Der Londoner „Guardian“ berichtete kürzlich, dass in Großbritannien der Verkauf von Kleidung begonnen habe, die alle zehn Sekunden den genauen Standort des Trägers übermittle. Der vermeintlich gute Zweck besteht darin, dass man beobachten kann, wo sich die halbwüchsigen Kinder gerade aufhalten, und zwar metergenau. Das Ganze kostet jetzt 15 Pfund im Monat, wird aber zweifellos noch billiger werden. Wenn solche Techniken der allgegenwärtigen Ortung auf breiter Linie Einzug halten und verbunden werden mit Risikominimierung – etwa das Fahrverhalten von Kraftfahrern überwacht wird und davon die Versicherungsprämie abhängig gemacht wird –, dann gelangen wir in den Bereich der Vollüberwachung. Diese Entwicklung scheint mir momentan die kritischste zu sein.

Funkchips ermöglichen Identifizierung von Mensch und Tier

Komplettüberwachung rund um die Uhr

Langfristig gesehen, wird es allerdings noch problematischer, weil sich dieser Trend zur Miniaturisierung fortsetzt. Das Stichwort lautet: Nanotechnologie. Nanokomponenten – und das können Batterien, Sensoren oder Sender sein – sind nur unter dem Mikroskop erkennbar. Stellen Sie sich ein totalitäres Regime vor. Während in der Hauptstadt eine Protestdemonstration stattfindet, steigen Hubschrauber auf und überschütten die Demonstranten mit Nanopartikeln. Damit sind diese unwiderruflich auf Dauer gekennzeichnet und an allen möglichen Kontrollstellen identifizierbar. Das ist natürlich eine Horrorvorstellung sondergleichen, aber eine, die durchaus einen gewissen Realitätsgehalt aufweist.

Winzige Markierungen für jedermann

Der Horror könnte Wirklichkeit werden

conturen: Die entgegengesetzte Vorstellung wäre ein totaler Zusammenbruch aller relevanten Informations- und Datensysteme. Halten Sie einen solchen totalen Blackout für denkbar?

Schaar: Das ist eine interessante Frage. Die Wahrscheinlichkeit, dass es zu einem solchen „totalen Blackout" kommt, erscheint mir heute angesichts der sehr verteilten Datenerhaltung und Datenverarbeitung geringer als zu Zeiten des Großrechnereinsatzes vor 20 Jahren. Wenn man aber darüber nachdenkt, wie sich diese autonomen Systeme entwickeln, würde ich die von Ihnen angesprochene Möglichkeit nicht völlig von der Hand weisen: Ich nenne als Stichwort nur „Computerviren". Wenn bestimmte Viren über die Netze in die Basiskomponenten eindringen und diese unbrauchbar machen, dann will ich nicht ausschließen, dass zumindest relevante Teile der Informationstechnik, von der wir immer abhängiger werden, ausfallen könnten. Übrigens gibt es solche Szenarien, die von Staaten entwickelt werden. Hier lautet das Stichwort „Cyberwar". Auf dem Kriegsschauplatz der Informationstechnik denkt man sehr genau darüber nach, wie man das System eines gegnerischen Staates völlig lahm legen könnte. Und da sich darüber nicht nur ein Staat Gedanken macht, sondern viele Staaten ähnliche Überlegungen anstellen, wäre es durchaus denkbar, dass solche Ideen in internationalen Konflikten realisiert werden.

„Cyberwar": Computerviren könnte zu einem Totalausfall aller Datensysteme führen

Mittel bei kriegerischen Auseinandersetzungen

conturen: Vor mehreren Jahrzehnten prägte Karl Popper für die demokratischen Gesellschaften des Westens den Begriff „Offene Gesellschaft" – im Unterschied zu den „Geschlossenen Gesellschaften" diktatorischer und totalitärer Regime. Heute sind die westlichen Gesellschaften „offen" in einem ganz anderen Sinne, als Popper es sich vorstellte. Führt diese neue „Offenheit", wie sie durch die modernen Technologien und Informationssysteme erzielt wird, zu einem zivilisationsgeschichtlichen Wandel?

Schaar: Diese „Offenheit" im Sinne von Entwicklungsoffenheit und Teilhabe gibt es auch heute noch. Ich glaube nicht an einen Entwicklungsdeterminismus in dem Sinne, dass die Informationstechnik quasi automatisch in einem totalitären Überwachungsstaat enden muss. Letztlich kommt es darauf an, wie die Technologie weiter entwickelt und eingesetzt wird. Informationstechniken eröffnen gerade auch vielen älteren Menschen phantastische Möglichkeiten, sich individuell wesentlich stärker in gesellschaftliche Prozesse einzubringen, als den ihnen vorangegangenen Generationen. Für die Jungen und Jüngeren ist die Form der weltweiten Vernetzung ohnehin längst zur Normalität geworden. Aber selbst jene Menschen, die aufgrund körperlicher Gebrechen ihr Haus oder ihre Wohnung nicht mehr oder nur noch selten verlassen können, bieten die neuen Technologien gleichwohl die Chance, an Diskussionen teilzunehmen und in der Welt zu sein. Auch Minderheitengruppen mit bestimmten Interessen können sich auf diesem Wege weltweit austauschen. Das ist eine neue Dimension von Offenheit, die aber – und das ist mein Thema – mit einer größeren Transparenz gegenüber Dritten verbunden ist, die einen überwachen, steuern und manipulieren können. Hier neue Wege zu finden, bleibt uns leider nicht mehr allzu viel Zeit. Entwicklungsgeschichtlich

Die guten Seiten der Informationstechnologien nicht übersehen

Neue Dimension der Offenheit

verhält es sich so, dass die Informationstechnologie ihre explosionsartige Entwicklung sozusagen in der letzten Sekunde genommen hat und der Mensch eine gewisse Zeit benötigt, um sich darauf einzustellen – sowohl in seinem Verhalten als auch in seinen Wertvorstellungen. Das ist eine unglaubliche Herausforderung für die Gesellschaft. Aber ich bin ein Optimist. Und so hoffe ich, dass die Lernfähigkeit der Menschen und der Gesellschaft dazu führt, mit dieser Herausforderung umzugehen.

Explosionsartige Entwicklung der Technik

conturen: Aber wie erklären Sie es, dass ungeachtet der von Ihnen beschriebenen Lage auf dem Gebiet des Datenschutzes das Problem in seiner politischen Brisanz von der Öffentlichkeit kaum erkannt wird? Im Grunde zeigt sich doch kein ernsthafter Widerstand.

Schaar: Dem kann ich so nicht zustimmen. Ich beobachte eher eine zunehmende Sensibilität. Erkenntnisse entstehen dadurch, dass Menschen bestimmte Erfahrungen machen. Sind diese Erfahrungen negativ besetzt, kann daraus eine Dynamik der Gegenwehr erwachsen. Diese Gegenwehr kann unter Umständen problematischen Charakter annehmen, wenn sie etwa in eine moderne Maschinenstürmerei ausartet. Von daher sind die Kräfte in unserer Gesellschaft, die Verantwortung tragen, gefordert, diese auch wirklich wahrzunehmen.

Sensibilität nimmt zu, kann aber eine problematische Dynamik der Gegenwehr bewirken

conturen: Könnte der Prozess fortschreitender Kontrolle und Ausforschung, verbunden mit einer weiteren Einschränkung von Persönlichkeitsrechten, zu einem Verlust der Demokratie führen?

Schaar: Bei der Informationstechnik haben wir ein Maß an Globalisierung erreicht, das wahrscheinlich die Globalisierung in allen anderen Bereichen – einschließlich der des Handels – weit in den Schatten stellt. Meine Befürchtung ist, dass sich die westlichen Gesellschaften mit langen demokratischen Traditionen – dazu gehören die USA und auch die meisten Länder Europas – in einer Art Konvergenzprozess befinden mit autoritären Staaten. In China beispielsweise wird die Technik immer stärker zur Überwachung von Bürgern eingesetzt, während diese Entwicklung gleichzeitig einhergeht mit einem sehr umfassenden Freihandelsansatz. Das heißt, wir haben sozusagen eine ökonomische Liberalität bei immer autoritärer werdenden staatlichen Strukturen und immer intensiverer Überwachung des alltäglichen Verhaltens. Ich hoffe, dass sich diese Entwicklung im Sinne der Stärkung von Bürger- und Menschenrechten umkehren lässt.

Wirtschaftliche Liberalität wird von autoritärer werdenden staatlichen Strukturen begleitet