Humanistische Union

Gefangen im Netz der Datenbanken

Thilo Weichert

Grundrechte-Report 1997, S. 34-40

"Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Eingriffe sind nur im überwiegenden Interesse der Allgemeinheit aufgrund eines Gesetzes zulässig." Mit dieser Formulierung des Art. 4 Abs. 2 der Verfassung für das Land Nordrhein-Westfalen wurde 1978 in Deutschland erstmals ein Grundrecht auf Datenschutz normiert. Diesem Vorbild folgten, zumeist wortreicher, mehrere Bundesländer, zum Beispiel das Saarland, Berlin, Brandenburg oder Sachsen. Bei der Überarbeitung des Grundgesetzes nach der Vereinigung der Bundesrepublik mit der DDR konnte sich der deutsche Verfassunggeber nicht dazu durchringen, ein "Grundrecht auf Datenschutz" ausdrücklich in die Verfassung hineinzuschreiben. So bleibt es bei der Rechtsprechung des Bundesverfassungsgerichts, das anläßlich der Überprüfung des Volkszählungsgesetzes 1983 feststellte:

"Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner personenbezogenen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 I i. V. m. Art. 1 I GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

Diese Rechte auf Datenschutz gelten nicht nur gegenüber dem Staat. Sie sind auch im Wirtschaftsleben von privaten Unternehmen zu beachten. Einschränkungen des Grundrechts sind nur beim Überwiegen entgegenstehender Interessen zulässig.

Das Urteil des Bundesverfassungsgerichtes hatte Vorbildcharakter für Politik und Rechtsprechung in anderen europäischen Staaten. Inzwischen hat sich über eine Datenschutzrichtlinie der Europäischen Union ein relativ hoher rechtlicher Datenschutzstandard durchgesetzt: Personenbezogene Daten dürfen prinzipiell nur für den bei der Erhebung verfolgten Zweck genutzt werden. Staatliche Eingriffe bedürfen eines hinreichend bestimmten Gesetzes. Aber auch bei privaten Datenverarbeitern ist eine rechtliche Legitimation notwendig. Dem Datenmißbrauch muß durch technische, organisatorische und verfahrensrechtliche Vorkehrungen vorgebeugt werden.

Mit dem durch die Verfassung gesicherten Recht auf Datenschutz soll eine Gesellschaft verhindert werden, wie sie von George Orwell in seinem Roman "1984" beschrieben wurde, in der der Staat die Bürgerinnen und Bürger unter dauernder Überwachung hält und damit manipuliert und einschüchtert. Eine solche Gesellschaft hatten viele Menschen vor Augen, die in den 80er Jahren gegen Volkszählung, Geheimdienstbeobachtung und zentrale Polizeidatenbanken protestierten. Trotz des Volkszählungsurteils und der zahlreichen Bürgerproteste wurden jedoch die zentralen Staatscomputer ausgebaut. Das polizeiliche INPOL-System, das NADIS-System der Geheimdienste, das Zentrale Verkehrsinformationssystem ZEVIS oder das Ausländerzentralregister AZR wurden technisch verfeinert und erhielten eine gesetzliche Grundlage. Statt die Verdatung der Menschen zurückzuschrauben, wurde das bisher Praktizierte von den Parlamenten nachträglich legitimiert und festgeschrieben. Um der technischen Entwicklung keine Hindernisse in den Weg zu legen, wurden zugleich die rechtlichen Grundlagen für noch weiter gehende Überwachungsmaßnahmen geschaffen.

Entgegen den Vorgaben des Verfassungsgerichts, die Transparenz und Berechenbarkeit fordern, wurden

staatliche Befugnisse gerade dort ausgeweitet, wo diese Prinzipien mißachtet werden: bei sogenannten Vorfeldermittlungen und verdeckten Maßnahmen. Nicht mehr eine Gefahr oder ein konkreter Verdacht ist Voraussetzung für die Erfassung von Menschen; bloße Vermutungen oder die Zugehörigkeit zu Risikogruppen genügt, um ins Visier staatlicher Fahndung zu geraten. Zum Einsatz kommen geheime Ermittlungsmethoden, von denen die Betroffenen nichts erfahren und mit denen in die intimsten Lebensbereiche eingebrochen wird. Aus allgemeinen Sicherheitsgründen findet heute schon an vielen Orten die Überwachung mit Videokameras statt, deren Bilder in großen Schaltzentren überwacht und ausgewertet werden. Um die ungerechtfertigte Inanspruchnahme staatlicher Leistungen zu verhindern, knüpft der Staat ein immer enger werdendes Netz von Kontrollen, mit dem auch der letzte Sozialhilfebetrug, die letzte Subventionserschleichung und die letzte unbegründete Beantragung politischen Asyls aufgedeckt werden soll. Die Daten des Sozialamtes werden mit den Daten der Arbeitsverwaltung oder der Kraftfahrzeugverwaltung abgeglichen. Asylsuchende müssen im automatisierten System AFIS wie Kriminelle ihre Fingerabdrücke abspeichern lassen; so sollen Anträge unter falschem Namen verhindert werden. Mit Hilfe einer Chipkarte soll ihr Aufenthaltsort jederzeit kontrolliert und jede erhaltene Leistung registriert werden. Unter dem Vorwand der Mißbrauchskontrolle und der gerechten Güterverteilung sammeln die Behörden intimste private Details und bauen computergesteuerte Ressourcenmanagement-Systeme auf. Wer sich der Kontrollogik der Bits und Bytes entziehen will, fällt entweder durch die Maschen des sozialen Netzes ins Bodenlose oder wird um so gnadenloser vom elektronischen Datennetz eingefangen. Dabei werden das verfassungsrechtliche Gebot der Zweckbindung und das der informationellen Gewaltenteilung ins Gegenteil verkehrt: Die Kooperation der Geheimdienste mit der Polizei, der Polizei mit der Ausländerverwaltung, der Ausländer- und Asylverwaltung mit den Sozialbehörden, der Sozialbehörden mit Gesundheits-, Kraftfahrzeug-, Melde- und Wohnungsbehörden sind nicht die Ausnahme, sondern die Regel.

Da Europa immer mehr zusammenwächst, beschränken sich Überwachung und Kontrolle nicht auf die nationale Ebene: Dem "Asylmißbrauch" soll mit dem europäischen AFIS unter dem Begriff "EURODAC" zu Leibe gerückt werden. Das Schengen- bzw. das Europäische Informationssystem soll die europaweite Fahndung ermöglichen. In einer europäischen Polizeibehörde EUROPOL soll grenzüberschreitend, verdeckt und verdachtsunabhängig gegen tatsächliche und vermeintliche Kriminelle ermittelt werden können, von Lissabon bis Narvik. Dabei greifen die staatlichen Verwaltungen nicht mehr nur auf große zentrale Computersysteme zurück, wie sie bis in die 80er Jahre hinein vorherrschten. Es wird eine sich revolutionär verändernde Informationstechnik genutzt, die schneller, kleiner, leistungsfähiger, vernetzter und billiger ist als das, was zu den Zeiten der Angst vor dem Großen Bruder technisch möglich war. Die Bedingungen zur Inanspruchnahme des Grundrechts auf Datenschutz werden weniger durch rechtliche oder politische Vorgaben geprägt als vom technisch Möglichen.

Die Telekommunikation in international verknüpften Netzen, insbesondere im Internet, ermöglicht einerseits eine räumlich und zeitlich nicht mehr zu fassende weltweite Kommunikation, aber auch die Kontrolle hierüber. Die Nutzung von Chipkarten im Zahlungsverkehr, im Gesundheitsbereich, bei der Mobilkommunikation oder im Verkehrswesen erlaubt die elektronische Registrierung von bisher anonymen Alltagsverrichtungen. Die Automation des gesamten Privatlebens, insbesondere der Informationsbeschaffung und der Kommunikation, aber auch von Dienstleistungen über Telebanking, Teleshopping oder Telelearning, macht bisher anonyme Teile unserer Konsum- und Massengesellschaft zu kontrollier- und manipulierbaren Größen für Staat und Wirtschaft. Die Automation des Arbeitslebens perfektioniert die Kontrolle der Beschäftigten. Hochauflösende Satellitentechnik macht die Überprüfung von Agrarsubventionen ebenso wie die Aufdeckung von Umweltverstößen oder die Regulierung von Verkehr möglich. Biometrische Angaben, vom Fingerabdruck über Gesichtskontur und Augenhintergrund bis hin zum genetischen Strichcode, sind elektronisch speicherbar und werden zur eindeutigen Identifizierung durch Arbeitgeber oder Polizei, Bankinstitut, Sozial- oder Asylverwaltung genutzt.

Ein Ende dieser Entwicklung ist nicht abzusehen. Es zeichnet sich vielmehr ab, daß immer mehr bisher getrennt angewandte Technologien zusammengeführt werden. Dies gilt nicht nur für elektronische Anwendungen, die den früheren Personalcomputer zur individuellen Informations- und

Kommunikationsstation, zum Arbeits- und Unterhaltungsgerät (TV), zum Haushaltsgerät und Lebensplaner werden lassen. Jede der täglichen Verrichtungen, die über telekommunikative Dienste gesteuert wird, ist auswertbar. In der Zusammenschau der erlangten Daten ergeben sich detaillierte Verhaltens-, Bewegungs- und Kommunikationsprofile. Die Folge ist, daß die Einzigartigkeit und Subjektivität jedes einzelnen Menschen als intelligentes und fühlendes Wesen zurückgedrängt werden zugunsten des reduzierten Bildes vom Menschen als produzierendes und konsumierendes Informationsmuster. Klassisches Exempel hierfür ist die Flüchtlingskontrolle in den Niederlanden: Asylsuchende erhalten eine Chipkarte, auf der ihre Grunddaten und ein Fingerabdruck gespeichert sind. Ohne die mit Hilfe des Fingerabdrucks im sogenannten Lifescan-Verfahren autorisierte Chipkarte erhalten die Flüchtlinge keine Sozialleistungen, keinen Eintritt in ihr Wohnheim, keine Arbeit. Durch tägliche automatisierte Meldepflichten an elektronischen Stationen werden sie in einem unsichtbaren Käfig gehalten; der Ausbruch hieraus wird mit der Illegalität bezahlt. Bei Tieren werden Microchips zur Identifizierung und Verhaltenskontrolle schon implantiert.

Man darf nicht dem Trugschluß erliegen, diese Entwicklung werde durch ein mehr oder weniger geheimes staatliches Machtzentrum eines "Big Brother" geplant. Sie ist vielmehr das zwanglose Resultat des technischen Fortschritts, der sich dezentral und weitgehend unkoordiniert entwickelt und fast "naturwüchsig" erscheint. Hauptakteur ist dabei nicht mehr der Staat. Von zentraler Bedeutung ist das Handeln der in Konkurrenz zueinander stehenden Wirtschaftsunternehmen, die in einem sehr freien Spiel strategische und taktische Allianzen eingehen: Banken, Versicherungen und sonstige Finanzdienstleister, Online-Dienste und Medienunternehmen, Adressenhändler und Auskunfteien, Versandhandelsunternehmen und private Sicherheitsfirmen, Rechenzentren und Telekommunikationsprovider und natürlich die Arbeitgeber sind die Stellen, wo sensible persönliche Daten erfaßt, gespeichert, ausgewertet und abgeglichen werden. Den privaten Datenverarbeitern geht es weniger um die Verteilung knapper Ressourcen oder um "Sicherheit" durch Überwachung, sondern um Profit. Die Gewinnerwartungen sind um so höher, je transparenter der Markt allgemein und die konkreten Geschäftspartner sind. Die Folge sind private Datenbanken mit intimsten Details über Vorlieben, Konsumverhalten, Finanzkraft und soziale Stellung. Der privaten Stellen bedienen sich auch zunehmend staatliche Instanzen. Bisher öffentlich wahrgenommene Aufgaben werden in private Hände verlagert. Nicht verzichtet wird darauf, die alten und neuen Funktionsträger miteinander informationstechnisch zu verknüpfen. Über Datenabgleiche und Rasterfahndungsmaßnahmen, aber auch schon durch direkte Abrufmöglichkeiten beschafft sich zum Beispiel die Polizei das für ihre präaktiven und repressiven Aufgaben nötige Hintergrundwissen vom Kfz-Produzenten bis zur Handelsauskunftei.

Verblüffend ist bei dieser Entwicklung, daß der Apparat, nicht die Politik, die Richtung vorgibt. Die politische Führung in den Parlamenten und Ministerien reagiert auf diese Entwicklung eher, als daß sie sie lenkt. Fehlende technische Kompetenz verurteilt die demokratisch legitimierten Entscheidungsträger zum Nachvollzug und Absegnen der Faktizität der Technik. Diese gestalten nicht mehr, sondern werden zur Legitimationsinstanz degradiert. Mangels technischer Kompetenz scheinen die Parlamente völlig überfordert, die sozialen, demokratischen und bürgerrechtlichen Implikationen der modernen Informationstechnik zu erfassen, geschweige denn politisch zu gestalten und rechtlich einzugrenzen.

Wenig schmeichelhaft ist die Rolle, die die Betroffenen in dieser grundrechtszerstörenden Entwicklung spielen. Diese sind nicht mehr reine Verdatungsobjekte, die sie in den 80er Jahren waren, sondern oft aktive Teilnehmer im telekommunikativen Prozeß. Durch ihre scheinbar völlig freiwillige Beteiligung, die ihnen den Eindruck der Selbstbestimmung vermittelt, ja die Illusion, die treibende Kraft zu sein, wird in vielen Bereichen erst die Fremdbestimmung durch Staat und Wirtschaft ermöglicht. Das Einklinken in Online-Dienste und Internet, das Nutzen von elektronischen Zahlungskarten und von Telediensten, von digitalem Fernsehen und Gesundheitschipkarten - all dies läßt erst die Datenspuren entstehen, die zu Zeiten des anonymen Massenkonsums nicht vorstellbar waren und die zu umfassenden Persönlichkeitsprofilen zusammengestellt werden können.

Was bedeutet dies nun hinsichtlich des Schutzes unserer Freiheitsrechte und unserer Privatsphäre? Völlig unsinnig wäre es, Maschinenstürmern gleich den Rückmarsch in die vorelektronische Zeit zu propagieren.

Das technische Know-how ist ein Fluch, aber auch eine Chance, mit der zu leben wir lernen müssen. Die freiheitsbedrohende Informationstechnik enthält auch ein gewaltiges positives Potential: Mühselige Verrichtungen werden zum Kinderspiel, Zeit und Energie für kreatives Schaffen werden freigesetzt, Informationsmöglichkeiten werden exorbitant ausgeweitet. Fatal wäre es jedoch, der technischen Entwicklung freien Lauf zu lassen und auf die technische Lösung der entstehenden sozialen Probleme zu vertrauen.

Die Verfassung und bisherige Diskussion geben auf die Herausforderungen nur ungenügende Antworten. Nicht nur die Technik, auch das Recht muß weiterentwickelt werden. Das Brief- und Postgeheimnis muß zu einem Grundrecht auf unbeobachtete Kommunikation ausgebaut werden. Das allgemeine Persönlichkeitsrecht darf nicht bei einem formalisierten Recht auf informationelle Selbstbestimmung stehenbleiben. Die Informations-, Meinungs- und Pressefreiheit muß zu einer garantierten Grundversorgung für Informationsbeschaffung und Kommunikation führen. Das Recht und die Politik müssen Antworten auf die Entwicklung der Technik finden.
