Zeitschrift für
Praxis und Wissenschaft
Schriftleitung:
Dr. Georg Wronka, Bonn
Dr. Rudolf Schomerus, Bonn
Prof. Peter Gola, Bonn
Irene Wind, Bonn
5. Jahrgang 1989 Heft 4
Seiten 153–200

Recht der Datenverarbeitung
RDV

Aufsätze

Prof. Paul Schwartz, University of Arkansas, Fayetteville, USA*

Die neuesten Entwicklungen im amerikanischen Datenschutzrecht

1. Als 1974 der Privacy Act, das amerikanische Bundesdatenschutzgesetz für die Datenverarbeitung der bundesstaatlichen Verwaltung, verabschiedet wurde, übernahm der amerikanische Gesetzgeber mit die Initiative für die Entwicklung des Datenschutzrechts[1]). Vier Jahre nach dem hessischen Datenschutzgesetz, drei vor dem Bundesdatenschutzgesetz und vier vor der französischen „loi relative à l'informatique" setzte er mit dem Privacy Act Maßstäbe für die Verarbeitung personenbezogener Daten. Das Gesetz räumt dem Bürger gegenüber den Bundesbehörden sowohl Benachrichtigungs- und Berichtigungsansprüche als auch ein Schadensersatzrecht bei unzulässiger Datenverarbeitung ein. Der Privacy Act, ein zu seiner Zeit fortschrittliches Gesetz, erscheint uns heute eher als schönes, verfallendes Monument denn als Anstoß zu einem aktuellen und alltagsprägenden Datenschutzrecht[2]). Es ist keine Übertreibung, vom Verfall des amerikanischen Datenschutzrechtes zu reden, ein Verfall, ermöglicht und begleitet durch den Mangel an öffentlicher Aufmerksamkeit. Das Interesse am Datenschutz hat so nachgelassen, daß jeder Hinweis darauf zumeist nur als Erinnerung an die jeweils notwendigen Sicherheitsvorkehrungen oder an die urheberrechtlichen Probleme einer automatischen Datenverarbeitung verstanden wird.
Auf die Frage, warum die Amerikaner sich zur Zeit so wenig für den Datenschutz interessieren, kann hier nicht eingegangen werden. Die nachfolgenden Bemerkungen sollen vielmehr die aktuellen Datenschutzvorschriften und ihre Entwicklung erläutern. Obwohl es zur Zeit, was den Datenschutz betrifft, nicht gut aussieht in dem Land, das der Welt „das Recht auf Privatheit" gegeben hat, sollte man nicht verzagen: Recht entwickelt sich zumeist nicht geradlinig.
2. In der Bundesrepublik ist man sich durchaus der Tatsche bewußt, daß die Verarbeitung personenbezogener Daten die Grundlagen einer demokratischen Ordnung gefährden kann. Demokratie hängt mit der Entscheidungsfähigkeit des Bürgers zusammen: der demokratische Staat entsteht durch die Beteiligung des Bürgers und lebt von seiner Teilnahme am gemeinsamen Willensbildungsprozeß[3]). Die Gefahr unkontrollierter Datenverarbeitung liegt darin, daß die freie Entfaltungsmöglichkeit und Entscheidungsfindung des einzelnen eingeschränkt wird, wenn für ihn nicht mehr überschaubar ist, „welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind"[4]). Die fortwährende Entwicklung der Informationstechnologie verstärkt diese Ungewißheit, indem sie die Möglichkeiten ausbaut, immer mehr personenbezogene Daten immer besser zu verarbeiten. Deshalb gehört es zu den wichtigsten Aufgaben der Rechtsordnung, den Datenströmen Grenzen zu setzen. Darauf hat das Bundesverfassungsgericht deutlich hingewiesen[5]).

Das Zusammenspiel allgemeiner und bereichsspezifischer Datenschutzgesetze sowie der Kontrolltätigkeit der Datenschutzinstanzen schafft ein, wenn nicht lückenloses, so doch immer dichteres Schutzsystem[6]). Auch die Gerichte übernehmen dabei eine wichtige Rolle: Arbeits-, Verwaltungs-, und Verfassungsgerichte haben inzwischen eine besondere Rechtsprechung zum Datenschutz entwickelt[7]). Kurzum, die Bundesrepublik versucht, ein ohnehin auf Vollständigkeit ausgerichtetes Datenschutzsystem ständig zu verbessern. Durch die Aufmerksamkeit und rechtzeitige Intervention der Datenschutzbeauftragten sind Reaktionen auf die technologischen und gesellschaftlichen Folgen der Datenverarbeitung praktisch vorprogrammiert.

Das amerikanische Datenschutzsystem wirkt demgegenüber wie eine beliebige Sammlung von Gesetzen, die weder einer Prüfung durch Datenschutzbeauftragte noch einer zureichenden Kontrolle durch Gerichte ausgesetzt sind. Der Bürger wird in Ungewißheit und Verwirrung darüber gelassen, wer seine personenbezogenen Daten

* Für ihre großzügige Unterstützung danke ich der Alexander von Humboldt-Stiftung.

1) Siehe C. Sasse, Sinn und Unsinn des Datenschutzes, 1976, S. 16ff.
2) Heftige Kritik am Privacy Act übt der Report of the Privacy Protection Commission: The Privacy Act of 1974, 1977, S. 30.
3) Simitis, Selbstbestimmung: Illusorisches Projekt oder reale Chance?, in: Die Zukunft der Aufklärung (1988) 165ff.
4) BVerfGE 65, S. 1 (43).
5) BVerfGE 65, S. 1 (41–44).
6) Darauf hat Riegel, Kontrolle und Transparenz der Datenverarbeitung, DuD 1988, S. 277 hingewiesen.
7) Siehe Gola, Das Recht auf informationelle Selbstbestimmung in der aktuellen Rechtsprechung, RDV 1983, S. 109.

wozu benutzt. Auf den Punkt gebracht: Es fehlen die Rechtsnormen, die Institutionen und die rechtlich gesicherten Kontrollinstanzen, die es erlauben, die amerikanischen Vorschriften als ein halbwegs geschlossenes Regelungssystem zu bezeichnen. Der Akzent liegt durchweg auf weitgehend ohne Rücksicht aufeinander entstehenden bereichsspezifischen Gesetzen[8]). Jede dieser Regelungen, ob Fair Credit Act, Privacy Act oder Family Education Rights and Privacy Act, stellt daher eine isolierte Antwort auf ein begrenztes Problem dar.

Zudem: Alle Datenschutzregelungen sind zwangsläufig zeitlich begrenzt. Die Vorläufigkeit solcher Maßnahmen ist im Hinblick auf die technische Entwicklung nicht die Ausnahme, sondern die Regel. Jedoch fordert gerade der amerikanische Weg, nur bereichsspezifische Vorschriften zu verabschieden, eine besonders intensive gesetzgeberische Tätigkeit und eine kontinuierliche juristische Beobachtung. Sollten diese Voraussetzungen nicht gegeben sein, wird die technologische Entwicklung dem Datenschutz nicht nur immer einen Schritt voraus sein, sondern auch das Zusammenwirken der verschiedenen Gesetze dem Zufall überlassen bleiben.

Es hat sich aber erwiesen, daß die amerikanischen Gesetze nicht als Anfang, sondern als vorzeitiger Schlußstrich unter die jeweils notwendige Regelung des einzelnen Bereiches zu verstehen sind. Seit einiger Zeit zeigen sich bereits die Schwachstellen der Gesetzgebung: So hat z. B. der Privacy Act durch eine großzügige Auslegung der Freigabe von Daten bei einer „routinemäßigen Benutzung" und durch die Nachlässigkeit der Überwachung erheblich an Wirkung verloren[9]). Diese Schwächen sind um so bedeutsamer als auf Landesebene nahezu keinerlei Datenschutzgesetze existieren.

Noch einmal zur Erinnerung: Im Gegensatz zur amerikanischen Praxis hat der deutsche Gesetzgeber zuerst „allgemeine" Datenschutzregelungen verabschiedet und dann seine Aufmerksamkeit konkreten Verarbeitungszusammenhängen gewidmet. Obwohl Generalklauseln zwangsläufig unpräzise sind, bilden solche globalen Regelungen die Rahmenbedingungen für weiterführende Entwicklungen. Man kann also sagen: deutscher Datenschutz fängt mit Generalklauseln an, amerikanischer Datenschutz hört mit (jedem) bereichsspezifischen Gesetz auf.

Das amerikanische Datenschutzsystem ist allerdings nicht nur wegen der lückenhaften Gesetzgebung zu bemängeln; im Gegensatz zur Bundesrepublik sind die Kontrollinstanzen in den Vereinigten Staaten nahezu inexistent. Als Beispiel mag hier nur die Tatsache dienen, daß es einen Datenschutzbeauftragten in den Vereinigten Staaten weder im öffentlichen noch im nicht-öffentlichen Bereich gibt. Nicht einmal die im Entwurf des Privacy Act vorgesehene Bundesdatenschutzkommission wurde eingerichtet. Die Ford-Regierung hat mit Erfolg dagegen gekämpft und die geplante Kommission durch das „Office of Management and Budget", einer Zentralbehörde unter der Aufsicht des Präsidenten, ersetzt[10]), die ihre Kontrollaufgaben nur höchst unzureichend erfüllt. Die Erfahrung zeigt nur zu gut, daß es diese Behörde im Normalfall vorzieht, der Bundesverwaltung einen möglichst breiten Spielraum zu überlassen, und es nachgerade vermeidet, deren Aktivitäten einer Prüfung zu unterziehen. Obwohl wichtige Studien von verschiedenen Bundesbehörden veröffentlicht wurden und Anhörungen zu besonders dringenden Problemen vor verschiedenen Ausschüssen des Kongresses stattfanden, besteht also nach wie vor keine Institution, die sich intensiv mit der Beobachtung der Datenverarbeitung und ihrer Auswirkungen befaßt.

Noch deutlicher ist der Gegensatz, sobald man den Datenschutz unter verfassungsrechtlichen Gesichtspunkten betrachtet. In der Bundesrepublik hat Datenschutz Verfassungsrang. Demgegenüber gibt es in den Vereinigten Staaten kein „Recht auf informationelle Selbstbestimmung". Das auf der Rechtsprechung beruhende „Recht auf Privatheit" („right of privacy") ist überaus ambivalent. So führt etwa die weite Auslegung des Anspruchs auf Schutz der „sexuellen Intimität" dazu, das Recht auf Abtreibung, auf Verhütungsmittel, und auf den Besitz, wenn auch nur zu Hause (!), von pornographischen Schriften[11]) zu schützen. Im Vergleich dazu hat das „Recht auf Privatheit" eine erstaunlich geringe Wirkung, wenn es mit der „Pressefreiheit" in Konflikt gerät. Dies ist um so verwunderlicher, als es die Medienentwicklung und die Veröffentlichungspolitik der Boulevardblätter waren, die 1898 Warren und Brandeis dazu anregten, ein „Recht auf Privatheit" zu formulieren, also „ein Recht, allein gelassen zu werden", das sich jedoch gegen die großzügig gestaltete amerikanische Verfassungstradition der „Pressefreiheit" nicht durchsetzen konnte[12]).

Aber auch sonst liegen die Defizite auf der Hand. Der Supreme Court hat sich erstmals 1977 zum Datenschutz geäußert. Anlaß der Entscheidung Whalen v. Roe[13]) war die im Bundesstaat New York vorgenommene Erhebung und Speicherung personenbezogener Daten von Patienten, die bestimmte ärztlich vorgeschriebene Medikamente einnahmen. Zweck dieser Maßnahme war es, die Verwendung einzelner rezeptpflichtiger Medikamente als Rauschgift zu bekämpfen. Der Supreme Court hat klargestellt, daß die Verarbeitung und Speicherung der Daten unter zwei verfassungsrechtlich relevanten Aspekten geprüft werden muß: dem individuellen Interesse, die Enthüllung persönlicher Angelegenheiten zu vermeiden, sowie dem Interesse, „bestimmte wichtige Entscheidungen völlig unabhängig zu treffen"[14]).

Keiner dieser beiden Ansatzpunkte wird vom Supreme Court unter Berücksichtigung der besonderen Situation des einzelnen im Zeitalter des Computers ausgelegt. Nach Meinung des Gerichtes wird ein persönlicher, vom Staat beobachteter und registrierter Vorgang erst dann verfassungsrechtlich relevant, wenn die Öffentlichkeit davon erfährt[15]). Dieses einseitige Verständnis führt dazu, daß es auf die Speicherung gar nicht mehr ankommt. Folglich hält es das Gericht bereits für ausreichend, die jeweiligen Datensicherheitsvorkehrungen zu prüfen. Weder die Gefahr einer möglichen Zweckentfremdung der Daten noch die Frage einer Verhältnismäßigkeit der Verarbeitung wurden vom Gericht

8) Simitis in: Simitis/Dammann/Mallmann/Reh, Kommentar zum BDSG, 3. Auflage 1981, Einleitung, Rdn. 70.
9) Vgl. oben Anm. 2, S. 91 ff.
10) K. Laudon, Dossier Society, 1986, S. 5–6.
11) So z. B. Roe v. Wade, 410 U.S. 113, 153 (1973). Siehe Ely, The Wages of Crying Wolf, 82 Yale L. J. 1973, S. 920 ff.
12) Warren & Brandeis, The Right of Privacy, 4 Harv. L. Rev. 1898, S. 193.
13) 429 U. S. 589 (1977).
14) 429 U. S. 589, 598–600 (1977).
15) 429 U. S. 589, 600–602 (1977).

bedacht. Der Supreme Court unterscheidet zudem zwischen verfassungsrechtlich relevanten persönlichen Daten und belanglosen, verfassungsrechtlich irrelevanten[16]). Im Gegensatz dazu weist das Bundesverfassungsgericht eine derartige Unterscheidung prinzipiell zurück: „... unter den Bedingungen der automatischen Datenverarbeitung gibt es kein ‚belangloses' Datum mehr. Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen".[17]) Ebenso oberflächlich ist die Freiheit, „bestimmte wichtige Entscheidungen völlig unabhängig zu treffen", behandelt worden. Nach Meinung des Gerichts ist die freie Entscheidung, die verordneten Medikamente einzunehmen, trotz Computerüberwachung nicht eingeschränkt, da Ärzte und Patienten ihre Wahl nach wie vor frei und allein treffen können[18]). Auf die Frage, ob das Verhalten der Beteiligten durch die den Betroffenen bekannte Tatsache der Speicherung ihrer Namen beeinflußt sein könnte, geht das Gericht letztlich nicht ein. Damit hat es der Supreme Court, im Unterschied zum Bundesverfassungsgericht, versäumt, ein Recht auf informationelle Selbstbestimmung anzuerkennen.

Seit der Entscheidung Whalen v. Roe hat sich letztlich kaum etwas geändert. Nach wie vor setzt die Lehre „Privatheit" mit „Privatsphäre" gleich[19]). „Privatheit" wird also nicht als unverzichtbare Voraussetzung der Kommunikationsfähigkeit und der Entfaltungschancen des einzelnen verstanden. Rechtsprechung und Lehre orientieren sich am Modell eines isolierten Menschen, genauer, jenes einsamen Cowboys, der zurückgezogen in seiner Wohnung lebt, während seine Daten in einer von ihm nicht überschaubaren Welt verarbeitet werden.

3. Dieses höchst unzureichende Regelungssystem hat der Reagan-Administration einen großen Spielraum für die Verwirklichung ihrer Pläne gewährt. Dazu zählte es auch, den Staat wie ein Unternehmen zu verwalten. Die Regierung war deshalb besonders darauf bedacht, Effizienz und Sparsamkeit der öffentlichen Verwaltung zu erhöhen, nicht zuletzt mit Hilfe des Einsatzes von Computern[20]). Die amerikanische Bundesverwaltung, schon jetzt der Welt größter Benutzer von Universalrechnern und Mikrocomputern, dürfte diesen Rang auch in absehbarer Zeit nicht verlieren. 1988 allein hat der Staat 17 Milliarden Dollar für Computer sowie die damit verbundenen Dienstleistungen ausgegeben[21]). Dieser Betrag entspricht 1,6 Prozent des gesamten Staatshaushaltes. Konsequenterweise ist die Verwaltung bemüht, alle Vorteile einer Automatisierung zu nutzen. So zahlt z. B. die Bundesverwaltung kleine Beträge zunehmend mit Kreditkarten[22]). Als Folge davon werden auch die Bürger ermutigt, ihre Verbindlichkeiten gegenüber den Behörden mit Kreditkarten zu begleichen. Mittlerweile bemüht sich die Finanzverwaltung um Einkommensteuererklärungen, die als Disketten eingereicht werden. Solche Maßnahmen vergrößern zwangsläufig die Menge der Daten, die sofort elektronisch abrufbar sind und darüberhinaus miteinander vernetzt werden können.

Die von den verschiedenen Behörden gespeicherten und verarbeiteten personenbezogenen Daten werden mehr und mehr miteinander abgeglichen, wiederum mit dem Zweck, die Leistungsfähigkeit der Verwaltung zu steigern. Obwohl es keine genauen Angaben über die Häufigkeit gibt, schätzt man, daß die Anzahl der Abgleiche während der ersten vier Jahre der Reagan-Regierung dreimal höher war als unter Präsident Carter[23]). Die Daten, die miteinander verglichen werden, stammen sowohl aus der öffentlichen Verwaltung als auch aus privaten Quellen. So wird eine Liste derjenigen Personen, die ihre staatlichen Ausbildungsdarlehen nicht zurückgezahlt haben, mit einer Aufstellung aller öffentlichen Bediensteten abgeglichen. Wer dabei als Schuldner ertappt wird, muß mit einer Teilpfändung seines Gehaltes[24]) rechnen. Der Ankauf von privaten Datensammlungen durch die Bundesverwaltung hebt zudem den Unterschied zwischen privatem und öffentlichem Wissen über den Bürger auf. Die Suche nach interessanten, d. h. auswertbaren, Dateien kann dabei weite Kreise ziehen und sich selbst auf die von einer Firmenkette für „Speiseeis" gespeicherten Angaben erstrecken[25]). So verspricht ein bekannter Konzern Kindern und Jugendlichen ein kostenloses Eis zum Geburtstag, allerdings unter der Voraussetzung, daß sie einen „Antrag" mit Angabe ihrer vollständigen Anschrift und ihres Geburtsdatums stellen. Der Konzern will dadurch seinen Absatz erweitern. Selbstverständlich werden die Informationen automatisch gespeichert. Davon profitiert auch die Bundesverwaltung, um die Personen zu erfassen, die ihrer Meldepflicht im Rahmen des Militärdienstes nicht nachgekommen sind.

4. Noch einige kurze Bemerkungen zu den wichtigsten neuen Gesetzen, dem „Computer Matching Act" von 1988, dem „Computer Security Act" von 1987, dem „Family Support Act" von 1988 und dem „Medicare Catastrophic Protection Act" von 1988.

Der Computer Matching Act[26]) ist ein Versuch, ein wenig Ordnung in den Datenabgleich zu bringen. Das Gesetz verbietet einen Abgleich personenbezogener Daten, die von Bundesbehörden gespeichert werden, wenn nicht ein schriftliches Abkommen zwischen den jeweils interessierten Behörden vorliegt. Der Abgleich muß im Federal Register, dem amerikanischen Bundesanzeiger, veröffentlicht werden. Soweit eine Aufnahme personenbezogener Daten durch einzelne Behörden erfolgt, verlangt das Gesetz, daß der Betroffene von der entsprechenden Stelle auf die Möglichkeit einer Prüfung seiner Daten aufmerksam gemacht werden muß. Dem Betroffenen darf solange kein Nachteil entstehen, bis er die Chance gehabt hat, Stellung zu nehmen. Das Gesetz sieht schließlich „Data Integrity Boards" vor, deren Aufgabe es ist, die Exaktheit der Daten zu kontrollieren und dadurch den Wert eines Abgleichs zu erhöhen.

Freilich: die Veröffentlichung im Bundesanzeiger, die Gewährleistung einer Stellungnahme des Bürgers sowie

16) 429 U. S. 589, 601–603 (1977).
17) BVerfGE 65, S. 1 (45).
18) 429 U. S. 589, 603 (1977).
19) Posner, The Right of Privacy, 12 Ga. L. Rev 1978, S. 393ff.; Posner, Uncertain Protection of Privacy by the Supreme Court, Ct. Rev. 1979, S. 173ff.
20) Executive Office of the President, Office of Management and Budget, Management of the United States Government, Fiscal Year 1989, S. 11ff.
21) aaO. (Anm. 21).
22) aaO. (Anm. 21), S. 6, 143ff.
23) Report of The Committe on Government Affairs, United States Senate, 1988, Report 100–516, S. 4.
24) aaO. (Anm. 21), S. 29ff.
25) Davis, Abusive Computers, Wall Street Journal, 20. August 1987, S. 1.
26) Public Law 100–503.

die Kontrolle der Angaben sind letztlich nicht mehr als Warnzeichen, garantieren also bestenfalls die Transparenz der Datenverarbeitung. Im Gegensatz zum Computer Matching Act fordert das Bundesverfassungsgericht ein „Gesetz oder eine andere Rechtsvorschrift" als Legitimationsgrundlage[27]). Ein „schriftliches Abkommen", mithin ein rein interner Verwaltungsvorgang, würde dieses Gebot nicht erfüllen[28]). Das Hessische Datenschutzgesetz geht noch weiter: „Personenbezogene Daten dürfen grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind".[29])

Obwohl im Privacy Act die Zweckentfremdung der Daten ausdrücklich untersagt ist, nimmt der „Computer Matching Act" keine Notiz davon. Als dürftiger Ersatz ist die Veröffentlichung im Federal Register vorgesehen, die nahezu niemanden über die beabsichtigte Weiterverarbeitung in Kenntnis setzt.

Der „Computer Security Act"[30]) überträgt dem National Bureau of Standards, einer Abteilung des Handelsministeriums („Commerce Department"), die Verantwortung, Richtlinien für die Bundesdateien zu erlassen. Diese Vorschriften sollen die „Sicherheit und Privatheit von sensiblen Daten" vergrößern. Der neue Fachausdruck, „sensible Daten", bezeichnet Informationen, die noch nicht als „geheim" eingestuft sind, deren Verlust oder Mißbrauch jedoch „dem Staatsinteresse" schaden könnte[31]). Die jeweils vorgesehenen Maßnahmen können vom Präsidenten der Vereinigten Staaten abgelehnt oder modifiziert werden. Kurzum, „Datensicherheit" ist ausschließlich Sache der Exekutive.

Ohne eine Blick auf seinen Hintergrund ist das Gesetz kaum verständlich. Die National Security Agency, eine Dachorganisation der Abwehreinheiten, hatte 1986 eine Anordnung vorgeschlagen, die dem Nationalen Sicherheitsberater das Recht einräumen sollte, neue Richtlinien für „sensible" Daten zu verabschieden[32]). Eine solche Befugnis, die Militär- und Sicherheitsdiensten einen großen Handlungsspielraum im Bereich der Datennutzung bieten würde, ging dem Kongreß zu weit. Nach Meinung der Abgeordneten sollte die Entscheidung nicht in den Händen des Militärs liegen. 1987 wurde dann der Computer Security Act beschlossen[33]).

Die Schwäche des Gesetzes liegt in der Vorstellung, die „Datensicherheit" könne geregelt werden, ohne auf das „Recht des einzelnen", die Verwendung seiner Daten zu bestimmen, Einfluß zu nehmen. Der Kongreß hat zudem die eigenen Kompetenzen beschränkt, indem er der Exekutive umfassende Entscheidungs- und Kontrollmöglichkeiten im Bereich der Datensicherheit zugestanden hat. In der Bundesrepublik ist man sich demgegenüber bewußt, wie sich etwa am Hessischen Datenschutzgesetz zeigt, daß man bei aller Verarbeitungsregelung auch das Informationsgleichgewicht zwischen Legislative und Exekutive bedenken muß: Wer Wissen besitzt, kann sich bald Macht aneignen. Solange die Exekutive die Fäden zur Konzentration und Steuerung der Informationsverarbeitung in der Hand hält, ist die Funktionsfähigkeit des Parlaments eingeschränkt.

Der Family Support Act[34]), ein Gesetz, welches das amerikanische Sozialhilfesystem grundlegend ändert, illustriert, wie stark der administrative Zwang ist, neue Daten zu erheben und abzugleichen. Ziel des Gesetzes ist es, Sozialhilfe unter der Voraussetzung zu ermöglichen, daß dieser Unterstützung eine Arbeitsleistung von Seiten des Empfängers gegenübersteht. Der „Kultur der Armut" („Culture of poverty") soll dadurch ein Ende bereitet werden[35]). Selbst Mütter mit kleinen Kindern kommen deshalb nur dann in den Genuß der Sozialhilfe, wenn sie entweder berufstätig sind oder an einem staatlich geförderten Ausbildungsprogramm teilnehmen. Konsequenterweise verlangt das Gesetz, daß immer mehr Väter, die ihren finanziellen Verpflichtungen nicht nachkommen, ausfindig gemacht und so zur Unterstützung ihrer Kinder herangezogen werden. Unter diesen Umständen ist der Gedanke naheliegend, Computer dafür einzusetzen. Der Family Support Act erlaubt daher nicht nur den Abgleich zwischen den umfangreichen Dateien des Arbeitsministeriums sowie den entsprechenden Dateien der Bundesstaaten, sondern sichert den einzelnen Behörden darüber hinaus großzügige Geldbeträge zum Aufbau neuer Informationssysteme zu[36]). Nach jeder Geburt wird zudem die Sozialversicherungsnummer der Eltern zusammen mit dem Namen des Kindes gespeichert[37]). Sollten die Eltern nicht mehr auffindbar sein oder sich weigern, das Kind zu unterstützen, dienen diese Daten dazu, das Gehalt der Eltern zu pfänden.

Der Family Support Act wurde von der überwiegenden Mehrheit des Kongresses verabschiedet und in der Presse positiv begrüßt[38]). Weder der Datenabgleich noch die Entstehung neuer Dateien wurden kritisiert. Eine nüchterne Betrachtung des Sozialhilfesystems der Vereinigten Staaten zeigt, daß diese Maßnahmen kaum als verhältnismäßig einzustufen sind. Viele Väter zahlen nicht, weil sie zu arm sind, um überhaupt einen nennenswerten Beitrag zur finanziellen Unterstützung zu leisten. Da sich der Family Support Act die Kostendämpfung als Ziel gesetzt hat, läßt er zudem grundlegende Probleme, die neue Kosten verursachen, unberücksichtigt. So zeigt z. B. eine aktuelle Untersuchung, daß die meisten Anträge auf Sozialhilfe abgelehnt werden, nicht etwa, weil den Antragstellern eine Unterstützung nicht zusteht, sondern weil sie die Formulare nicht richtig ausgefüllt haben[39]).

Schließlich ist in diesem Zusammenhang der Medicare Catastrophic Protection Act[40]) zu nennen. Durch dieses

27) BDSG vom 27. Januar 1977, § 3.
28) Simitis (Anm. 10) § 3, Rdn. 5, 6.
29) HDSG, § 13.
30) Public Law 100–235.
31) Public Law 100–235, Section 3(d) (4).
32) Der Vorschlag ist in dem unten, Anm. 33, angegebenen Anhörungsprotokoll, S. 37ff., abgedruckt.
33) Hearing Before the Subcommittee on Science, Research and Technology and the Subcommittee on Transportation, Aviation and Materials of the Committee on Science, Space and Technology, House of Representatives, One Hundredth Congress, 26. Februar 1987, No. 8, S. 5ff.
34) Public Law 100–1720.
35) a. M. Hacker, Getting Rough on the Poor, The New York Review of Books, S. 12ff., 13. Oktober 1988.
36) Public Law 100–1720, Sections 123–126.
37) Section 125.
38) Im Senat wurde das Gesetz mit 93 zu 3 Stimmen verabschiedet. Vgl. First, Think of Single Mothers, New York Times, September 20, 1988, A28.
39) Southern Governors' Association, Study of the AFDC/Medicaid Eligibility Process in the Southern States, 1988. Vgl. Tolchin, Many Rejected for Welfare Aid Over Paperwork, New York Times, 29. Oktober 1988, S. A1.
40) Public Law 100–436.

Gesetz wurde der Gesundheitsdienst für Rentner insofern verbessert, als die finanziellen Leistungen von seiten des Staates wesentlich erweitert wurden. Die damit zusammenhängenden Kosten werden innerhalb der nächsten fünf Jahre ca. 30 Milliarden Dollar betragen. Über die praktische Umsetzung dieses Programmes schweigt sich der Gesetzgeber jedoch aus. Für das Bundesministerium für Gesundheit („Department of Health and Human Services") liegt der Schwerpunkt des Medicare Catastrophic Protection Act bis jetzt in der Überwachung der medizinischen Dienstleistungen, die für den einzelnen erbracht werden. Um eine solche Kontrolle zu gewährleisten und zugleich sicherzustellen, daß die vorgeschriebenen Pflichtbeiträge des Betroffenen bezahlt worden sind, bevor der Staat zur Kasse gebeten wird, sollen 52000 Apotheken mit Computern ausgerüstet werden[41]). Zweck dieser Maßnahme ist es, der Verwaltung ein vollständiges Bild über bisher erbrachte Leistungen, einschließlich der jeweils verordneten Medikamente zusammen mit Angaben über Leistungsträger zu vermitteln.

In Zukunft wird es keine Rolle mehr spielen, wo sich der „Medicare" Patient aufhält. Informationen über ihn werden in allen Apotheken abrufbar sein. Die Entscheidung, diese Maßnahmen einzuführen, von denen 32 Millionen „Medicare" Empfänger betroffen sind, wurde ohne öffentliche Debatte und ohne eine Anhörung durch den Kongreß getroffen. Das Bundesministerium für Gesundheit geht davon aus, daß das Medicare-Computer-Projekt vom 1. Januar 1990 an operabel sein wird.

5. Das Regelungssystem in den Vereinigten Staaten verbessert zwar die Datensicherheit und erhöht die Leistungsfähigkeit der Verwaltung, unterläuft jedoch die Selbstbestimmung des einzelnen. Personenbezogene Daten werden mehr und mehr auf Vorrat gespeichert. Der Bürger, der Anspruch auf eine Sozialleistung hat, wird zum „verdächtigen" Sozialempfänger und muß in Kauf nehmen, daß seine Daten und Angaben gespeichert und für eine Vielzahl von Zwecken verarbeitet werden. Alles in allem: den Gefahren der automatischen Datenverarbeitung wurde in den Vereinigten Staaten viel zu wenig Aufmerksamkeit geschenkt. Bereits der Grundstein des Datenschutzrechtes, die Verarbeitungsmöglichkeiten offenzulegen und strikt zu begrenzen.

---

41) Vgl. Tolchin, System to Track Medicare Drugs, New York Times, July 13, 1988, S. A1.