Bärbel Ziegler-Jung

Datenschutzrecht in den Niederlanden
Aktuelle Entwicklungen im internationalen Vergleich*

Im Mittelpunkt der nachfolgenden Ausführungen zum Datenschutz in den Niederlanden stehen folgende Aspekte:

- die Entstehungsgeschichte des niederländischen Datenschutzrechts
- Grundzüge des Personenregistergesetzes
- bereichspezifische Regelungen
- das niederländische Datenschutzrecht im internationalen Vergleich.

Die Entstehungsgeschichte

Die Entstehungsgeschichte des niederländischen Datenschutzrechts kann in folgende drei Phasen untergliedert werden:

- Entwicklung von Problembewußtsein (1965-1971)
- Vorbereitung gesetzlicher Maßnahmen (1972-1980)
- Abschluß des Gesetzgebungsverfahrens (1981-1988).

Zu Beginn der ersten Phase steht die Diskussion der niederländischen Juristenvereinigung, die 1965 bei ihrem Jahrestreffen die Frage behandelte, ob der Gesetzgeber Maßnahmen zum Schutz der persönlichen Lebenssphäre des Individuums zu treffen hat. Im weiteren hatte ab 1968 die Diskussion über die Automation des Einwohnermeldewesens große Bedeutung, denn diese richtete sich auch auf die Einführung eines zentralen Personenkennzeichens. 1971 wurde ein Abhörverbot von Gesprächen in das Strafgesetzbuch aufgenommen. Ein Markstein bei der Entwicklung von Problembewußtsein war die 1971er Volkszählung, bei der ein nicht unerheblicher Teil der niederländischen Bevölkerung auch aus Datenschutzgründen eine Auskunftserteilung verweigerte. Datenschutzprobleme, die bislang nur in Juristenkreisen erörtert wurden, erreichten das Parlament und breitere Bevölkerungsschichten.

Ein Ergebnis der aufkommenden Datenschutzdiskussion war, daß die Regierung 1972 die Staatskommission 'Koopmans' einsetzte, die den Auftrag erhielt, notwendige gesetzgeberische Maßnahmen vorzubereiten. Aufgrund des Zwischenberichts der Kommission 'Koopmans', die den speichernden Stellen empfahl, nicht auf den Erlaß eines Datenschutzgesetzes zu warten, sondern selbst Datenschutzvor-

---

* Frau Dr. Bärbel Ziegler-Jung ist Dozentin an der Faculteit der Bestuurskunde der Universiteit Twente und hielt am 26. Januar 1990 einen Vortrag auf Einladung des Zentrums und des Instituts für Kirchenrecht der Westfälischen Wilhelms-Universität Münster.

schriften zu erstellen, fingen einige Stellen an, Datenschutzreglemente zu erarbeiten. Der Ministerpräsident erließ 1975 Richtlinien für die Reichsverwaltung, die Minimalforderungen für derartige Reglemente enthalten. Die ministeriellen Richtlinien stimulierten die Selbstregulierung im gesamten öffentlichen und auch im privaten Bereich. Damit enstanden erste bereichsspezifische Datenschutzregelungen. 1976 erschien der Endbericht der Kommission 'Koopmans', der neben einer ausführlichen Untersuchung von Datenschutzrisiken und -bedarf einen Vorentwurf für ein Personenregistergesetz umfaßte. Dieser Bericht bildete den Abschluß des zweiten Zeitabschnittes.

Die dritte Phase begann mit dem ersten Datenschutzgesetzentwurf, den die Regierung Ende 1981 veröffentlichte. Der Entwurf stimmte im wesentlichen mit dem Vorschlag der Kommission 'Koopmans' überein. Sein Anwendungsbereich bezog sich nur auf automatisiert geführte Personenregister. Wie die Datenschutzgesetze der skandinavischen Länder und Österreichs erhielt er ein Lizenzsystem. Eine Genehmigung war z.B. erforderlich für Personenregister mit 'sensiblen' Daten; Dateien mit 'weniger gefährlichen' Angaben, wie Mitgliederbeiträge von Vereinigungen, unterlagen nur einer Meldepflicht. Die übrigen Personenregister einer 'mittleren Kategorie' erforderten zwar keine Lizenz, die betreffenden speichernden Stellen mußten aber wie bei den genehmigungspflichtigen Personenregistern ein Datenschutzreglement erarbeiten. Die Kontrolle der Einhaltung des Gesetzes wurde an die Registrierkammer übertragen, die u.a. die Aufgaben erhielt, Lizenzen zu erteilen, Reglemente zu beurteilen und Meldungen in Empfang zu nehmen.

Der Gesetzentwurf wurde nicht sehr positiv aufgenommen. Die Kritik richtete sich vor allem auf die schwierige Abgrenzung von 'gefährlichen' und 'weniger gefährlichen' Personenregistern, die Undeutlichkeit vieler Gesetzesbegriffe und das Fehlen inhaltlicher Regelungen für den Umgang mit personenbezogenen Daten. Bei der parlamentarischen Behandlung überwog die Meinung, daß der Gesetzentwurf zu kompliziert, zu bürokratisch und zu kostspielig sei. Deswegen wurde das Gesetzgebungsverfahren nicht weitergeführt. Ein Gesetzgebungsteam des Justiz- und Innenministeriums erhielt den Auftrag, einen neuen Entwurf zu erstellen.

Im Rahmen einer allgemeinen Verfassungsnovellierung wurde das niederländische Grundgesetz 1983 u.a. um ein Grundrecht auf Achtung der persönlichen Lebenssphäre erweitert. Die Vorschrift legt im zweiten und dritten Absatz fest, daß innerhalb von fünf Jahren ein Datenschutzgesetz zu erlassen ist, das u.a. ein Auskunfts- und Berichtigungsrecht enthält. Durch diese Novellierung wurde der Gesetzgeber unter Druck gesetzt. Zwei Jahre nach der Verfassungsänderung veröffentlichte die Regierung den zweiten Datenschutzgesetzentwurf. In dem 85er Entwurf kam eine radikale Verminderung des Umfangs der Gesetzesvorschriften und ein anderes Gesetzgebungskonzept zum Ausdruck. Das Lizenzsystem wurde abgeschafft; anstelle desselben traten inhaltliche Vorschriften zur Speicherung und Übermittlung. Nach einer zweijährigen Beratungsperiode leitete die Zweite Kammer den Gesetzentwurf im Herbst 1987 weiter an die Erste Kammer des Parlaments. Da letztere grundlegende Kritik äußerte, war nicht auszuschließen, daß sie den Entwurf zurückweisen würde. Die Regierung konnte bei den letzten Beratungen im Spätherbst 1988 nicht alle Bedenken der Ersten Kammer ausräumen, so daß

die Annahme des Gesetzentwurfes Ende 1988 für den Außenstehenden ziemlich unerwartet kam. Für den Insider war deutlich, daß der Sozialminister einen wichtigen Einfluß auf den plötzlichen Abschluß des Gesetzgebungsverfahrens hatte. Der Sozialminister wollte unter allen Umständen zum 1.1.1989 ein sozialfiskales Personenkennzeichen einführen. Dies war nach den Bedingungen des Parlaments aber nur nach dem Inkrafttreten eines Datenschutzgesetzes möglich. Mitbedingt durch den politischen Druck wurden beide Gesetze schließlich am 27.12.1988 von der Ersten Kammer des Parlaments angenommen.

Eine ausführliche Auseinandersetzung mit der Entstehungsgeschichte des Personenregistergesetzes ist deswegen sinnvoll, weil sie uns hilft, typische Merkmale des niederländischen Datenschutzrechts zu verstehen (z.B. die Selbstregulierung). Es wird Ihnen sicherlich aufgefallen sein, daß es in den Niederlanden kein eigenes Datenschutzgesetz gibt. Das Gesetz, das mit dem Schutz personenbezogener Daten zu tun hat, heißt Personenregistergesetz. Dieser Name zeigt, daß der Gesetzgeber sich gleichermaßen auf Datenschutzbelange und den Bedarf an personenbezogenen Daten gerichtet hat.

Grundzüge des Personenregistergesetzes

Mit seinen 55 Artikeln ist das Gesetz auf beinahe die Hälfte des 81er Entwurfs reduziert. Die elf Abschnitte beinhalten folgende Regelungen:

- einleitende Bestimmungen (Definitionen, Ausnahmen von Anwendungsbereichen)
- allgemeine Bestimmungen (materielle Vorschriften)
- Datenübermittlungen an Dritte (allgemein und spezifisch für Adressen- und Informationshandel)
- Verhaltenscodes (Datenschutzzertifikat)
- spezifische Vorschriften für Personenregister von Einrichtungen der öffentlichen Verwaltung, des Unterrichts-, Gesundheits- und Sozialwesens (Reglementspflicht, Speicherungs- und Übermittlungsbestimmungen)
- Personenregister des Betriebs- und Berufslebens und der übrigen Bereiche (Meldepflicht)
- Rechte der Betroffenen (Kenntnisnahme und Korrektur)
- die Registrierkammer (Kontrollaufgaben und -befugnisse)
- internationale Aspekte
- Strafvorschriften
- Übergangs- und Schlußbestimmungen.

Die meisten Bestimmungen des Gesetzes sind am 1. Juli 1989 in Kraft getreten (Art. 54). Endgültig wird das Gesetz am 1. Juli 1990 wirksam. Schwerpunkte des Gesetzes sind der Grundsatz der Selbstregulierung der speichernden Stelle und das Prinzip der Selbsttätigkeit der Betroffenen. Der Gesetzgeber stellt die Selbstregulierung, die im 81er Entwurf bereits eine wichtige Rolle hatte, nunmehr zentral. Er verspricht sich von der Beteiligung der speichernden Stelle bei der Festlegung der Datenschutzregelungen mehr Problembewußtsein und Akzeptanz des Datenschutzes

und dadurch eine wirksame Gesetzgebung. Der Grundsatz der Selbstregulierung kommt in zweierlei Hinsicht zum Ausdruck. Zum ersten besteht im öffentlichen und 'semi'-öffentlichen Bereich eine Reglementspflicht. Dabei legen die betreffenden Datenhalter u.a. das Verfahren fest, das bei den Rechten des Betroffenen einzuhalten ist. Ähnliches gilt für die Meldepflicht im privatrechtlichen Bereich. Zweitens eröffnet der Gesetzgeber im vierten Abschnitt des Gesetzes die Möglichkeit, daß ein Verhaltenscode einer Organisation von speichernden Stellen ein Datenschutzzertifikat erhält, d.h., daß bestätigt wird, daß die Datenschutzregelungen dieser Stellen mit dem Datenschutzgesetz übereinstimmen.

Die Selbsttätigkeit des Betroffenen hat an Bedeutung gewonnen, da ihn die Registrierkammer bei der Ausübung seiner Rechte im heutigen Gesetz weniger unterstützt als im 81er Entwurf. Bei einem Konflikt mit dem Datenhalter kann er seine Rechte nur im Rahmen eines Zivilprozesses durchsetzen. Die Selbsttätigkeit des Registrierten ist auch durch die Tatsache wichtiger geworden, daß das Gesetz kaum noch Strafbestimmungen enthält. Während im 81er Entwurf beinahe jede gesetzeswidrige Handlung bestraft wurde, gilt dies heute nur noch für Verstöße gegen die Reglements- und Meldepflicht und für eine gesetzeswidrige Übermittlung personenbezogener Daten ins Ausland.

Ich möchte nun auf einige Aspekte des Gesetzes näher eingehen. Aus Zeitgründen mußte ich mich beschränken und habe vier Themen ausgewählt,. von denen ich meine, daß sie durch den unterschiedlichen Ansatz des niederländischen Gesetzgebers für die deutschen Strukturen besonders interessant sind.

- Zweck und Art des Gesetzes
- Anwendungsbereich
- Selbstregulierung
- Amtshilfe.

Ich mache also keine Ausführungen zu den allgemeinen Bestimmungen, den Rechten des Betroffenen und den Kontrollvorschriften. Die allgemeinen Bestimmungen und Rechte des Betroffenen weichen von den deutschen Datenschutzgesetzen ab, jedoch nicht so gravierend wie die Regelungen der Selbstregulierung.

Zweck und Art des Gesetzes

Eine Aufgabenbestimmung wie die deutschen Datenschutzgesetze kennt das Personenregistergesetz nicht. Übrigens ist die Aufnahme des Zwecks in den Gesetzestext in den Niederlanden nicht üblich. Er ergibt sich entweder aus einer Präambel oder - in den meisten Fällen - aus der Gesetzesbegründung. Bei meinen Ausführungen zur Entstehungsgeschichte erwähnte ich den Schutz der persönlichen Lebenssphäre als Ziel des niederländischen Datenschutzrechts. Was darunter zu verstehen ist, wurde bislang kaum ausgearbeitet. Die Kommission 'Koopmans' gab in ihrem Endbericht vier Gefahrenzonen zur Konkretisierung an:

- Verletzung des Bedürfnisses an Geheimhaltung persönlicher Angelegenheiten durch Verlust des Kontextes von Daten

- Verletzung des Selbstbestimmungsrechts durch Verstoß gegen die Zweckbindung von Daten
- Mangel an Transparenz von Entscheidungen
- Verletzungen durch Adressenhandel.

Weiterhin führt die Kommission aus, daß ein Recht auf persönliche Lebenssphäre die Ansprüche auf ein rechtmäßiges und richtiges Bildnis eines bestimmten Individuums beinhalte. Sie betonte dabei, daß es nicht um absolute Ansprüche gehe. Wir können feststellen: von einem informationellen Selbstbestimmungsrecht wird in den Niederlanden nicht ausgegangen. Hier herrscht ein pragmatischer Ansatz vor; die Konkretisierung der persönlichen Lebenssphäre wird offengelassen.

Nun zur Art des Gesetzes. In der Literatur wird es überwiegend als 'Rahmengesetz' bezeichnet. Die Argumente für diese Auffassung lauten:

- das Gesetz enthält viele unbestimmte Rechtsbegriffe
- es findet eine Delegation wichtiger Gesetzesmaßnahmen statt.

Ich kann mich dieser Meinung nach einem Blick auf andere Datenschutzgesetze nicht anschließen. Das Personenregister weist kaum mehr unbestimmte Rechtsbegriffe als die deutschen Datenschutzgesetze auf. Inhaltlich ist das Wichtigste selbst im Gesetz festgelegt. In 9 Fällen überträgt das Parlament die inhaltliche Ausgestaltung einer Vorschrift an die Regierung. Davon betreffen aber nur 5 Fälle wesentliche materielle Bestimmungen. Ich meine, daß Anzahl und Gegenstand der Delegation noch nicht die Bezeichnung als Rahmengesetz rechtfertigen.

Anwendungsbereich

Aus der Bezeichnung des Gesetzes folgt, daß es sich auf Personenregister bezieht. Nach Art. 1 ist ein Personenregister "eine zusammenhängende Sammlung von sich auf verschiedene individuelle natürliche Personen beziehenden Daten, die automatisiert geführt wird, oder die im Hinblick auf eine zweckmäßige Einsichtnahme in die Daten systematisch angelegt ist". Anders als der 81er Entwurf kommt das Gesetz also grundsätzlich auf automatisierte und manuelle Personenregister zur Anwendung. Für letztere ist ausschlaggebend, daß sie eine gewisse Systematik in der Datensammlung enthalten. Damit werden wenig strukturierte und nicht systematisch zugängliche, konventionelle Datensammlungen vom Anwendungsbereich ausgenommen. Ausgeschlossen werden weiterhin verschiedene andere Personenregister wie Datensammlungen, die ausschließlich zum 'persönlichen Gebrauch' bestimmt sind, Datenbestände von Presse, Radio und Fernsehen und Personenregister der Polizei und öffentlichen Sicherheit (Art. 2). Dateien von kirchlichen Organisationen fallen dagegen unter den Anwendungsbereich des Gesetzes.

Selbstregulierung

Bei einer Untersuchung der Selbstregulierungsformen des Personenregistergesetzes stellt sich zuerst die Frage, warum für öffentliche bzw. nichtöffentliche Datenhalter unterschiedliche Regelungen getroffen werden. Der Gesetzgeber begründet seine

Entscheidung, im privatrechtlichen Bereich eine Meldepflicht anstelle der Reglementspflicht einzuführen, mit bestehenden Datenschutzgefährdungen. Er vertritt dabei die Meinung, daß Personenregister des öffentlichen Bereichs restriktivere Regelungen erfordern würden, da ihre Anzahl, der Umfang der gespeicherten personenbezogenen Angaben und der Datenaustausch im allgemeinen umfassender und damit risikoreicher seien. Hinzu käme, daß der Bürger, der auf öffentliche Dienstleistungen angewiesen sei, in den meisten Fällen nicht selbst bestimmen könne, ob er Angaben über seine Person zur Verfügung stellen möchte. Bei privatrechtlichen Verhältnissen sei eine Entscheidungsfreiheit gegeben. Als weiteres Argument führt der Gesetzgeber an, daß der Regelungstyp 'Reglement' nicht für den privaten Bereich geeignet sei.

Nach Art. 20 Abs. 1 geht es bei dem Reglement um eine Beschreibung der Arbeitsweise des Personenregisters. Art. 20 Abs. 2 gibt elf Beispiele für diese Darlegung an. Sie umfaßt exemplarisch Regelungen zu den Fragen, wer welche Datenarten über welche Personenkategorien für welche Zwecke speichert bzw. erhält, wer direkten Zugang zu dem Register hat, in welchen Fällen die Daten aus dem Register entfernt werden, welche Verknüpfungen mit anderen Datenbeständen stattfinden, mit welchen Verfahren die Rechte der Registrierten auf Kenntnisnahme und Korrektur erteilt werden und welche Grundzüge die Datenverwaltung des Personenregisters aufweist.

Die Anmeldung der Personenregister privatrechtlicher Stellen erfolgt anhand eines ministeriellen Formulars, das an die Registrierkammer zu senden ist (Art. 24). Der Inhalt der Meldepflicht ist inzwischen gesetzlich festgelegt. Im Ergebnis hat die betreffende private Stelle die gleichen Angaben wie der öffentliche Datenhalter im Reglement zu erteilen. Nur anstelle der Darlegung der Grundzüge der Datenverwaltung sind internationale Aspekte getreten.

Interessant ist noch im Bereich der Selbstregulierung das Datenschutzzertifikat für Verhaltenscodes, die Verbände von Datenhaltern ausgearbeitet haben; es gilt grundsätzlich für alle speichernden Stellen. Da jedoch in der Praxis im wesentlichen privatrechtliche Organisationen mit der Erstellung solcher Codes befaßt sind, wird der vierte Abschnitt des Gesetzes vor allem im nicht-öffentlichen Bereich Bedeutung erlangen. Um ein Datenschutzzertifikat zu erhalten, müssen die betreffenden Verbände von Datenhaltern den Verhaltenscode der Registrierkammer vorlegen. Letztere erteilt das Zertifikat, wenn die Antragsteller einen bestimmten Wirtschaftszweig befugtermaßen vertreten, wenn der Code sorgfältig vorbereitet und dabei hinreichend mit den betreffenden Datenhaltern abgestimmt wurde, und wenn er den gesetzlichen Datenschutzvorschriften und anderen billigerweise zu stellenden Datenschutzanforderungen entspricht (Art. 15). Das Zertifikat beinhaltet die Erklärung der Registrierkammer, daß der Code den gesetzlichen und anderen Datenschutzbestimmungen genügt.

Die Funktion dieses Prüfungsverfahrens besteht darin, den betreffenden Organisationen Deutlichkeit über mögliche Verstöße ihrer Verhaltenscodes gegen Datenschutzregelungen zu verschaffen. Daneben kann ein Datenschutzzertifikat bewirken, daß das Vertrauen der Vertagspartner zunimmt. Das Zertifikat dient auch als Gutachten in einem Prozeß über Verletzungen von Datenschutzbestimmungen. Dabei hat es aber keine den Richter bindende Wirkung. Sollten die Verbände der

Datenhalter zukünftig keine Verhaltenscodes verfassen, dann kann der Gesetzgeber selbst Maßnahmen ergreifen und branchenspezifische Regelungen treffen (Art. 16). Erlauben Sie mir eine kritische Bemerkung zu der so wichtig erachteten Selbstregulierung:

Sie umfaßt m.E. in ihrer Ausgestaltung im Personenregistergesetz kaum eine echte Regelungstätigkeit. Die Ausarbeitung eines Reglements nach Art. 20 läuft in der Praxis hauptsächlich auf eine Bestandsaufnahme und Veröffentlichung der Betriebsweise des Personenregisters, seines Zwecks und Inhalts und der bestehenden Datenströme hinaus. Inhaltliche Regelungen hat der Datenhalter nur zur Festlegung von Löschungsfristen und zur Bestimmung von Verfahren zur Erteilung der Rechte des Registrierten zu treffen. Darum vermute ich, daß die Selbstregulierung eher die Funktion der Transparenz, des Erreichens von Datenschutzbewußtsein hat; eine inhaltliche Gestaltung von Personenregistern ist kaum gegeben. Die zukünftige Praxis wird zeigen, ob meine Vermutung stimmt.

Amtshilfe

Das Personenregistergesetz erleichtert den Austausch personenbezogener Daten im öffentlichen Bereich. Die Zweckbindung von Daten wird unter drei Bedingungen aufgehoben:

- wenn andere öffentliche Stellen die personenbezogenen Daten zur Aufgabenerfüllung benötigen
- wenn die persönliche Lebenssphäre des Registrierten nicht unverhältnismäßig verletzt wird
- und wenn die Daten nicht unter ein Berufs- bzw. Amtsgeheimnis fallen (Art. 18 Abs. 3).

Einer der Gründe dieser Vorschrift ist, den Datenzugriff zur Bekämpfung des Mißbrauchs öffentlicher Leistungen zu intensivieren.

Da die Bestimmung sehr allgemein formuliert ist, kann Sie einen Datenaustausch im öffentlichen Bereich zum Nachteil der betroffenen Bürger ermöglichen. Die Praxis wird zeigen, ob die Gesetzesvorschrift sich als die am meisten datenschutzgefährdende Regelung des Personenregistergesetzes erweist, wie ein Parlamentsmitglied während einer Beratung in der Zweiten Kammer behauptete.

Bereichsspezifisches Datenschutzrecht

Über bereichsspezifisches Datenschutzrecht habe ich bereits bei dem Thema 'Selbstregulierung' gesprochen. Die branchenspezifischen Verhaltenscodes (z.B. von Banken) oder Modellreglemente im öffentlichen Bereich (von Gemeinden) sind ein Beitrag zu konkreten Regelungen für spezifische Risiken bzw. spezifischen Datenverkehr. Weitere bereichsspezifische Regelungen enthalten:

- das Gesetz über öffentliche Sicherheitsdienste (1987)
- das Gesetz zur Einführung des sozialfiskalen PKZ (1988)
- der Entwurf zum Polizeiregistergesetz

- der Entwurf zur kommunalen Basisadministration
- verschiedene Regelungen für Gesundheitsdaten (u.a. der Gesetzentwurf zum Behandlungsvertrag).

Außerdem bestehen Berührungspunkte mit dem Gesetz zur Öffentlichkeit der Verwaltung, soweit es um den Zugang personenbezogener Daten geht, die in Dokumenten der öffentlichen Verwaltung enthalten sind. Aus Zeitgründen kann ich nicht auf alle diese Regelungen eingehen. Ich möchte deshalb nur etwas über die ersten zwei genannten Gesetze und über das Verhältnis von Personenregistergesetz und bereichsspezifischem Datenschutzrecht sagen.

Das Gesetz über öffentliche Sicherheitsdienste

Dieses Gesetz enthält eine gesetzliche Basis für die niederländischen öffentlichen Sicherheitsdienste, und zwar hinsichtlich ihrer Aufgaben und der dazu erforderlichen Personenregistern. Für datenschutzrechtliche Überlegungen sind vor allem drei Aspekte interessant:

- Speicherung und Übermittlung von Daten
- Auskunfts- und Korrekturrecht
- Kontrolle.

Bei der Speicherung ist für unser Thema wichtig, daß die Aufgabenstellung der Sicherheitsdienste so weit gefaßt ist, daß die Speicherung der erforderlichen Daten in sehr vielen Fällen zulässig ist. Sehr eingreifend ist auch die Vorschrift, die die speichernden Stellen zur Auskunft an öffentliche Sicherheitsdienste verpflichtet, auch wenn ihr Reglement oder Verhaltenscode dies nicht erlaubt. Der Datenbedarf der öffentlichen Sicherheit hat also erste Priorität.

Bei der *Übermittlung von Daten* gilt der Grundsatz, daß Geheimhaltung geboten ist, es sei denn, daß eine Offenbarungspflicht besteht. Es ist sehr schwierig, die Fälle anzugeben, in denen solch eine Offenbarungspflicht gegeben ist. Das Gesetz sagt nur ganz allgemein, daß die Übermittlung zur in dem Gesetz umschriebenen Aufgabenerfüllung erforderlich sein muß. Als weitere Abgrenzungskriterien gibt es die Übermittlung an interne Stellen (andere öffentliche Organe) und externe Einrichtungen (außerhalb des öffentlichen Bereichs) an. Eine genaue inhaltliche Angabe der Übermittlungsbefugnisse findet aber nicht statt. *Auskunfts- und Korrekturrecht* werden ausgeschlossen.

Einziges *Kontrollorgan* ist der nationale Ombudsmann, an den sich der Bürger mit Beschwerden über das Verhalten von öffentlichen Sicherheitsdiensten wenden kann. Die parlamentarische Kontrolle ist marginal.

Hieraus kann ich einige Schlußfolgerungen ziehen: das Gesetz macht einen lückenhaften Eindruck: Speicherungs- und Übermittlungsbefugnisse sind sehr extensiv festgelegt. Es ist bedauerlich, daß die Registrierkammer keine Kontrollbefugnisse erhalten hat, und daß die Möglichkeiten des Parlaments nicht, wie während der Diskussion des Gesetzentwurfs vorgeschlagen, ausgeweitet wurden. Dies hätte auch die fehlenden Rechte des Betroffenen kompensieren können.

Das Gesetz zur Einführung eines sozial-fiskalen Personenkennzeichens

Dieses Gesetz, das wie erwähnt am 27.12.1988 zusammen mit dem Personenregistergesetz verabschiedet wurde, bezweckt eine Neugestaltung der Verwaltung, der Übermittlung und des Austauschs von Versichertendaten. Die Neugestaltung geschah, um die Sozialversicherungsgesetze besser ausführen zu können, um Mißbrauch von Sozialleistungen zu bekämpfen, und um Daten für Planung und Politik zu liefern. Zur Unterstützung der Verwirklichung dieser Ziele wird das sozialfiskale Personenkennzeichen eingeführt, d.h. die Verwendung des fiskalen PKZ wird erweitert; ab 1.1.1989 wird es auch im Sozialversicherungsbereich benutzt. Das Sofi-Gesetz enthält insbesondere Vorschriften zur Ausgestaltung der Versichertenverwaltung (von fallbezogener zur personenbezogenen Datenverwaltung) und ausführliche Bestimmungen für Datenübermittlungen. Im Hinblick auf unser Thema möchte ich auf die Datenschutzbestimmungen näher eingehen. Da es mir für die deutsche Situation von besonderem Interesse erscheint, stelle ich auch Ausführungen zum sozial-fiskalen PKZ an.

Datenschutzbestimmungen des Sofi-Gesetzes

Der Gesetzgeber ist davon ausgegangen, daß der erhöhte Austausch von Versichertendaten den Bedarf an geeigneten Datenschutzmaßnahmen erhöht. Von zentraler Bedeutung sind die Geheimhaltungsvorschriften, die für alle Stellen gelten, die über Sozialversichertendaten verfügen. Dabei wird eine Zweckbindung festgelegt. Wie meistens gibt es verschiedene Ausnahmen von dem Offenbarungsverbot, z.B. wenn eine gesetzliche Vorschrift eine Offenbarung gebietet, wenn der Betroffene eingewilligt hat, bei Versicherungsbetrug oder für Zwecke wissenschaftlicher Forschung und Statistik.

Neben Geheimhaltungsvorschriften enthält das Gesetz auch eine allgemeine Datenschutzbestimmung. Danach unterbleiben Datenübermittlungen der Ausführungsorgane grundsätzlich, wenn dadurch die persönliche Lebenssphäre der Betroffenen unverhältnismäßig verletzt wird. Eine Verhältnismäßigkeitsbeurteilung orientiert sich an Datenschutzreglementen der Organe.

Datenschutzüberlegungen hat der Gesetzgeber auch hinsichtlich der Einführung des sozial-fiskalen Personenkennzeichens angestellt. In der Gesetzesbegründung geht er ausführlich auf das Minderheitsvotum des Rats der Sozialversicherung ein, der sich aus Datenschutzgründen gegen eine Verknüpfung von Steuer- und Sozialversicherungsdaten einsetzte und für ein eigenes Personenkennzeichen für die Sozialversicherung plädierte. Der Gesetzgeber weist darauf hin, daß die Organe der Sozialversicherung bereits das fiskale PKZ bei der Kommunikation mit dem Fiskus, Arbeitgebern, -nehmern und Unterstützungsempfängern verwenden würden, und daß dadurch die Datenschutzprobleme nicht zugenommen hätten. Er meint, daß der Gebrauch eines sozial-fiskalen PKZ eher den schutzwürdigen Belangen der Registrierten diene, denn er verringere die Möglichkeit, Personen zu verwechseln.

Bezüglich des Datenaustausches der Ausführungsorgane ist der Gesetzgeber der Auffassung, daß ein spezifisches soziales Personenkennzeichen die gleiche Wirkung

wie das sozial-fiskale Personenkennzeichen hätte und ineffizient wäre. Darüber hinaus würde ein spezifisches PKZ auch keine funktionelle Trennung der Steuer- und Sozialverwaltung zustande bringen. Weiterhin geht der Gesetzgeber auch auf die vielfach geäußerte Befürchtung ein, daß sich die sozial-fiskale Personennummer zu einem allgemeinen Personenkennzeichen entwickeln könnte. Er ist der Auffassung, daß diese Gefahr nicht realistisch ist, da die Verwendung des sozial-fiskalen Personenkennzeichens nur auf den Steuer- und Sozialversicherungsbereich gerichtet sei. Eine weitere Beschränkung sei durch die Geheimhaltungsvorschriften und Artikel 6 des Personenregistergesetzes gegeben, nach denen eine Weitergabe sozial-fiskaler Nummern und der dazugehörigen personenbezogenen Daten für andere als Steuer- und Sozialversicherungszwecke unzulässig sei. Zusammenfassend konstatiert der Gesetzgeber, daß die tatsächliche Einrichtung der Versichertendatenverwaltung und die gesetzlichen Garantien ausreichend sind, um einer unerwünschten Verwendung der Sofi-Nummer entgegenzuwirken. Die Meinung des Gesetzgebers ist nicht unwidersprochen geblieben. In der Literatur wird auf eine mögliche Gefährdung schutzwürdiger Belange der registrierten Bürger durch das Sofi-Gesetz gewiesen.

Die Kritik richtet sich vor allem auf eine Zunahme des Austausches personenbezogener Daten und eine Abnahme der Transparenz der Datenströme im öffentlichen Bereich. Ich meine, daß es verschiedene Anhaltspunkte gibt, die diese Kritik bestätigen. Ich kann nur feststellen, daß das Sofi-Gesetz Möglichkeiten zur erweiterten Verwendung personenbezogener Sozialdaten und damit zur Beeinträchtigung von Datenschutzbelangen bietet. Ob diese Gefährdung beschränkt bleibt, wird u.a. von einer restriktiven Anwendung des Zweckbindungsgrundsatzes abhängen. Die Einführung des sozial-fiskalen Personenkennzeichens ermöglicht eine Aufhebung der Trennung der Funktionsbereiche der öffentlichen Verwaltung. Letzteres kann zukünftig noch durch die Einführung eines zentralen Personenregisters der Sozialversicherungen verstärkt werden. Inwieweit das Personenkennzeichen auch Datenverknüpfungen im öffentlichen Bereich und mit dem privaten Sektor erleichtert, ist gegenwärtig noch nicht abzusehen. Um unerwünschte Entwicklungen zu vermeiden, sollten amerikanische Erfahrungen mit der 'social security number' berücksichtigt werden. Insgesamt vermittelt die neue Datenorganisation der niederländischen Sozialversicherung den Eindruck, daß sie die Macht der Verwaltung stärkt und die Position des Bürgers schwächt.

Das Personenregistergesetz im Rechtsvergleich

Mehrfach wurde gefragt, ob das niederländische Personenregistergesetz eine effektive gesetzliche Lösung bedeutet. Ich vermute, daß es nicht besser und nicht schlechter als andere europäische Datenschutzgesetze funktionieren wird. Meiner Meinung nach wird es entweder zu ähnlichen oder zu anderen Lösungen führen. 1985, in meiner rechtsvergleichenden Dissertation, nahm ich an, daß das niederländische Konzept der Selbstregulierung eine Benachteiligung der Betroffenen

verursachen würde.[1] Heute bin ich vorsichtiger geworden. Obwohl ich aus methodischen Gründen versuchte, die deutsche und niederländische Situation objektiv zu beurteilen, weiß ich heute, daß sich einige 'subjektive' deutsche Kriterien, die des Volkszählungsurteils, in meine Bewertung eingeschlichen haben. Heute, nachdem ich die niederländische Rechtskultur besser kenne, ist mir deutlich, daß die Selbstregulierung eine auf die niederländische Situation zugeschnittene Lösung beinhaltet, und daß die Maßstäbe des Volkszählungsurteils größtenteils nur zur deutschen Rechtsstaatstradition passen. Damit will ich aber nicht sagen, daß beide Länder nicht voneinander lernen können. Die Datenschutzprobleme überschreiten die Grenzen. Die automatisierte Verarbeitung personenbezogener Daten und der internationale Datenverkehr nehmen zu. Die technischen Infrastrukturen gleichen einander und die meisten westlichen, in Bälde auch östlichen Industrieländer haben sich einer demokratischen Staatsform und dem Schutz der Menschenrechte verpflichtet.

Der internationale Charakter des Datenschutzproblems fordert ein grenzüberschreitendes Konzept. Um dieses zu erreichen, müssen die Niederlande, Deutschland und andere Länder ihren eigenen Ansatz aufgeben und sich auf gemeinsame Basisregeln einigen. Ich glaube, daß eine traditionelle Harmonisierung nicht mehr der geeignete Weg ist. Sie bedeutet einen langwierigen und schwierigen Verhandlungsprozeß, in dem, wie die Erfahrungen im Europarat zeigen, nicht das zu lösende Datenschutzproblem zentral steht, sondern nationale Eigenbelange überwiegen. Einen anderen, sehr interessanten Lösungsweg erarbeitete die internationale Konferenz der Datenschutzbeauftragten im August 1989 in Berlin: sie nannten ihn Überschreitung des nationalen Ansatzes. Ausgangspunkt ist dabei, daß die Datenschutzgesetze grundsätzlich provisorische, novellierungsbedürftige Regelungen beinhalten. Überschreitung bedeutet hier, daß bei einer Änderung der nationalen Vorschriften die Ansätze anderer Länder berücksichtigt werden müssen. Ich meine, daß dieses Konzept sehr anspruchsvoll ist. Es bietet aber auch einen vielversprechenden Lösungsweg. Dieser Lösungsweg fordert von uns, daß wir uns über das Datenschutzrecht anderer Länder informieren. Ich hoffe, daß dieser Beitrag ein kleiner Schritt in diese Richtung sein kann.

---

[1] B.R. ZIEGLER-JUNG, *Datenverkehrsrecht und Gesundheitsdatenschutz in der BRD und den Niederlanden*, Enschede 1985; B.R. ZIEGLER-JUNG, *Das niederländische Datenschutzgesetz*, in: DuD 1989. S.329f; B.R. ZIEGLER-JUNG, *Das sozial-fiskalische Personenkennzeichen in der niederländischen Gesetzgebung*, in: DuD 1989. S.551f.