

## **Vorblatt**

**Entwurf eines Gesetzes  
zum Schutz vor unbefugter Verwendung personen-  
bezogener Daten  
(Datenschutzgesetz)  
(Gesetzentwurf der Abgeordneten Hirsch, Dichgans,  
Kirst und Genossen)**

### **A. Problem**

Durch den wachsenden Einsatz moderner technischer Methoden der Datenverarbeitung können gewisse in Wirtschaft und Verwaltung benötigte Daten immer schneller und leichter beschafft werden. Integrierte Systeme ermöglichen es, Daten, die z. B. zu einer Person an verschiedenen Stellen vorhanden sind, abzurufen und so eine Übersicht zu erhalten, die die Privatsphäre beeinträchtigen kann. Die Handhaben zum Schutze der Privatsphäre sind nicht ausreichend, um möglichen Mißbrauch weitgehend zu unterbinden. Der Gesetzgeber darf es nicht versäumen, rechtzeitig Schutzvorschriften zu erlassen.

### **B. Lösung**

Der Entwurf will die Problematik hinsichtlich personenbezogener Daten, soweit sie vom Bund und durch wirtschaftlich verwertbare Datenbanken Privater erfaßt werden, regeln. Der Schutz der personenbezogenen Daten bei Ländern und Kommunen fällt in die Gesetzgebungskompetenz der Länder. Das Schutzsystem des Entwurfs sieht vor, daß der Bürger gegenüber den Datenbanken umfassende Auskunftsansprüche, ein Recht auf Berichtigung fehlerhafter oder auf Löschung unbefugt gespeicherter Daten bzw. Schadensersatzansprüche hat. Die

Weitergabe von personenbezogenen Daten soll nur aufgrund besonderer Rechtsgrundlage zulässig sein.

### **C. Alternativen**

Mit dem Gesetzentwurf wird Neuland betreten, so daß natürlich zu den einzelnen Vorschlägen Alternativen möglich sind. Soweit sie bekannt waren, sind sie bei der Ausarbeitung des Entwurfs diskutiert und zum Teil in der beigefügten Begründung erwähnt worden.

### **D. Kosten**

Die Kosten für die Aufsicht richten sich im wesentlichen nach der Zahl der meldepflichtigen Datenbanken. Für die bundeseigenen Einrichtungen sind die entstehenden Kosten zu tragen, während für private Datenbanken Gebühren erhoben werden könnten.

Welche Veränderungen bzw. Ergänzungen an den technischen Anlagen notwendig werden, ist noch nicht abschätzbar und wird für die verschiedenen Typen unterschiedlich sein, wobei sie angesichts der Bedeutung des Schutzes der Privatsphäre nach den vorliegenden Auskünften in jeder Hinsicht tragbar sein dürften.

**Antrag**  
**der Abgeordneten Hirsch, Dichgans, Kirst und Genossen**

Der Bundestag wolle beschließen:

**Entwurf eines Gesetzes**  
**zum Schutz vor unbefugter Verwendung personenbezogener**  
**Daten**  
**(Datenschutzgesetz)**

Der Bundestag hat das folgende Gesetz beschlossen:

1. ABSCHNITT

Allgemeine Vorschriften

§ 1

**Bereich des Datenschutzes**

Der Datenschutz erfaßt alle für Zwecke der herkömmlichen und der maschinentechnischen Datenverarbeitung erstellten Unterlagen, insbesondere alle gespeicherten personenbezogenen Daten und die Ergebnisse ihrer Verarbeitung.

§ 2

**Inhalt des Datenschutzes**

Die vom Datenschutz erfaßten Unterlagen, Daten und Ergebnisse sind so zu ermitteln, weiterzuleiten, zu verarbeiten und aufzubewahren, daß sie nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können.

§ 3

**Anspruch auf Datenschutz**

(1) Jeder hat ein Recht auf Auskunft über die zu seiner Person gesammelten Daten, sofern dies nicht durch Gesetz ausgeschlossen ist.

(2) Sind über den Betroffenen aufgezeichnete Daten falsch, unvollständig, überholt oder im Verhältnis zum angestrebten Zweck falsch gewichtet, so kann er Berichtigung, Löschung oder Erweiterung der Daten verlangen. Stellt die Speicherung als solche im einzelnen oder zusammen mit anderen Daten ein unzulässiges Eindringen in die Privatsphäre dar, so kann der Betroffene eine Löschung verlangen, auch wenn die Daten an sich richtig sind.

(3) Wird der Betroffene durch eine widerrechtliche Speicherung, Einsicht, Änderung oder Vernichtung oder durch einen widerrechtlichen Abruf in seinen Rechten verletzt, kann er Schadensersatz verlangen. Darüber hinaus kann der Betroffene Widerruf verlangen, wenn verletzende Daten an Dritte gelangt sind.

2. ABSCHNITT

Datenbanken des Bundes

§ 4

**Geltungsbereich**

(1) Die Vorschriften dieses Abschnittes gelten für Datenbanken des Bundes und der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, in denen personenbezogene Daten gespeichert und neben der Verwertung für Zwecke der einspeichernden Stelle

auch für andere Stellen oder Dritte zur Auskunft oder Einsicht bereitgehalten werden. Ausgenommen sind das Bundesamt für Verfassungsschutz, der militärische Abschirmdienst und der Bundesnachrichtendienst.

(2) Die Vorschriften dieses Abschnittes gelten nicht für Personalakten, sofern diese nicht einem Informationssystem eingegliedert sind.

(3) Die Vorschriften gelten ferner nicht für politische oder Presse-Informationssysteme, die für die Öffentlichkeit bestimmte Äußerungen von Personen speichern und verwerten.

(4) Für das Bundeszentralregister hat es bei den Vorschriften des Gesetzes über das Zentralregister und das Erziehungsregister vom 18. März 1971 sein Bewenden.

(5) Personenbezogene Daten aus Datenbanken oder Datensammlungen der in Absatz 1 bezeichneten Stellen, für die die Vorschriften aus diesem Abschnitt nicht gelten, dürfen Dritten nur weitergegeben werden, wenn die Voraussetzungen des § 8 Abs. 1 und 2 vorliegen. Ist eine Auskunft erteilt worden, so ist der Betroffene davon zu unterrichten, sofern es sich nicht um die Auskunft eines der in Absatz 1 Satz 2 genannten Dienste handelt oder dies sonst spezialgesetzlich ausgeschlossen ist; § 9 Abs. 5 und 6 gilt entsprechend.

#### § 5

##### Anmeldepflicht

(1) Jede im Geltungsbereich des § 4 betriebene Datenbank, in der personenbezogene Daten gespeichert werden, ist bei dem von der Aufsichtsbehörde geführten Datenbank-Register anzumelden.

(2) Die Anmeldepflicht besteht ungeachtet der Methode, mit der Informationen erlangt, zusammengestellt, verarbeitet oder weitergegeben werden.

(3) Bei der Anmeldung ist nachzuweisen, welche organisatorischen, maschinen- und programmtechnischen Vorkehrungen getroffen sind, damit der Zugriff auf die Daten nur durch dazu Berechtigte gewährleistet ist.

#### § 6

##### Eintragung in das Register

(1) Die Anmeldung muß folgende Angaben enthalten:

1. Behörde, Dienststelle oder sonstige Bezeichnung,
2. System der Datenspeicherung,
3. Zweck der Datenspeicherung,
4. Art der gespeicherten Daten,
5. die Bediensteten, die ermächtigt sind, Daten einzuspeichern oder zu entnehmen, durch Bezeichnung der Dienststellung.

(2) Jede Änderung der einzutragenden Tatsachen ist der Aufsichtsbehörde unverzüglich anzuzeigen.

#### § 7

##### Protokoll

(1) Werden Datenbanken maschinentechnisch oder elektronisch geführt, so ist das Programm so zu gestalten, daß Auskunft erteilt werden kann über (Protokoll):

- a) das Datum jeder Eingabe von Daten,
- b) das Datum jeder Entnahme bzw. Übermittlung von Daten,
- c) den Namen des Bearbeiters,
- d) den Namen und die Anschrift der die Daten anfordernden Personen oder Dienststellen,
- e) die Art der weitergegebenen Daten,
- f) den Zweck, zu dem Daten angefordert wurden.

(2) Das Protokoll nach Absatz 1 ist zu erstellen, unabhängig, ob die Datenausgabe verschlüsselt oder verbalisiert erfolgt, entfällt jedoch, wenn der Betroffene nicht identifizierbar ist.

(3) Gibt die Datenbank auf ein Ersuchen keine Auskunft, so ist das unter Angabe des Grundes zu protokollieren.

(4) Ausgenommen von der Pflicht, ein Protokoll nach Absatz 1 zu erstellen, sind Datenbanken, in denen nur statistisches Material ohne die Identitätsmerkmale der Betroffenen eingespeichert und verwertet werden.

#### § 8

##### Auskunfts berechtigung

(1) Eine Weitergabe personenbezogener Daten an Dritte ist nur zulässig, wenn dem Empfänger ein Recht auf Kenntnisnahme auf Grund einer Rechtsvorschrift zusteht, es sei denn, daß bei der Auskunft keine Rückschlüsse auf Einzelpersonen möglich sind.

(2) Eine generelle Befugnis, personenbezogene Daten innerhalb eines Verwaltungsressorts oder zwischen verschiedenen Verwaltungsressorts oder Behörden oder Einrichtungen der öffentlichen Hand beliebig abzurufen, auszutauschen oder zu verwerten, besteht nicht. Jedes Verwaltungsressort darf unbeschadet eines Rechts nach Absatz 1 nur Daten abrufen, die es selber eingegeben hat.

(3) Einzelangaben über personenbezogene Daten oder sachliche Verhältnisse natürlicher oder juristischer Personen, die für eine Statistik gemacht wurden, sind geheimzuhalten.

(4) Bei den statistischen Datenbanken sind die Erhebungsformulare mit den Identitätsmerkmalen der Befragten zu vernichten, soweit die davon gewonnene Statistik abgeschlossen ist. Bei Langzeit-, Wanderungs- und Strömungstatistiken, die ein Zurückschauen auf einmal befragte Personen erfordern, dürfen die gewonnenen Daten nur nach einem bundeseinheitlichen Personenkennzeichen gespeichert werden.

Eine Zuordnungsliste von Personenkennzeichen und Namens- und Adressenteil darf sich nur bei den noch im Gesetz über das Meldewesen zu bestimmenden Vergabestellen befinden.

Daten, die unter dem PKZ gespeichert sind, dürfen nicht mehr mit dem Namens- und Adressenteil versehen werden.

### § 9

#### Recht auf Auskunft

(1) Über die erste Dateneingabe personenbezogener Daten in einer Datenbank ist dem Betroffenen ohne Antrag eine Mitteilung gebührenfrei zu übersenden, es sei denn, er hat der Datenaufnahme ausdrücklich zugestimmt oder die Eingabe der Daten beruht auf einer unmittelbaren Befragung des Betroffenen.

(2) Auf Antrag ist dem Betroffenen jederzeit gemäß § 3 Abs. 1 Einsicht in die über ihn gespeicherten Daten zu gewähren. Sind die Daten nur maschinenlesbar gespeichert, ist dem Antragsteller ein Ausdruck zu erteilen. Der Ausdruck kann auf die Eingaben beschränkt werden, die seit dem letzten Ausdruck hinzugekommen sind; darüber hinaus erhält der Betroffene auf besonderen Antrag einen vollständigen Ausdruck.

(3) Auf Antrag ist dem Betroffenen über alle ihn betreffenden Dateneingaben und Auskünfte nach dem Protokoll (§ 7 Abs. 1) Auskunft zu erteilen. Binnen vier Wochen nach Zustellung dieser Auskunft kann der Betroffene eine Kopie der über ihn an andere Stelle oder Dritte im Auskunftszeitraum erteilten Auskünfte verlangen.

(4) Alle Ausdrücke mit Ausnahme der Mitteilung nach Absatz 1 sind gebührenpflichtig. Die Gebühr ist nach dem tatsächlichen Verwaltungsaufwand zu bemessen.

(5) Absätze 2 und 3 gelten nicht für Datenbanken des Bundeskriminalamtes, sofern es sich bei den eingespeicherten Daten um kriminaltechnische Daten handelt.

(6) Die Absätze 1 bis 3 gelten nicht für ohne Identitätsmerkmale gespeicherte Daten.

### § 10

#### Verschwiegenheitspflicht

(1) Alle Personen, die mit der Datenerfassung, dem Datentransport, der Datenspeicherung oder in sonstiger Weise mit der Datenverarbeitung betraut sind, ist, unbeschadet sonstiger Geheimhaltungspflichten, untersagt, die bei ihrer amtlichen Tätigkeit erlangten Kenntnisse über Unterlagen, Daten und Ergebnisse unbefugt zu offenbaren oder zu verwerten oder anderen unbefugten Personen die Kenntnisse zu ermöglichen, sowie solche Daten zu einem anderen als bei der Erhebung angegebenen Zweck zu nutzen, soweit nicht der Betroffene einwilligt hat.

(2) Die Pflicht zur Geheimhaltung besteht auch nach der Beendigung der in Absatz 1 bezeichneten Tätigkeit.

(3) Gesetzliche Informations-Befugnisse und Auskunftspflichten bleiben unberührt.

### § 11

#### Datenaustausch mit Datenbanken nach Landesrecht

Datenaustausch zwischen Datenbanken nach § 4 Abs. 1 und Landesrecht unterstehenden Datenbanken im Rahmen eines automatischen Zugriffssystems darf nur erfolgen, wenn das einschlägige Landesrecht mit den in diesem Gesetz festgelegten Grundsätzen übereinstimmt.

### 3. ABSCHNITT

#### Private Datenbanken

### § 12

#### Geltungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für Datenbanken von Unternehmen privaten Rechts gleich welcher Rechtsform, sofern dabei in Ausübung eines Gewerbes oder Berufes personenbezogene Daten gespeichert werden, die neben der Verwendung für eigene Zwecke auch zur Weitergabe an Dritte bereitgehalten werden.

(2) Die Vorschriften gelten nicht für Personalakten, sofern diese nicht in ein umfassenderes Auskunftssystem eingegliedert sind.

(3) § 4 Abs. 3 gilt entsprechend.

(4) Die Aufsichtsbehörde entscheidet in Zweifelsfällen, ob eine Datenbank den Vorschriften dieses Gesetzes unterliegt.

(5) Personenbezogene Daten aus Datenbanken oder Datensammlungen, der in Absatz 1 bezeichneten Unternehmen, die Daten nicht zur Weitergabe an Dritte bereithalten und für die die Vorschriften aus diesem Abschnitt deshalb nicht gelten, dürfen Dritten nur weitergegeben werden, wenn die Voraussetzungen des § 16 vorliegen. Ist eine Auskunft erteilt worden, so ist der Betroffene davon zu unterrichten.

### § 13

#### Anmeldepflicht

(1) Jede im Geltungsbereich des § 12 betriebene Datenbank ist bei dem von der Aufsichtsbehörde geführten Datenbankregister anzumelden.

(2) Anmeldepflichtig sind der Inhaber der Datenbank oder dessen Stellvertreter, bei juristischen Personen, Gesellschaften und nicht rechtsfähigen

Vereinen die nach Gesetz oder Satzung zur Vertretung berufenen Personen.

(3) Die Anmeldepflicht besteht ungeachtet der Methode, mit der Informationen erlangt, zusammengestellt, verarbeitet oder verwertet werden.

(4) Bei der Anmeldung ist nachzuweisen, daß organisatorische, maschinentechnische und programmtechnische Vorkehrungen getroffen sind, damit der Zugriff auf die Daten nur durch dazu Berechtigte gewährleistet ist.

#### § 14

##### **Eintragung in das Register**

(1) Die Anmeldung muß folgende Angaben enthalten:

1. Name, Firma oder sonstige Bezeichnung,
2. Ort der Niederlassung,
3. System der Datenspeicherung,
4. Art der gespeicherten Daten,
5. Zweck der Datenspeicherung,
6. die Angehörigen des Unternehmens, die ermächtigt sind, in eigener Verantwortung Daten einzuspeichern und zu entnehmen, durch Bezeichnung ihrer Stellung.

(2) Jede Änderung der einzutragenden Tatsachen ist der Aufsichtsbehörde unverzüglich anzuzeigen.

#### § 15

##### **Protokoll**

§ 7 gilt für Datenbanken dieses Abschnittes entsprechend.

#### § 16

##### **Auskunfts berechtigung**

(1) Eine Weitergabe personenbezogener Daten an Dritte ist nur zulässig, wenn dem Empfänger ein Recht auf Kenntnisnahme auf Grund einer Rechtsvorschrift, der Einwilligung des Betroffenen oder eines sonstigen vom Recht anerkannten Rechtfertigungsgrundes zusteht, es sei denn, daß der Betroffene bei der Auskunft nicht identifizierbar ist.

(2) Als Auskunft an Dritte gilt auch eine Auskunft an Mitglieder von Verbänden, deren Zusammenschluß unter anderem zumindest auch der Erleichterung des Datenaustausches innerhalb des Verbandes dient.

#### § 17

##### **Recht auf Auskunft**

(1) § 9 Abs. 1, 2, 3 und 6 gelten für Datenbanken dieses Abschnittes entsprechend.

(2) Der Unternehmer der Datenbank kann für Auskünfte nach § 9 Abs. 2 und 3 ein Entgelt verlangen, das die durch die Auskunft entstehenden Betriebskosten nicht übersteigen darf.

#### 4. ABSCHNITT

##### Aufsichtsbehörden

#### § 18

##### **Zuständigkeit**

Der Bundesminister . . . nimmt die in diesem Gesetz der Aufsichtsbehörde übertragenen Aufgaben und Befugnisse wahr gegenüber:

- a) den Behörden und Einrichtungen des Bundes,
- b) den der Aufsicht des Bundes unterstellten Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts,
- c) gegenüber den Datenbank-Unternehmen privaten Rechts.

#### § 19

##### **Register**

(1) Die Aufsichtsbehörde führt das Register der diesem Gesetz unterstehenden Datenbanken.

(2) Das Datenbank-Register ist öffentlich und kann von jedem, der ein berechtigtes Interesse glaubhaft macht, eingesehen werden, soweit nicht ausdrücklich im Gesetz etwas anderes bestimmt wird.

#### § 20

##### **Aufgaben, Tätigkeitsbericht**

(1) Die Aufsichtsbehörde führt die Aufsicht über die nach diesem Gesetz zum Register anzumeldenden Datenbanken, um die Privatsphäre der Betroffenen vor unbefugter Verwendung personenbezogener Daten zu schützen.

(2) Soweit die Aufsichtsbehörde nicht selbst eingreifen kann, unterrichtet sie die zuständige Fachaufsichtsbehörde über festgestellte Verstöße und regt Vorkehrungen zur Verbesserung des Datenschutzes an.

(3) Der Bundesminister . . . leitet dem Bundestag jährlich einen Tätigkeitsbericht zu. Der Bericht soll insbesondere auch die Entwicklung bei der Errichtung neuer Datenbanken und bei der Datenüberwachung in der Bundesrepublik Deutschland erläutern und die Erfahrungsberichte der zuständigen Landesbehörden berücksichtigen.

#### § 21

##### **Befugnis der Aufsichtsbehörde**

(1) Soweit es zur Erfüllung der der Aufsichtsbehörde in diesem Gesetz übertragenen Aufgaben erforderlich ist, können Beauftragte der Aufsichtsbehörde

1. vom Unternehmer der Datenbank Auskunft über seine Tätigkeit verlangen,
2. innerhalb der Dienst- bzw. Geschäftszeiten die Räume der Datenbank betreten und Unterlagen einsehen und prüfen.

(2) Die verlangten Auskünfte zu erteilen, die Unterlagen der Datenbank vorzulegen und deren Prüfung zu gestatten sowie das Betreten der entsprechenden Räume zu dulden, sind verpflichtet

- a) bei Datenbanken nach § 4 der Behörden-, Anstalts- oder Stiftungsvorstand,
- b) bei Datenbanken nach § 12 der Inhaber oder die nach Gesetz, Satzung oder sonst zur Vertretung berufenen Personen.

(3) In einer von der Aufsichtsbehörde angeforderten Auskunft ist die Rechtsgrundlage des Auskunftsverlangens anzugeben und eine angemessene Frist zur Erteilung der Auskunft zu bestimmen.

(4) Ist die Aufsichtsbehörde der Auffassung, daß der Zweck der Datenbank oder die Art der gespeicherten Daten in unzumutbarer Weise in das Persönlichkeitsrecht einer oder mehrerer Personen eindringt, so kann sie gegenüber Datenbanken nach § 12 anordnen, daß Eintragungen über diese Personen in der Datenbank gelöscht, berichtigt oder nicht darin eingegeben werden und daß die Abordnung sämtlichen Empfängern der betreffenden Daten mitzuteilen ist. In besonders schwerwiegenden Fällen kann die Aufsichtsbehörde die begrenzte oder dauernde Stilllegung des Betriebs der Datenbank verfügen.

(5) Liegen die Voraussetzungen des Absatzes 4 bei Datenbanken nach § 4 vor, so hat die Aufsichtsbehörde bei der zuständigen Fachaufsichtsbehörde anzuregen, entsprechend tätig zu werden.

(6) Bei Datenbanken nach § 12 kann die Aufsichtsbehörde Durchsuchungen durchführen. Die §§ 102 bis 107 StPO und § 110 StPO finden mit der Maßgabe entsprechend Anwendung, daß an die Stelle der Staatsanwaltschaft die Aufsichtsbehörde tritt.

(7) Die bei der Aufsichtsbehörde beschäftigten oder von ihr beauftragten Personen haben vorbehaltlich der dienstlichen Berichterstattung und der Anzeige von Gesetzeswidrigkeiten die durch Auskünfte nach Absatz 1 Nr. 1 oder Maßnahmen nach Absatz 1 Nr. 2 erlangten Kenntnisse und Unterlagen über einzelne Datenbanken und Daten geheimzuhalten. Die Pflicht zur Geheimhaltung besteht auch nach der Beendigung der Tätigkeit für die Aufsichtsbehörde.

## § 22

### Verwaltungsverfahren

(1) Bei dem Verfahren vor der Aufsichtsbehörde sind zu hören:

1. wer die Einleitung eines Verfahrens beantragt hat,
2. Datenbank-Unternehmen, gegen die sich das Verfahren richtet,
3. Personen und Personenvereinigungen, deren Interesse durch die Entscheidung erheblich berührt werden und die die Aufsichtsbehörde auf ihren Antrag zum Verfahren beigelegt hat,

4. bei Maßnahmen nach § 21 Abs. 4 und 5 der Betroffene, wenn die Zahl der Betroffenen begrenzt und ihre Teilnahme am Verfahren daher tunlich ist.

(2) Die Aufsichtsbehörde hat den Beteiligten Gelegenheit zur Stellungnahme zu geben und sie auf Antrag eines Beteiligten zu einer mündlichen Verhandlung zu laden, wenn eine solche für erforderlich gehalten wird.

(3) Entspricht der Unternehmer einer Datenbank einem auf § 3 Abs. 2 gestützten Anspruch nicht, kann der Betroffene auch bei der Aufsichtsbehörde ein Einschreiben nach § 21 Abs. 4 oder 5 beantragen. Wird dieser Antrag abgelehnt, so unterliegt diese Entscheidung nicht der Anfechtung.

(4) Im übrigen bleibt der Rechtsweg gegen den Unternehmer der Datenbank unberührt.

## § 23

### Zwangsmittel

(1) Die Aufsichtsbehörde kann die Befolgung der Verfügungen gegen Datenbanken nach § 12 mit Zwangsmitteln nach den Bestimmungen des Verwaltungs-Vollstreckungsgesetzes vom 29. April 1963 (Bundesgesetzbl. I S. 157) durchsetzen.

(2) Die Höhe des Zwangsgeldes beträgt bis zu 50 000 Deutsche Mark.

## 5. ABSCHNITT

### Straf- und Bußgeldbestimmungen

## § 24

### Strafbestimmungen

(1) Mit Freiheitsstrafe bis zu einem Jahr und mit Geldstrafe oder mit einer dieser Strafen wird bestraft, wer

- a) personenbezogene Daten, die ihm im Zusammenhang mit der Datenverarbeitung bekanntgeworden sind, unbefugt offenbart oder verwertet,
- b) den Zugriff auf solche Daten unbefugt gewährt,
- c) Datenleitungen anzapft, um den Datentransport zu stören oder Daten unbefugt abzurufen,
- d) Programme einführt, die Informationen so speichern und wiederauffinden, daß sie dem ursprünglichen bei der Anmeldung genannten Zweck zuwiderlaufen,
- e) die in der Datenbank gespeicherten Daten zu anderen als den im Register verzeichneten Zwecken verwendet oder dies zuläßt.

(2) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer in Kenntnis ihres

rechtswidrigen Erwerbs Informationen, die nach Absatz 1 in strafbarer Weise erlangt wurden, entgegennimmt, verwendet, bearbeitet oder in sonstiger Weise darüber verfügt.

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einem anderen einen Vermögensvorteil zu verschaffen, so ist die Strafe Freiheitsstrafe bis zu drei Jahren; daneben kann auf Geldstrafe erkannt werden. Ebenso wird bestraft, wer fremde personenbezogene Daten, die ihm in seiner Eigenschaft als Angehöriger oder Beauftragter der Aufsichtsbehörde bekanntgeworden sind, unbefugt verwertet.

#### § 25

##### Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

- a) seiner Anmeldepflicht nach § 5 bzw. § 13 dieses Gesetzes nicht nachkommt,
- b) den Vorschriften über das Protokoll (§§ 7, 15) zuwiderhandelt,
- c) es unterläßt oder sich weigert, dem Betroffenen die ihm nach § 9 oder § 17 zustehenden Mitteilungen, Auszüge und Kopien zu übermitteln,
- d) einer unanfechtbar gewordenen Verfügung der Aufsichtsbehörde nach § 21 Abs. 4 zuwiderhandelt, sofern die Verfügung auf die Bußgeldbestimmungen dieses Gesetzes verweist,
- e) Auflagen der Aufsichtsbehörde zuwiderhandelt, die in einer Verfügung nach Buchstabe d enthalten sind,
- f) eine nach § 21 Abs. 3 angeforderte Auskunft falsch erteilt.

(2) Die Ordnungswidrigkeit kann, wenn sie

- a) vorsätzlich begangen ist, mit einer Geldbuße bis zu 50 000 Deutsche Mark,
- b) fahrlässig begangen ist, mit einer Geldbuße bis zu 10 000 Deutsche Mark

geahndet werden.

#### § 26

##### Bußgeldverfahren, Zuständigkeit

Für die Verfolgung von Ordnungswidrigkeiten nach § 25 dieses Gesetzes ist die Aufsichtsbehörde die Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten.

#### § 27

##### Zuständigkeit für den Einspruch

Im gerichtlichen Verfahren wegen einer Ordnungswidrigkeit nach § 25 dieses Gesetzes entscheidet auf Einspruch das Landgericht, in dessen Bezirk die betroffene Datenbank steht.

#### 6. ABSCHNITT

##### Schlußbestimmungen

#### § 28

##### Ermächtigungen

(1) Der Bundesminister . . . wird ermächtigt, durch Rechtsverordnung zu regeln,

1. welche Vorkehrungen zu treffen sind, um unter Berücksichtigung der wirtschaftlichen Belastbarkeit und bei Beachtung der Kenntnisse des jeweils neuesten Standes der technischen Entwicklung den in § 5 Abs. 3 und § 13 Abs. 4 auf personellem und technischem Gebiet des Datenschutzes aufgestellten Erfordernissen zu genügen,
2. in welcher Form die nach § 9 Abs. 3 oder § 17 Abs. 1 zu erteilende Auskunft zu ergehen hat, insbesondere welche Abkürzungen und maschinentechnischen Vereinfachungen zugelassen sind,
3. in welcher Form die Mitteilung der ersten Dateneingabe in eine Datenbank an den Betroffenen zu erfolgen hat,
4. welche Grundsätze bei der Erstattung der durch das Verfahren vor der Aufsichtsbehörde entstehenden Kosten Anwendung finden.

#### § 29

##### Änderung des StatG

§ 12 des Gesetzes über die Statistik für Bundeszwecke wird wie folgt geändert:

Absatz 1 Satz 1 erhält folgende Fassung:

„Einzelangaben über persönliche und sachliche Verhältnisse von befragten Personen oder Gewerbeunternehmen, die für eine Bundesstatistik gemacht wurden, sind geheimzuhalten.“

Absatz 2 wird ersatzlos gestrichen.

#### § 30

##### Inkrafttreten

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

Bonn, den 2. Dezember 1971



Hirsch  
Bauer (Würzburg)  
Dr. Dr. h. c. Bechert (Gau-Algesheim)  
Brück (Holz)  
Dr. Dübber  
Dürr  
Frau Eilers  
Engholm  
Hansen  
Dr. Hauff  
Frau Huber  
Killat-von Coreth  
Dr. Müller-Emmert  
Peters (Norden)  
Dr. Schmidt (Krefeld)  
Dr. Schmitt-Vockenhausen  
Schoettle  
Schonhofen  
Schwabe  
Spillecke

Dichgans  
Adorno  
Benda  
Bremer  
Dr. Evers  
Dr. Furler  
Frau Geisendörfer  
Dr. Gruhl  
Dr. Hammans  
Dr. Jungmann  
Dr. Dr. h. c. Löhr  
Mommel  
Ruf

Prinz zu Sayn-Wittgenstein-Hohenstein  
Dr. Schmidt (Wuppertal)  
Dr. Schneider (Nürnberg)  
Dr. Schulz (Berlin)  
Dr. Schwörer  
Frau Tübler  
Wagner (Günzburg)  
Frau Dr. Walz

Kirst  
Frau Dr. Diemer-Nicolaus  
Graaff

## Begründung

### Vorbemerkung

Dieser Gesetzentwurf kann nicht den Anspruch erheben, in allen Punkten völlig ausdiskutiert und ausgereift zu sein. Entsprechend der Tatsache, daß mit dieser Gesetzesinitiative völliges Neuland betreten wird, wären umfangreiche Anhörungen erforderlich gewesen, um die wesentlichen Weichenstellungen des Entwurfs abzusichern. Hiervon glaubten die Urheber absehen zu können, da es Ihnen in erster Linie darauf ankam, mit einer fundierten Diskussionsunterlage einen Anstoß zu geben. Sie halten aber für nötig, daß die zuständigen Ausschüsse des Bundestages unter anderem folgende Punkte auch in einem Hearing sorgfältig abwägen:

- a) Ist die Verrechtlichung der Verwaltung von personenbezogenen Daten, wie sie die Bestimmungen des § 8 Abs. 1 und Abs. 2 fordern (vgl. auch Begründung), verfassungsrechtlich zwingend, oder tut auch eine die Verwaltung weniger belastende Konzeption der Rechtsstaatlichkeit Genüge?
- b) Wie können die Geheimdienste über die Bestimmungen des § 4 Abs. 1 und 5 sowie des § 8 Abs. 1 und 2 hinaus den Zielsetzungen des Gesetzes unterworfen werden?
- c) Sind die Bestimmungen über den Geltungsbereich des Gesetzes in § 4 und § 12 so abgefaßt, daß nur die Datenbanken erfaßt werden, die ernste Mißbrauchsmöglichkeiten bieten?

### I. Allgemeines

Der Einsatz der elektronischen Datenverarbeitung hat in den vergangenen Jahren in steigendem Umfang zugenommen. Die Datenverarbeitung hat sich in Forschung, Wirtschaft und Verwaltung als hervorragendes Hilfsmittel zur rationellen Erledigung vieler Aufgaben erwiesen. Sie eröffnet zudem die Möglichkeit, leichtere und schnellere Informationssammlung zu betreiben und dadurch Planungs- und Entscheidungshilfen zu gewinnen, die bisher so kurzfristig in diesem Umfang nicht bereitgestellt werden konnten. Durch die Automation ist die Gefahr einer Beeinträchtigung oder Verletzung der Privatsphäre in verstärktem Maße in den Vordergrund getreten, da es mit Hilfe der elektronischen Datenverarbeitung möglich ist, integrierte Informationssysteme zu schaffen, und damit Daten über Einzelpersonen aus verschiedensten Bereichen der Verwaltung und Wirtschaft zentral zusammenzuführen. Die für die bisherigen Arbeitsmethoden bestehenden Schutz- und Geheimhaltungsvorschriften reichen für die neuen Verfahren und Techniken nicht aus.

Nachteiligen Auswirkungen des Einsatzes der elektronischen Datenverarbeitung vorzubeugen, ist Ziel

dieses Gesetzes. Es ist ein gleichermaßen verfassungsrechtliches wie gesellschaftspolitisches Gebot, ausreichende Sicherungsmaßnahmen zum Schutz der Privatsphäre des einzelnen zu treffen.

Der Datenschutz rückte erstmals in das Rampenlicht der öffentlichen Diskussion, als die amerikanische Bundesregierung plante, die in den einzelnen Bundesbehörden gespeicherten Daten in einer zentralen statistischen Datenbank zusammenzuführen (Hearings on the Computer and Invasion of Privacy before a Subcommittee of the House-Committee on Government Operations, 89th Cong. 2nd Sess. (1966); Computer Privacy, Hearings before the Subcommittee on Administrative Practice and Procedure on the Senate Committee on the Judiciary, 90th Cong. (1967/68); Privacy and the National Data Bank Concept, 35th Report to the House by the Committee on Government Operations, 90th Cong., 2nd Sess., House Report No/1842 (1969).

Die amerikanische Öffentlichkeit brachte diese Pläne vorläufig zu Fall. Der Kongreß wurde aufgefordert, eine Datenschutzgesetzgebung zu schaffen.

Die Literatur zur „Computer — Privacy“ ist inzwischen fast unübersehbar angeschwollen (vgl. z. B. Alan F. Westin, Privacy and Freedom, New York 1967, 2. Aufl. 1970; Arthur A. Miller, Personal Privacy in the Computer Age, the Challenge of a New Technology in an Information Oriented Society, 67 Mich. L. Rev. 1089 [1969]); Warner-Stone, The Data Bank Society, London 1970). Das rasante Vordringen des Computers in alle gesellschaftliche Bereiche verleiht dem Datenschutz in naher Zukunft eine dem Umweltschutz entsprechende Bedeutung (Cornelius Gallagher, Technology and Society; a conflict of Interest, Congressional Record, Vol. 115, No. 55, 91st Cong.)

Gesetzgebung zum Schutze der Privatsphäre gegenüber Computerdatenbanken ist in der sich erst entwickelnden rechtswissenschaftlichen Literatur auch in Deutschland schon mehrfach gefordert worden (vgl. Kamlah, Right of Privacy, Köln 1969; ders. DOV 70, 361 ff.; Seidel, Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten, NJW 70, 1581; Simitis, Informationskrise des Rechts und Datenverarbeitung, Karlsruhe, 1970, S. 109 ff. ders. NJW 71, 680; Steinmüller, EDV und Recht, JA-Sonderheft 6, S. 86; Podlech, Verfassungsrechtliche Probleme öffentlicher Datenbanken, DOV 70, 473).

Obwohl der Deutsche Bundestag auf Initiative von Mitgliedern der Interparlamentarischen Arbeitsgemeinschaft die Bundesregierung durch seine Entschließung vom 28. März 1969 (Umdruck 631) aufforderte, dem Schutz der Privatsphäre besondere Aufmerksamkeit zu widmen, hielt die Bundesregierung noch im 2. Bericht zur Datenverarbeitung in der Bundesverwaltung (Drucksache VI/648) ein Da-

tenschutzgesetz nicht für erforderlich. Inzwischen hat jedoch auch sie die Vorlage eines Datenschutzgesetzes angekündigt (Antwort der Bundesregierung auf die Kleine Anfrage der Abg. Hirsch, Dichgans, Mertens und Genossen vom 5. Oktober 1970, Drucksache VI/1223, S. 3).

Die verschiedenen Datenschutzgesetze und Entwürfe der Länder befassen sich — entsprechend der begrenzten Gesetzgebungszuständigkeit — lediglich mit der Regelung der Verhältnisse der Landesstaatlichen Datenbanken und verdeutlichen damit die Notwendigkeit einer den übrigen Bereich umgreifenden bundesgesetzlichen Initiative. (Vgl. Hess. Datenschutzgesetz vom 7. Oktober 1970, HessGVBl. 70, 625; BayEDVG vom 12. Oktober 1970, BayGVBl. 70, 457; § 13 Gesetz über die Datenzentrale Baden-Württemberg vom 17. November 1970, BWGVBl. 70, 492; dem Landtag von Rheinland-Pfalz liegt ein Entwurf der Fraktion der CDU vor, der dem Hess. Datenschutzgesetz ähnelt.)

Die Gesetzgebungskompetenz des Bundes deckt das zu regelnde Gebiet nicht vollständig ab, wie auch die Bundesregierung auf die Anfrage der Abg. Hirsch, Dichgans, Mertens und Genossen (Drucksache VI/1223) geantwortet hat. Dementsprechend versucht der vorliegende Entwurf die vorhandenen Kompetenzen des Bundes auszufüllen. Das übrige muß dem jeweiligen Landesgesetzgeber überlassen bleiben. Der Entschluß, ein Gesetz zum Schutz der Privatsphäre vor mißbräuchlicher Handhabung von Datenbanken zu schaffen, wurde in einer Sondervollversammlung der Interparlamentarischen Arbeitsgemeinschaft im Februar 1969 gefaßt. Der vorliegende Entwurf ist das Ergebnis der intensiven Diskussion und Beratungen, die seither in der Kommission für Fragen der Elektronischen Datenverarbeitung geführt wurde.

Der Gesetzentwurf enthält sämtliche im internationalen Stand der Rechtswissenschaft und Datenschutzgesetzgebung herausgebildeten Forderungen bzw. Regelungen:

1. Die Einführung eines Datenbankregisters mit einer damit verbundenen Anmeldepflicht (§§ 5, 6, 13, 14 sowie § 18 ff.).
2. Die Einführung eines Datenprotokolls (§§ 7, 15).
3. Ein Recht auf Dateneinsicht bzw. -auskunft (§§ 9, 17).
4. Ein Berichtigungs-, Lösungs- und Fortschreibungsanspruch gegenüber Falschinformationen bzw. widerrechtlichen gespeicherten Informationen (§ 3).
5. Das Verbot eines beliebigen Datenaustausches durch Pränormierung der Datenabfrage (§ 8 Abs. 1 und 2, § 16). Ausschluß des Datenverbundes im Wege der Amtshilfe (§ 8 Abs. 2).
6. Die bedingte Einbeziehung von statistischen Datenbanken (Umkehrschluß aus § 4 Abs. 1).
7. Die Verankerung eines Schadensersatzanspruchs (§ 3 Abs. 3).
8. Die Sicherung des Datenschutzes (§ 2, §§ 24 ff.).

9. Die Einbeziehung herkömmlicher Datenbanken ohne EDV, z. B. Ladendiebskarteien (§ 1).

## II. Zu den einzelnen Vorschriften

### 1. ABSCHNITT

#### Zu § 1 (Bereich des Datenschutzes)

Diese Vorschrift wurde dem Hessischen Datenschutzgesetz entnommen. Der Bereich des Datenschutzes wurde jedoch erweitert. Auch herkömmliche Unterlagen unterfallen dem Datenschutz.

#### Zu § 2 (Inhalt des Datenschutzes)

Auch diese Vorschrift wurde in Anlehnung an das Hessische Datenschutzgesetz formuliert.

#### Zu § 3 (Anspruch auf Datenschutz)

Diese Vorschrift stellt sozusagen die Magna Charta der Rechte des Betroffenen dar: Einsichtsrecht, Berichtigungsrecht.

#### Zu Absatz 1

Ohne das allgemeine Einsichtsrecht des Betroffenen bezüglich der ihn betreffenden Daten ist ein Datenschutzgesetz ein Speer ohne Spitze. Die Beschränkungen eines Einsichtsrechts müssen in Gesetzen enthalten sein. Schon nach der gegenwärtigen Rechtslage ist das Einsichtsrecht ausgeschlossen

1. in bestimmten Fällen der Strafprozeßordnung (StPO Ermittlungsakten) oder beschränkt (Strafakten: Einsicht nur durch den Verteidiger),
2. nach § 40 Bundeszentralregistergesetz (BZRG),
3. nach Artikel 10 Abs. 3 GG und nach dem Gesetz zu Artikel 10 GG, das nun vom Bundesverfassungsgericht für verfassungsmäßig erklärt wurde,
4. nach § 9 Abs. 5 dieses Gesetzentwurfs,
5. nach § 4 Abs. 1, letzter Satz dieses Gesetzentwurfs.

#### Zu Absatz 2

Der Absatz 2 enthält den Anspruch auf Berichtigung, der ohne Einschränkungen zu gewähren ist. Niemand kann ein Interesse daran haben, daß falsche Informationen über den Betroffenen irgendwo gespeichert sind. Der Berichtigungsanspruch umfaßt auch das Recht, Datenangaben zu erweitern, um Mißverständnissen vorzubeugen. Die Datenbank kann daher verpflichtet sein, in Einzelfällen auch Gegendarstellungen des Betroffenen in ihre Datensammlung aufzunehmen.

Der Absatz 2 enthält ferner den Anspruch auf Beseitigung. Das Bundesverfassungsgesetz (Mikrozensusurteil, BVerfGE 27,1) stellt fest, daß selbst das Eindringen in persönliche Daten ein Eingriff in die Privatsphäre sein kann. Erfolgt ein solches Eindringen ohne Rechtsgrundlage, so muß der Bürger das Recht haben, Beseitigung zu verlangen.

*Zu Absatz 3*

Da die widerrechtliche Speicherung von Daten sowie die Entstellung von Daten ein Eingriff in das Persönlichkeitsrecht darstellt (vgl. Kamlah, Right of Privacy, Köln, 1969, S. 100., 143 ff.) muß dem Betroffenen auch ein Schadensersatzanspruch zustehen, wenn seine Rechte verletzt werden. Selbstverständlich erstreckt sich ein solcher Schadensersatzanspruch auch auf den Ersatz des immateriellen Schadens, der in solchen Fällen der Verletzung des Persönlichkeitsrechts stets im Vordergrund stehen wird. Die von der Rechtsprechung hierzu entwickelten Grundsätze sind anzuwenden. Eine Ergänzung des Schadensersatzanspruchs ist der Widerrufsanspruch. Der Widerruf kann auch dadurch erfolgen, daß die Datenbank verpflichtet wird, an Empfänger der falschen Daten eine Widerrufsmitteilung zu versenden. Vergleiche hierzu § 21 Abs. 4 dieses Entwurfs. Bei § 3 Abs. 3 ist ausgedrückt, daß der Betroffene natürlich auch einen Anspruch darauf hat, daß die Datenbank eine solche Mitteilung versendet.

## 2. ABSCHNITT

Entsprechend dem Wunsche der Kommission wurden die öffentlichen Datenbanken und die privaten Datenbanken in getrennten Abschnitten behandelt.

**Zu § 4 (Geltungsbereich)***Zu Absatz 1*

Die Abgrenzung des Geltungsbereichs bereitet besondere Schwierigkeiten. Datenbanken können nicht nur Computer-Datenbanken sein. Es muß vermieden werden, daß die Adressaten dieses Gesetzes den Vorschriften ausweichen, indem sie ihre Datenbestände nicht auf einem Computer speichern, sondern in konventioneller Form. Automationsfeindliche Auswirkungen dieses Gesetzes sind zu vermeiden. Es kommt lediglich darauf an, den notwendigen Schutz der Privatsphäre zu gewährleisten. Bei der Abgrenzung des Geltungsbereichs wurde ein in der Kommission entwickelter Vorschlag angenommen, der die Zweckbestimmung einer Datenbank hervorhebt, die auf Datenaustausch gerichtet ist. Dieser Abgrenzungsvorschlag wird durch Äußerungen in der Literatur bestätigt (vgl. Simitis, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 71, S. 680).

In § 4 Abs. 1 Satz 2 wurden die Nachrichtendienste vom Geltungsbereich dieses Gesetzes ausgenommen; für diese Datenbanken gilt jedoch der Absatz 4, worauf besonders hinzuweisen ist (vgl. unten).

*Zu Absatz 2*

Um den Geltungsbereich des Gesetzes nicht zu weit auszudehnen, sind Personalakten ausgenommen worden. Eine den Zielsetzungen dieses Gesetzes entsprechende Regelung erfolgt besser im Bundesbeamtenrechtsrahmengesetz, dem Bundesbeamtengesetz und in den beamtenrechtlichen Neben-

gesetzen. Da das Einsichtsrecht in Personalakten im Bereich des Beamtenrechts schon gewährleistet ist, wäre lediglich eine bessere Durchführung des Berichtigungsanspruchs des Beamten sicherzustellen. Die Rechtsprechung des Bundesverwaltungsgerichts zu diesem Problem kämpft noch mit dem ominösen Prinzip der Vollständigkeit in Personalakten, das einem Berichtigungsanspruch von Beamten häufig entgegengehalten wird. Die Beamtengesetze müßten auch die in §§ 8 und 9 dieses Gesetzes gewährten Rechte für die Beamten sicherstellen. Dieses Gesetz soll jedoch auch für Personalakten gelten, wenn diese der Gefahr ausgesetzt sind, in einem Informationssystem auch von unbefugten Dritten eingesehen zu werden.

*Zu Absatz 3*

An die Öffentlichkeit gerichtete Äußerungen von Politikern sind ohnehin nicht privat, d. h. unterfallen nicht dem Persönlichkeitsschutz, wenn sie berichtet werden. Daher diese Ausnahme im Interesse des geplanten politischen Informationssystems des Bundestages und der Presse.

Natürlich wird es häufiger vorkommen als bisher, daß Abgeordnete mit früheren Äußerungen konfrontiert werden, die in einem Computer leichter aufzufinden sind, als bis heute in den Protokollen des Bundestages. Vielleicht wäre hier zum Schutze eines anzuerkennenden Sinneswandels eine Einschränkung zu erwägen.

*Zu Absatz 4*

Das Bundeszentralregistergesetz vom 18. März 1971 (BGBl. 71 S. 243) betrifft eine der bedeutensten Datenbanken des Bundes. Die Rückwirkungen dieses Gesetzes auf das BZRG werden zunächst bewußt außer acht gelassen. Zu einem späteren Zeitpunkt wird es jedoch notwendig werden, das BZRG auf die Vereinbarkeit mit dem Ziel dieses Gesetzes hin zu prüfen.

*Zu Absatz 5*

Nach Absatz 1 unterfallen Datenbanken nicht diesem Gesetz, die nicht dem Datenaustausch dienen. Dies soll jedoch nicht bedeuten, daß in einer solchen Datenbank gespeicherte Daten rechtlich freigestellt sind. Im Rahmen der mit diesem Gesetz angestrebten Verrechtlichung der Datenverwaltung ist es daher notwendig, auch auf solche Datenbanken wenigstens § 8 Abs. 1 und 2 anzuwenden. Dies gilt auch für die in § 4 Abs. 1 Satz 2 genannten Nachrichtendienste. Es ist nicht zu befürchten, daß EDV-Datenbanken den Bestimmungen dieses Gesetzes dadurch auszuweichen versuchen, daß sie die Zweckbestimmung nach § 4 Abs. 1 ablehnen. § 4 Abs. 4 Satz 2 würde dann nämlich bestimmen, daß über jede aus der Datenbank an Dritte erteilte Auskunft der Betroffene zu unterrichten ist. Die Datenbank dagegen, die dem Geltungsbereich des Abschnittes unterfällt, kann sich mit den Erfordernissen des § 7 begnügen. Sie muß nur dann dem Betroffenen Auskunft über erteilte Auskünfte erteilen, wenn dieser es nach § 9 verlangt.

Von der Benachrichtigungspflicht bei erteilter Auskunft mußten jedoch wiederum die Nachrichten-

dienste ausgenommen werden. Eine Verrechtlichung der Datenverwaltung dieser Dienste kann nur durch spezielle Gesetze erreicht werden. Im übrigen ist mit Alan F. Westin darauf hinzuweisen, daß Nachrichtendienste in erster Linie politisch zu kontrollieren sind (Westin, *Science, Privacy and Freedom Issues and Proposals for the 1970's* 66 Col.L.Rev. 1227 [1966]).

#### Zu § 5 (Anmeldepflicht)

Der Gesetzentwurf folgt dem Vorschlag, der im britischen Data Surveillance Bill (1969, Baker, Windlesham) gemacht wurde. Das britische Data Surveillance Bill, daß sowohl in House of Commons als auch dem House of Lords vorgelegen hat, ist dort nicht erlassen worden. Dennoch gilt es als eine Pioniertat, deren Bedeutung von der einschlägigen Literatur anerkannt wird. (Niblett, *Digital Information and the Privacy Problem*, OECD-Papier — unveröffentlicht p. 31; Malcolm Warner, Michael Stone, *the Data Bank Society*, London 1970, S. 194).

Die Anmeldepflicht soll nicht davon abhängen, ob eine bestimmte Art von Computer benutzt wird, da die technische Entwicklung vollkommen offen ist. Die Computertechnik ist allenfalls der Anlaß, nicht jedoch der tiefere Grund für den Erlaß eines solchen Gesetzes. Selbst wenn es Computer noch nicht gäbe, würde man sich nach Ansicht von Westin heute über solche Gesetze Gedanken machen (Westin, *political and legal dimensions of computer Data-Banks*, Vortrag, Workshop on the Data Bank Society, London 1970).

Durch den Absatz 3 wird der Aufsichtsbehörde ermöglicht, auf geeignete maschinentechnische Vorkehrungen zum Schutze der Privatsphäre hinzuwirken. Die technischen Schutzmöglichkeiten sind einerseits sehr vielfältig, andererseits auch unvollkommen. Sie gesetzlich zu regeln, wäre unmöglich. Der technische Fortschritt würde viele Regelungen eines Gesetzes sehr schnell überholen. Daher § 28 Abs. 1 Nr. 1 dieses Gesetzentwurfs.

#### Zu § 6 (Eintragung in das Register)

##### Zu Absatz 1 Nr. 5

Nicht die zum Anmeldezeitpunkt beschäftigten Bediensteten sind mit ihren Namen zu melden, sondern lediglich die abstrakte Bezeichnung ihrer Dienststellung. Die Anmeldung der Namen jedes derzeit bei einer Datenbank Beschäftigten würde zu weit gehen, sie würde einen umfangreichen und unzumutbaren Änderungsdienst verursachen.

#### Zu § 7 (Protokoll)

Wenn der Betroffene nicht die Kontrolle über seine Daten verlieren soll, ist in einem Protokoll festzuhalten, welche Stellen oder Personen außer der einspeichernden Stelle Zugang haben. Es muß sich dabei nicht um ein selbständiges, körperlich greifbares Protokoll handeln. Den Datenbankunterneh-

mern ist es überlassen, wie sie das Protokoll in ihrer Datenbank verwirklichen.

Die Einrichtung eines Protokolls ist für maschinentechnische oder elektronische Datenbanken sowohl in den englischen als auch in anderen Gesetzesvorschlägen gefordert worden (Data Surveillance Bill 1969, § 4; Bill 182 (Mr. Reid, Ontario, Canada), § 5; Assembly Bill, No. 1982, (1970). Zur Änderung des California Government Code § 6253 [c]).

Auch die Bundesrepublik hat im 2. EDV-Bericht für den Bereich des Meldewesens eine Protokollpflicht gefordert, die auf die selbsttätige Datenübermittlung beschränkt ist (Drucksache VI/648, S. 18).

Ist der Betroffene bei den gespeicherten Daten oder bei Auskünften nicht identifizierbar, so liegt kein Eingriff in sein Persönlichkeitsrecht vor (Kamlah, a. a. O., S. 155 ff.). Es ist daher angezeigt, für diese Fälle eine Ausnahme zu machen.

#### Zu § 8 (Auskunftsberichtigung)

§ 8 Abs. 1 ist die Kernvorschrift des Gesetzes. Sie besagt, daß die Datenverwaltung zu verrechtlichen ist. Mit dieser Vorschrift folgt der Entwurf den im Mikrozenssurteil des Bundesverfassungsgerichts aufgestellten Forderungen (BVerfGE 27,1). Für die Datenverwaltung gilt danach der Vorbehalt des Gesetzes unbeschränkt. Dies ist vom Bundesverfassungsgericht im Scheidungsaktenurteil (BVerfGE 27, 344) noch einmal präzisiert worden. Die Interpretation beider Urteile ist noch streitig (vgl. Kamlah, *Datenüberwachung und Bundesverfassungsgericht DOV 70, 361 ff.*; Seidel, *Persönlichkeitsrechtliche Probleme der Elektronischen Speicherung privater Daten*, NJW 70, 1581 ff.; Simitis, a. a. O., NJW 71, 673).

Der große Schritt zur Erweiterung des Rechtsstaates, den das Bundesverfassungsgericht getan hat, wirft natürlich auch Probleme auf, die besonders die Verwaltung treffen. Viele Vertreter der Verwaltung fordern daher, das Erfordernis einer Rechtsgrundlage für die Datenverwaltung weit zu fassen, insbesondere die Verwaltung für ermächtigt anzusehen, die Daten zu ermitteln, die zur Aufgabenerfüllung notwendig sind. Als Schranke für die Ermittlungsbefugnis sollte das Verhältnismäßigkeitsprinzip herangezogen werden.

Dieser Forderung kann jedoch nicht entsprochen werden. In einer Zeit, in der die Leistungsverwaltung die Eingriffsverwaltung zunehmend verdrängt, ist ein Schluß von der Aufgabe auf die Befugnis, Daten zu ermitteln, nicht mehr zulässig. Würde man der Verwaltung die Befugnis einräumen, allgemein unter den Schranken des Verhältnismäßigkeitsprinzips alle verwaltungsrelevanten Daten zu ermitteln und auszutauschen, so würde jeder Beamte selbst zu entscheiden haben, ob er auf vorhandene Datenbestände im Einzelfall zugreifen darf oder nicht. Dies wäre nicht mehr tragbar, sobald der Zugriff auf Daten eines Informationssystems ohne Einschaltung einer anderen Person möglich wird, die an der

Quellenbehörde über die Abgabe der Daten an die Anfragende Behörde zu entscheiden hat.

Auch gibt es keinen allgemeinen Rechtsfertigungsgrund des überwiegenden Interesses des Staates, der überwiegenden Staatsraison. Eingriffe des Bürgers müssen gesetzlich vorher bestimmt sein.

Die Verrechtlichung der Datenverwaltung soll natürlich nur private Daten betreffen. Es ist auch nicht beabsichtigt, mit diesem Gesetz den Informationsanspruch der Öffentlichkeit insbesondere auch des Parlaments, der in Artikel 5 GG verankert ist, einzuschränken. Artikel 5 GG und das allgemeine Persönlichkeitsrecht schließen sich nicht gegenseitig aus, sie beschränken nur einander. Soweit Artikel 5 GG eine öffentliche Berichterstattung über Personen zuläßt, kann auch Auskunft gegeben werden. Die Beweislast für das Vorliegen des Rechtsfertigungsgrundes nach Artikel 5 GG trifft natürlich die auskunftserteilende Behörde.

#### Zu Absatz 2

Hier wird der weit verbreiteten Auffassung entgegengetreten, daß unter dem Motto der Amtshilfe Behörden untereinander Daten austauschen dürften, auch wenn es sich um personenbezogene Daten handelt. Diese Auffassung ist unter zunehmenden rechtsstaatlichen Erfordernissen nicht mehr aufrechterhalten. Es mehren sich die Stimmen, die in der Datenermittlung und Datenweitergabe einen Eingriff gegenüber dem Bürger sehen. Die Amtshilfe ist lediglich eine Rechtsgrundlage gegenüber der angegangenen Behörde, Hilfe zu leisten. Sie deckt nicht den in der Amtshilfe möglicherweise liegenden Eingriff gegenüber dem Bürger.

Die Kommission hat durch zwei Gutachten feststellen lassen, daß die Vorschrift des Absatzes 2 nicht gegen Artikel 35 GG verstößt.

#### Zu Absatz 3

Hier wird das an sich schon nach § 12 des Gesetzes über die Statistik für Bundeszwecke (BGBl. 1953, S. 1314) geltende Statistikgeheimnis wiederholt. Nach § 29 des Entwurfs wird jedoch der Inhalt des § 12 Statistikgesetz insoweit geändert, als Einzelangaben aus dem Urmaterial von Statistiken überhaupt nicht mehr zulässig sein sollen. In einer zukünftigen statistischen Datenbank wird es kaum möglich sein, die nach dem jetzigen § 12 Statistikgesetz noch zulässige Einzelauskunft entsprechend den gesetzlichen Voraussetzungen zu erteilen. Die Möglichkeit von Einzelauskünften aus statistischen Datenbanken stellt eine ernste Bedrohung der Privatsphäre dar. Die Diskussion in den Vereinigten Staaten hat gezeigt, daß schon eine statistische Datenbank als solche eine Gefährdung der Privatsphäre sein kann. Daher ist es unumgänglich, Einzelauskünfte aus einer statistischen Datenbank generell zu unterbringen (Privacy and the National Data Bank Concept, 35th Report to the House by the Committee on Government Operations, 90th Cong. 2nd Sess. House Report No. 1842).

### Zu § 9 (Recht auf Auskunft)

#### Zu Absatz 1

Der Betroffene muß erfahren, wo Daten über ihn gespeichert sind. Andernfalls kann er seine Rechte nicht wahrnehmen. Daher hat die Datenbank dem Betroffenen eine Eröffnungsmitteilung zu übersenden. Ausgenommen sind Fälle, in denen der Betroffene offenbar mit der Speicherung von Daten rechnen muß.

#### Zu Absatz 2

Hier wird die Durchführung des Einsichtsrechts geregelt.

#### Zu Absatz 3

Nach dieser Vorschrift kann der Betroffene einen Auszug aus dem Protokoll verlangen, in dem die Verwendung seiner Daten festgehalten ist. Wenn er nach Erhalt dieses Protokollauszugs feststellt, daß die Auskunftserteilung in einem Einzelfalle bedenklich war, kann er eine Kopie dieser Auskunft verlangen.

#### Zu Absatz 4

Die Behörden sollen an den Gebühren natürlich nichts verdienen. Die Gebühren sind daher nach dem tatsächlichen Aufwand zu bemessen. Es steht zur Debatte, den Absatz 4 bei der Endredaktion in den Bereich der Kostengesetze zu verweisen.

### Zu § 10 (Verschwiegenheitspflicht)

Die Verschwiegenheitspflicht des Personals bei Datenbanken ist eine selbstverständliche Absicherung des Datenschutzes. Vergleiche auch Hessisches Datenschutzgesetz, Artikel 15 Bay EDVG.

### Zu § 11 (Datenaustausch mit Datenbanken nach Landesrecht)

Durch § 11 wird dem Bund der Anschluß an Landesinformationssystemen verboten, gegenüber denen die Bürger nicht in gleicher Weise, wie in diesem Gesetz vorgesehen, geschützt sind. Ein bundesweites Informationssystem ist somit nur dann möglich, wenn sich die zuständigen Landesgesetzgeber dazu entschließen, entsprechende Datenschutzgesetze zu erlassen. Der Bund hat keine andere Möglichkeit, auf die Landesgesetzgeber einzuwirken (Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Hirsch, Dighans, Mertens und Genossen, durch den Bundesminister des Innern vom 5. Oktober 1970, Drucksache VI/1223).

## 3. ABSCHNITT

### Zu § 12 (Geltungsbereich)

Es wurde in Anlehnung an die Geltungsbereichsabgrenzung des § 4 Abs. 1 Satz 1 eine Bestimmung des Geltungsbereichs versucht, die auf die privaten Datenbanken paßt. Die privaten Datenbanken im

einzelnen aufzuzählen, die man mit dem Gesetz besonders ansprechen möchte, wurde bisher nicht für möglich gehalten. Unter das Gesetz sollen unter allen Umständen fallen: Das Auskunftsgewerbe einschließlich der sogenannten Schufa, die Versicherungen, insbesondere die Kranken- und Lebensversicherungen, die Kreditinstitute, soweit sie eigene Kreditauskunftssysteme oder Kreditdatenaustausch betreiben, private sonstige Auskunfteien und Detekteien, medizinische Datenbanken, soweit sie Patientendaten speichern, insbesondere auch die sogenannten ärztlichen Verrechnungsstellen, Adressenverlage. Diese Aufzählung ist gewiß unvollständig.

Auch hier wurden Personalakten ausgenommen, da so gut wie selbstverständlich ist, daß jeder Gewerbebetrieb größerer Ordnung über seine Arbeitnehmer Personalakten führt. Soweit solche Personalakten nicht in Auskunftssysteme eingegliedert sind, empfiehlt es sich nicht, sie diesem Gesetz zu unterstellen. Es ist jedoch notwendig, für die Personalakten im Rahmen des BGB den Gedanken dieses Gesetzes entsprechende Regelungen zu entwerfen. Vorschläge dieser Art wurden bereits im Ausschuß erörtert. Sie wurden zurückgestellt, da in den jetzigen Beratungen zum neuen Betriebsverfassungsrecht bereits entsprechende Vorschläge in Beratung sind. Es wird zu bedenken gegeben, ob es nicht vorteilhaft ist, schon auf diese Beratungen einzuwirken. Der § 12 Abs. 3 soll der Aufsichtsbehörde ermöglichen, mit einem feststellenden Verwaltungsakt zu erreichen, daß einzelne private Datenbanken die Vorschriften dieses Gesetzes beachten.

§ 12 Abs. 5 entspricht seinem Sinne nach dem § 4 Abs. 5. Er soll verhindern, daß Unternehmer mit großem Datenanfall den Verfahrensvorschriften des Gesetzes ausweichen können. Um die Benachrichtigungspflicht des Absatzes 5 Satz 2 zu vermeiden, gibt es für die Unternehmer von Datenbanken nur einen Weg: Sich dem Geltungsbereich des Gesetzes unterstellen.

Keinesfalls sollen Unternehmen von der Verpflichtung, das Persönlichkeitsrecht der Betroffenen zu achten, frei sein, wenn sie den Verfahrensvorschriften des Gesetzes und den damit verbundenen Pflichten nicht unterliegen.

#### Zu § 13 (Anmeldepflicht)

Bei Absatz 4 wurde eine gegenüber § 5 Abs. 3 schärfere Formulierung für notwendig erachtet.

#### Zu § 14 (Eintragung in das Register)

Bei § 14 Abs. 1 Ziffer 6 wurde versucht, entsprechend der Formulierung in § 6 Abs. 1 Ziffer 5 zu vermeiden, daß im Anmeldezeitpunkt konkret beschäftigte Personen genannt werden müssen. Es genügt die Angabe der Stellung der Personen, die in eigener Verantwortung Daten einspeichern und entnehmen dürfen. Unter Stellung ist die Funktion im Betrieb zu verstehen.

#### Zu § 15 (Protokoll)

Hier war ein Generalverweis auf § 7 ausreichend.

Es wird darauf hingewiesen, daß es für die Kreditauskunfteien einmal Verordnungen gegeben hat, die die Führung eines Protokolls in Form eines Auskunftsbuches vorschreiben. Diese Verordnungen haben auch heute noch formell Gültigkeit. Sie werden dem Vernehen nach jedoch nicht angewendet. Im Zeitalter der kommenden Computer-Auskunft wird jedoch die Führung des Protokolls technisch leichter möglich sein als bisher.

In diesem Zusammenhang ist von Interesse, daß sich die amerikanischen Kreditauskunfteien nicht grundsätzlich gegen die Protokollierungspflicht gestraut haben. (Vgl. Fair Credit Reporting Act, S. 823 (1969), der von den Auskunfteien unterstützt wurde, und Hearings on Fair Credit Reporting zu H. R. 16340, Sullivan-Committee, 1970, Statement of Mr. Spafford (ACB), p. 145, Jordan (TRW-Credit Data), p. 1601; nun auch geltendes Recht: 15 U.S.C. § 1681 g (3) [1971].)

#### Zu § 16 (Auskunftsberechtigung)

Was für den Staat gilt, gilt auch für die private Wirtschaft. Das Eindringen in und die Indiskretion von personenbezogenen Daten ist ein Eingriff in das Persönlichkeitsrecht. Hier ist jedoch lediglich der auch im Zivilrecht anerkannte Rechtfertigungsgrund des überwiegenden berechtigten Interesses anzuerkennen. Dieser Rechtfertigungsgrund folgt aus dem Gedanken des § 193 StGB. Auf ihn stützen sich auch bisher die Kreditauskunfteien (vgl. Jäger, Wahrnehmung berechtigter Interessen durch Auskunfteien, NJW 56, 1224).

Im amerikanischen Fair Credit Reporting Act, das dem Vernehen nach seit Mitte April in Kraft ist (Congressional Record, H 3108, Apr. 27, 1971; 15 U.S.C. § 1681 [1971]) hat der Gesetzgeber das berechnete Interesse der Kreditwirtschaft an Kreditauskünften sogar ausdrücklich anerkannt. Dies empfiehlt sich jedoch nicht im Rahmen eines umfassender geltenden Gesetzes, wie es mit diesem Entwurf vorgeschlagen wird.

#### Zu Absatz 2

Der Absatz 2 soll klarstellen, daß die Vereinsform nicht geeignet ist, den Absatz 1 zu umgehen. Die Vereine der Auskunfteien z. B. „Bürger“ oder „Creditreform“ oder bekannte Detekteien, sind in der Form des bürgerlich rechtlichen Vereins, des wirtschaftlichen Vereins organisiert. Diese Form wurde bei der Gründung der Gewerbe gewählt, um Bedenken zu begegnen, die daraus hergeleitet werden konnten, daß diese Institutionen ständig private Tatsachen über Dritte, die unter Umständen auch ehrenrührig sein konnten, an Dritte weitergeben. Die Formulierung des Absatzes 2 wurde so gehalten, daß auch andere Verbände darunter fallen, deren Zusammenschluß u. a. auch dazu dient, den Datenaustausch unter den Mitgliedern und zwischen den Mitgliedern und dem Verband zu erleichtern.

**Zu § 17** (Recht auf Auskunft)

Auch hier konnte weitgehend auf § 9 verwiesen werden. Im Absatz 2 soll ausgedrückt werden, daß eine Auskunft, deren Gewerbe es natürlich ist, Auskünfte zu erteilen, gerade an der Auskunft gemäß § 17 nichts verdienen soll.

Eine Kreditauskunft wird dem Betroffenen eine Kreditauskunft nicht aushändigen können, da dieser mit der Kreditauskunft u. U. Mißbrauch treiben könnte, indem er sich in kurzer Zeit, gestützt auf die Kreditauskunft, bei mehreren Banken, einen höheren Kredit verschafft, als dieser von der Auskunft für zulässig erachtet wird. Solche und ähnliche Besonderheiten des privaten Bereichs werden bei den Ausführungsbestimmungen nach § 28 Abs. 1 Ziffer 2 zu berücksichtigen sein. Vielleicht ist im Falle der Auskünfte dem amerikanischen Vorbild zu folgen, daß der Betroffene lediglich in einer Außenstelle der Auskunft persönlich oder begleitet durch einen Beistand Einsicht nehmen darf (vgl. H. R. 16340, 91st Cong. 2nd Sess. 1970, Fair Credit Reporting Act, Sec. 31; 15 U.S.C. § 1681 h [1971]).

## 4. ABSCHNITT

**Zu § 18** (Zuständigkeit)

Aufsichtsbehörden. Hier konnte wieder eine für beide Geltungsbereiche weitgehend einheitliche Formulierung gewählt werden. Notwendige Abweichungen sind in den einzelnen Vorschriften hervorgehoben.

Der in dem ersten Vorentwurf von 1969 enthaltene Ombudsman in Form des Bundesamtes für die Überwachung von Datenbanken, wurde im zweiten Vorentwurf aufgegeben. Die Aufsicht über die Datenbanken wurde dem Bereich des Bundesministers . . . zugeordnet. Es soll damit die Schaffung eines unserem Verfassungssystem fremden Ombudsmans vermieden werden.

**Zu § 19** (Register)

Da das Datenbankregister öffentlich ist, kann das Publikum feststellen, bei welchen Stellen möglicherweise Daten über Personen gespeichert sind. Das bewirkt eine zusätzliche Kontrolle.

**Zu § 20** (Aufgaben, Tätigkeitsbericht)

In § 20 Abs. 2 kommt zum Ausdruck, daß natürlich eine beim Bundesministerium . . . liegende Aufsichtsbehörde nicht in andere Ressorts hineinreden kann. Das Ressortprinzip ist soweit wie möglich zu wahren. Die Aufsichtsbehörde ist daher gegenüber anderen Bundesbehörden darauf beschränkt, die zuständige Fachaufsichtsbehörde zu alarmieren und die Verbesserung von Zuständen und die Abstellung von Gesetzesverletzungen anzuregen. Kommen die anderen Behörden solchen Aufforderungen nicht nach, so kann natürlich ein solcher Tatbestand in den nach § 20 Abs. 3 zu erstellenden jährlichen Tätigkeitsbericht eingehen.

Der Tätigkeitsbericht der Aufsichtsbehörde soll dem Bundestag ermöglichen, dieses Gesetz neuen Entwicklungen schnell und rechtzeitig anzupassen. Es kann nicht erwartet werden, daß dieses Gesetz schon eine endgültige Regelung der Datenverwaltung erreichen wird.

**§ 21** (Befugnisse der Aufsichtsbehörde)

Die Absätze 1 bis 3 übertragen der Aufsichtsbehörde bzw. ihren Bediensteten, die notwendigen Untersuchungsbefugnisse.

*Zu Absatz 4*

Die Geltung des Absatzes 4 ist auf private Datenbanken beschränkt, da der Aufsichtsbehörde gegenüber öffentlichen Datenbanken nicht so weite Befugnisse eingeräumt werden können.

Der Rechtsschutz des Betroffenen soll nicht seiner eigenen Initiative überlassen bleiben. Die Aufsichtsbehörde soll auch von Amts wegen einschreiten können. Maßstab für das Einschreiten sind jedoch die Rechte des Betroffenen.

§ 21 Abs. 4 ist somit eine Ergänzung des § 3.

Erläßt die Aufsichtsbehörde eine Anordnung nach Absatz 4, so liegt ein anfechtbarer Verwaltungsakt vor. Nach § 42 VWGO wäre das Verwaltungsgericht zur Entscheidung über eine Anfechtungsklage der Datenbank berufen. Die Beiladung des Betroffenen ist notwendig, wenn es um die Löschung bestimmter Daten geht. Ist ein Rechtsstreit des Betroffenen gegen die Datenbank wegen eines Anspruchs nach § 3 beim Landgericht anhängig, oder wird er anhängig gemacht, so empfiehlt es sich, die Entscheidung des Verwaltungsgerichts auszusetzen, bis die zivilrechtliche Vorfrage entschieden ist, um inhaltlich widersprechende Urteile zu vermeiden.

*Zu Absatz 5*

Gegenüber öffentlichen Datenbanken ist die Aufsichtsbehörde auf Anregungen beschränkt.

*Zu Absatz 7*

Als letzter Absatz war in der entsprechenden Vorschrift des Vorentwurfs folgende Vorschrift enthalten: Vorentwurf § 15 Abs. 7: „Die durch Auskünfte und Maßnahmen nach Absatz 1 erlangten Kenntnisse und Unterlagen dürfen nicht für ein Besteuerungsverfahren einschließlich eines Steuerstrafverfahrens verwendet werden“. Die Vorschrift war von der Redaktion gedacht als eine Verlängerung entsprechender Vorschriften aus anderen Gesetzen, z. B. § 13 des Gesetzes über die Statistik für Bundeszwecke, § 46 GWB. Die Bediensteten der Aufsichtsbehörde gelangen zu Daten, die auch nach anderen Gesetzen nicht den Steuerbehörden zur Verfügung gestellt werden dürfen. Diese Gesetze schützen scheinbar den Steuerkriminellen, haben jedoch aufgrund einer Interessenabwägung im Auge, volle Beantwortungswahrheit bei der für diese Gesetze notwendigen Daten zu erreichen, indem eine Garantie für die Nichtverwendung im Steuerverfahren gegeben wird. Wenn diese anderen Gesetze einen solchen Aus-



nahmeschutz gewähren, so muß der Bedienstete der Aufsichtsbehörde ebenfalls unter einem solchen Ausnahmeschutz stehen. Anderenfalls würde es eintreten, daß der Bedienstete der Aufsichtsbehörde, deren Zweck es gerade ist, die Privatsphäre besonders zu schützen, dazu verwendet werden kann, beim Besteuerungsverfahren ermitteln zu helfen. Demgegenüber wurde in der Kommission vorgebracht, daß nicht einzusehen sei, warum ausgerechnet der Steuerkriminelle mit dem weißen Kragen vom Gesetzgeber stets mit Glacéhandschuhen angefaßt werde.

Die Kommission beschloß mit Mehrheit, daß die Vorschrift zu streichen ist.

#### **Zu § 22 (Verwaltungsverfahren)**

##### *Zu Absätze 1 und 2*

Die Vorschrift wurde in Anlehnung an entsprechende Vorschriften aus anderen Gesetzen formuliert.

§ 22 Abs. 1 Nr. 3 entspricht z. B. einer Formulierung des § 51 GWB.

##### *Zu Absätze 3 und 4*

Der Betroffene hat stets das Recht, bei der Aufsichtsbehörde ein Einschreiten von Amts wegen anzuregen. Wird ein solches Einschreiten beantragt und ergeht von der Aufsichtsbehörde gegenüber dem Betroffenen ein ablehnender Bescheid, so ist klarzustellen, daß ein solcher Bescheid nicht vor den Verwaltungsgerichten anfechtbar sein soll, wenn es sich um eine private Datenbank handelt. Andernfalls würde eine Spaltung des Rechtsweges zu befürchten sein. Lehnt die Behörde ein Einschreiten ab, so hat der Betroffene sein Recht auf dem ihm zur Verfügung stehenden Rechtsweg zu suchen.

Es könnte noch erwogen werden, den Zivilgerichten die Entscheidung über den Verwaltungsakt zuzuweisen, durch den die Aufsichtsbehörde gegenüber einer privaten Datenbank nach Absatz 4 vorgeht.

Dies ist jedoch unzweckmäßig, da die Anordnung der Aufsichtsbehörde nach § 21 Abs. 4 nicht auf Antrag des Betroffenen ergehen muß. Sie kann auch aus Vorschriften des öffentlichen Rechts begründet sein. Dem Betroffenen steht es frei, seine Rechte nach § 3 vor den ordentlichen Gerichten geltend zu

machen. Er bedarf des Rechtsschutzes vor den VG nicht noch zusätzlich. Die Möglichkeit der Beiladung bleibt unberührt.

#### **Zu § 23 (Zwangsmittel)**

Der Aufsichtsbehörde stehen Zwangsmittel natürlich nur gegenüber privaten Datenbanken zu.

### 5. ABSCHNITT

#### **Zu § 24 (Strafbestimmungen)**

Die Strafbestimmungen sind aus sich heraus und aus dem übrigen Gesetzestext verständlich. Sie beehren die Vorschriften des Gesetzes mit Strafe. Daneben sind einige selbständige Straftatbestände aufgenommen worden, z. B. das Anzapfen von Datenleitungen, denn § 298 StGB bestraft lediglich das Anhören des gesprochenen Wortes.

#### **Zu § 25 (Ordnungswidrigkeiten)**

Diese Vorschriften sind im Zusammenhang mit den entsprechenden Vorschriften des Gesetzes verständlich.

#### **Zu § 26 (Bußgeldverfahren, Zuständigkeit)**

### 6. ABSCHNITT

#### **Zu § 28 (Ermächtigungen)**

Durch Rechtsverordnungen soll alles geregelt werden, was sich wegen des technischen Fortschritts einer gesetzlichen Regelung entzieht.

Hier ist Raum geschaffen worden, die Vorschriften des Gesetzes den Anforderungen der Technik anzupassen.

#### **Zu § 29 (Änderung des StatG)**

Diese Vorschrift wurde schon bei der Begründung des § 8 Abs. 3 mitbehandelt.