19 Seiten

Der Landesbeauftragte
für den Datenschutz
Nordrhein Westfalen

Der Landesbeauftragte für den Datenschutz NRW

Reichsstraße 43, 4000 Düsseldorf 1
Postfach 20 04 44

Tel. (0211) 38 42 40
Durchwahl 3 84 24 47
Telefax (0211) 38 42 410

An die
Präsidentin des Landtags
Nordrhein-Westfalen
Platz des Landtags 1

4000 Düsseldorf

Datum 19.01.1993
Aktenzeichen - 23.1.1 -

Betr.: Gesetz über den Verfassungsschutz in Nordrhein-Westfalen
(Verfassungsschutzgesetz Nordrhein-Westfalen - VSG NW);
hier: Gesetzentwurf der Landesregierung
- Drucksache 11/4743 vom 04.01.1993 -

Sehr geehrte Frau Präsidentin!

Für die Beratungen des vorgenannten Gesetzentwurfs übersende ich anliegende Stellungnahme mit der Bitte um Weiterleitung an die mit dem Gesetzentwurf befaßten Ausschußmitglieder.

300 Überstücke dieses Schreibens und der Anlage sind beigefügt.

Mit freundlichen Grüßen

Maier-Bode

(Maier-Bode)

**Der Landesbeauftragte
für den Datenschutz
Nordrhein-Westfalen**

Betr.: Gesetz über den Verfassungsschutz in Nordrhein-Westfalen (Verfassungsschutzgesetz Nordrhein-Westfalen - VSG NW);
hier: Gesetzentwurf der Landesregierung
- Drucksache 11/4743 vom 04.01.1993 -

Zu dem Entwurf eines Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen gebe ich aus datenschutzrechtlicher Sicht folgende Stellungnahme ab:

Bei dem vorliegenden Gesetzentwurf geht es mit besonderem Gewicht darum, einen angemessenen, den Aufgaben eines modernen, wirksamen Verfassungsschutzes Rechnung tragenden Datenschutz zu gewährleisten. Dabei ist zu bedenken, daß in diesem Bereich mit besonders sensiblen personenbezogenen Daten umgegangen wird, deren Erhebung und Speicherung sich nach der Natur der Sache weitgehend der Kenntnis des Betroffenen entzieht. Um so notwendiger ist es, Regelungen zu treffen, die den Datenschutz der Bürgerinnen und Bürger sicherstellen.

Die Landesregierung erreicht dieses gesetzte Ziel mit ihrem Entwurf nur sehr eingeschränkt.

Ich bin mir bewußt, daß Datenschutz und Verfassungsschutz in einem Spannungsverhältnis zueinander stehen und weder dem einen noch dem anderen ein absoluter Vorrang eingeräumt werden kann. Es ist Aufgabe des Gesetzgebers, die Belange des Daten-

schutzes und die des Verfassungsschutzes zu gewichten und gegeneinander abzuwägen. Eine Lösung allerdings, die der Aufgabenerfüllung des Verfassungsschutzes deutlich Vorrang vor den Belangen des Datenschutzes einräumt, entspricht nicht dem Recht auf informationelle Selbstbestimmung und vernachlässigt die Anforderungen, die das Bundesverfassungsgericht zur Wahrung dieses Grundrechts aufgestellt hat. Im Rechtsstaat darf nicht jedes Mittel eingesetzt werden, das zur Erfüllung der behördlichen Aufgaben dienen kann.

Es ist nicht zu verkennen, daß der Entwurf des Verfassungsschutzgesetzes Nordrhein-Westfalen sich eng an das Bundesverfassungsschutzgesetz anlehnt. Insoweit wurden jedoch auch dessen Mängel in datenschutzrechtlicher Hinsicht übernommen.

Es muß festgestellt werden, daß der Gesetzentwurf in Teilen damit deutlich hinter die bisher in Nordrhein-Westfalen vorherrschende datenschutzfreundliche Praxis der Verfassungsschutzbehörde zurückgeht. Die von mir in meinem 10. Tätigkeitsbericht (S. 74) geäußerte Hoffnung, daß die dem Datenschutz gegenüber aufgeschlossene Haltung und Praxis der Verfassungsschutzbehörde auch Eingang in das zu erwartende Verfassungsschutzgesetz Nordrhein-Westfalen finden wird, erfüllt der vorliegende Entwurf nicht.

Das Land Nordrhein-Westfalen sollte die Chance nutzen, in Abkehr von einzelnen Vorschriften des Bundesverfassungsschutzgesetzes für die Bürgerinnen und Bürger Nordrhein-Westfalens neue gesetzgeberische Maßstäbe zu setzen. Dabei ist zum Teil nicht mehr zu regeln als das, was in den vergangenen Jahren bereits im Lande Nordrhein-Westfalen Praxis war. Eine wirksame Zusammenarbeit zwischen Bund und Ländern wird dadurch keineswegs beeinträchtigt, wie z. B. auch die neuen landesgesetzlichen Regelungen in Berlin und Schleswig-Holstein zeigen.

Kontinuierlich zurückgehende Zahlen von Bürgereingaben zur Datenverarbeitung des Verfassungsschutzes in Nordrhein-Westfalen signalisieren nach meiner Auffassung einen erheblichen

Vertrauensvorschuß der Bürgerinnen und Bürger dieses Landes in die korrekte und sachgerechte Verarbeitung personenbezogener Daten durch die Verfassungsschutzbehörde. Einige vorgesehene Regelungen des Entwurfs sind geeignet, diese Entwicklung umzukehren.

Mit meinen nachfolgenden Anregungen geht es mir nicht darum, die Arbeit des Verfassungsschutzes durch eine Anhäufung von Bedenken zu behindern. Vielmehr sollen damit aus meiner Sicht Verbesserungsvorschläge zu den rechtlichen Grundlagen der behördlichen Tätigkeiten auf diesem Gebiet gemacht werden, um die praktische Handhabung des Gesetzes im Rahmen der Verfassung rechtlich einwandfrei zu gewährleisten. Besonderes Anliegen sind mir dabei drei Regelungskomplexe: die Generalklausel zu den Befugnissen (§ 5), die Sicherheitsüberprüfung (§ 3 Abs. 2) und das Auskunftsrecht des Betroffenen (§ 14).

Im einzelnen nehme ich zu dem Gesetzentwurf wie folgt Stellung:

1. Zu § 3 Abs. 1:

   In Absatz 1 Nr. 3 sollten die Begriffe "Gewalt" und "auswärtige Belange" näher definiert werden, um eine normenklare Grundlage für ein Tätigwerden der Verfassungsschutzbehörde zu schaffen. § 3 Abs. 3 letzter Satz sowie die übrigen Normen, die auf Gewaltbestrebungen im Sinne des § 3 Abs. 1 verweisen, verdeutlichen die Notwendigkeit einer solchen Definition. Hierbei sollte geprüft werden, ob nicht wegen der besonderen Aufgabenzuweisungen an die Verfassungsschutzbehörde ein engerer Gewaltbegriff als der in der Rechtsprechung zu § 240 Strafgesetzbuch entwickelte festzuschreiben wäre.

   Als Beispiel einer Definition des Begriffs "auswärtige Belange" wird auf § 6 Abs. 5 des Gesetzes über den Verfassungsschutz im Lande Schleswig-Holstein (VSG SH) hingewiesen, wonach auswärtige Belange nur gefährdet werden, wenn

innerhalb des Geltungsbereichs des Grundgesetzes Gewalt ausgeübt oder durch Handlungen vorbereitet wird und diese sich gegen die politische Ordnung oder Einrichtungen anderer Staaten richten.

2. Zu § 3 Abs. 2:

Der Bereich **Sicherheitsüberprüfungen** ist im vorliegenden Entwurf nur unzureichend und damit nicht normenklar erfaßt worden. Im Hinblick auf die derzeit im Innenministerium stattfindenden Arbeiten an einem Geheimschutzgesetz wird die Streichung der Vorschrift angeregt. Ein Hinweis in § 3 Abs. 2, daß die Verfassungsschutzbehörde bei Sicherheitsüberprüfungen mitwirkt und näheres im Geheimschutzgesetz geregelt ist, würde nach meiner Auffassung genügen, wenn sichergestellt wäre, daß ein Geheimschutzgesetz gleichzeitig mit dem Verfassungsschutzgesetz in Kraft treten würde.

Zu bevorzugen wäre indes, die beabsichtigten Regelungen eines Geheimschutzgesetzes als eigenen Abschnitt in den vorliegenden Gesetzentwurf einzuarbeiten. Auf diese Weise ließe sich die Tätigkeit der Verfassungsschutzbehörde umfassend gesetzlich regeln.

3. Zu § 3 Abs. 3:

Hinsichtlich des unter Buchstaben a) bis c) definierten Begriffs "Bestrebung" ist klarzustellen, wann es sich um für ein Tätigwerden der Verfassungsschutzbehörde beachtliche Bestrebungen handelt. Ähnlich wie in § 6 Abs. 4 VSG SH ließe sich Absatz 3 dahingehend ergänzen, daß eine nach Maßgabe des VSG NW beachtliche Bestrebung eine aktiv kämpferische aggressive Haltung gegenüber der bestehenden Verfassungsordnung voraussetzt.

4. Zu § 4:

Die Notwendigkeit, in § 4 "die Rechts- und **Amtshilfe** ohne inhaltliche Änderung gegenüber der bestehenden Rechtslage" (vgl. Gesetzesbegründung zu § 4) zu regeln, ist nicht erkennbar.

Ich rege deshalb an, § 4 zu streichen. Zumindest sollte in dem Gesetzestext jedoch eine Klarstellung eingefügt werden, daß die Zulässigkeit der Verarbeitung personenbezogener Daten sich nach den Vorschriften des 2. Abschnitts des Entwurfs beurteilt. Der Hinweis in der Gesetzesbegründung, daß die Vorschrift der Verfassungsschutzbehörde keine Datenverarbeitungsrechte gibt, reicht nicht aus um zu verhindern, daß bei den ersuchten Behörden das Mißverständnis entsteht, hier sei eine besondere Datenverarbeitungsregelung getroffen.

5. Zu § 5 Abs. 1:

Diese Vorschrift stößt als **Generalklausel** auf verfassungsrechtliche Bedenken.

Nach den im Volkszählungsurteil des Bundesverfassungsgerichts aufgestellten Grundsätzen sind Einschränkungen des Rechts auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem Gebot der Normenklarheit entspricht und den Verhältnismäßigkeitsgrundsatz beachtet (BVerfGE 65, 43 - 44). Von Art und Umfang und denkbarer Verwendung der Daten sowie der Gefahr des Mißbrauchs hängt es ab, inwieweit das Recht auf informationelle Selbstbestimmung zu derartigen gesetzlichen Regelungen zwingt (BVerfGE 65, 45 - 46). Lediglich bei weniger schwerwiegenden Einschränkungen des Rechts auf informationelle Selbstbestimmung können als Generalklauseln ausgestaltete Auffangnormen in den Datenschutzgesetzen ausreichen. Bei einer stärkeren Belastung des Betrof-

fenen sind jedoch bereichspezifische Regelungen für den jeweiligen Verwaltungszweig, insbesondere für die Sicherheits- und Strafverfolgungsbehörden erforderlich (vgl. Weyer, Datenschutzgesetz Nordrhein-Westfalen, Essen 1988, zu Artikel 1, 2 GG, Artikel 4 LV Rdnr. 5).

6. Zu § 5 Abs. 2:

Wie bereits zu § 5 Abs. 1 ausgeführt, sind bei schwerwiegenden Eingriffen in das Recht auf informationelle Selbstbestimmung bereichspezifische gesetzliche Regelungen unerläßlich. Diese gesetzlichen Grundlagen müssen dem rechtsstaatlichen Gebot der Normenklarheit entsprechen. Voraussetzungen und Umfang der Beschränkungen müssen darin klar und für den Bürger erkennbar geregelt sein (BVerfGE 65, 44). Verwaltungsvorschriften, Erlasse und Richtlinien sind keine Rechtsnormen in materiellem Sinne.

§ 5 Abs. 2 läßt dies unberücksichtigt, obwohl gerade die nach Maßgabe des § 7 anzuwendenden Methoden und Gegenstände einschließlich technischer Mittel zur **heimlichen Informationsbeschaffung** unstreitig gravierende Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen. Den Anforderungen des Bundesverfassungsgerichts entspricht es nicht, wenn ein nicht abschließend aufgeführter Methoden- und Gegenstandskatalog in einer **Dienstvorschrift als Befugnisnorm** für Eingriffe der Verfassungsschutzbehörde in das Recht auf informationelle Selbstbestimmung ausreichen soll. Dies ist um so bedenklicher, als laut Gesetzesbegründung damit die z. Z. bekannten Mittel wiedergegeben werden sollen, obwohl z. B. mit dem heimlichen Mithören ohne Inanspruchnahme technischer Mittel oder der Beobachtung des Funkverkehrs auf nicht für den allgemeinen Empfang bestimmten Kanälen weitere Mittel bereits jetzt zur Verfügung stehen.

Gerade weil es, wie in der Gesetzesbegründung ausgeführt, nicht möglich ist, alle in Zukunft in Betracht kommenden

Mittel zur heimlichen Informationsbeschaffung abschließend aufzuzählen, müssen jedenfalls die z. Z. bekannten gesetzlich festgeschrieben sein. Nur so ist es dem Gesetzgeber möglich, eine Wertentscheidung zu treffen, ob und ggf. welche neueren technischen Möglichkeiten überhaupt eingesetzt werden dürfen.

Ich empfehle daher dringend, die besonderen Eingriffsbefugnisse der Verfassungsschutzbehörde jeweils einzeln im Gesetz zu regeln. Gerade weil die Tätigkeit der Verfassungsschutzbehörde weitgehend im Geheimen stattfindet, ist es erforderlich, die Befugnisse für eine derartige Tätigkeit normenklar zu fassen. Für den Polizeibereich hat dies der Landesgesetzgeber bereits in den §§ 16 - 21 PolG NW geregelt. Entsprechende ausformulierte Vorschläge für den Verfassungsschutzbereich habe ich dem Innenministerium vorgelegt.

7. Zu § 5 Abs. 3:

Soweit Satz 2 der Vorschrift die Regelvermutung festschreibt, daß für den Betroffenen eine geringere Beeinträchtigung anzunehmen ist, wenn Informationen aus allgemein zugänglichen Quellen oder durch behördliche Auskunft gewonnen werden können, stellt dies eine Umkehr des in § 12 Abs. 1 Satz 3 i. V. m. § 13 Abs. 2 Satz 1 Buchst. a und c - g DSG NW festgelegten Grundsatzes dar. Danach sind personenbezogene Daten grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben.

Die Gesetzesbegründung zu § 5 Abs. 3 erläutert nicht klar, welche Gründe für die in Absatz 3 genannte Regelvermutung und damit letztendlich dafür sprechen, daß für den Bereich der Verfassungsschutzbehörde der Grundsatz des § 12 Abs. 1 Satz 3 DSG NW durchbrochen werden soll. Übersehen wird dabei offenbar, daß selbst einfache Anfragen, etwa bei kleineren Gemeinden, die erkennbar vom Verfassungsschutz

ausgehen, durchaus geeignet sind, die Betroffenen in ihrem sozialen Umfeld erheblich zu belasten.

8. Zu § 7 Abs. 2:

Die Vorschrift sieht eine **Datenerhebung in der Wohnung** durch die Verfassungsschutzbehörde zur Gewinnung von Informationen über eine drohende gemeine Gefahr oder eine Lebensgefahr für einzelne Personen vor. Der Verfassungsschutzbehörde werden somit Aufgaben der Gefahrenabwehr zugewiesen, die gemäß § 10 Satz 2 Polizeiorganisationsgesetz NW i. V. m. § 1 Abs. 1 Satz 1 Polizeigesetz NW in die Zuständigkeit der Polizei fallen. Für die Polizei gelten zudem in diesem Bereich engere Vorschriften (§ 18 Abs. 2 i. V. m. Abs. 1 Nr. 1 PolG NW).

Der Vorschrift fehlt zudem eine entsprechende Zweckbindungs- und Löschungsregelung in der Weise, daß die Löschung der erhobenen Daten ihrer Zweckbestimmung wegen unmittelbar nach Abwehr der in der Vorschrift beschriebenen Gefahr zu erfolgen hat. Die in § 7 Abs. 3 Satz 3 vorgesehenen Einschränkungen der Verwendung der nach Absatz 2 erhobenen Daten nach Maßgabe des § 7 Abs. 3 und 4 des Gesetzes zu Artikel 10 Grundgesetz ist in dieser Hinsicht nicht weitreichend genug.

9. Zu § 7 Abs. 4:

Im Hinblick auf § 10 Abs. 3 und der dort vorgesehenen 10jährigen Aufbewahrungsfrist ist nicht nachzuvollziehen, warum eine Mitteilung über Maßnahmen gemäß § 7 Abs. 3 schon nach fünf Jahren nicht mehr erteilt zu werden braucht, obwohl dies noch weitere fünf Jahre möglich wäre. Die Fristen sollten deshalb vereinheitlicht werden.

Ein Hinweis wie in § 8 Abs. 5 letzter Satz VSG SH, wonach der betroffenen Person nach der Mitteilung der Rechtsweg offen steht, bietet sich darüber hinaus an.

10. Zu § 10 Abs. 1:

Anders als in § 19 Abs. 1 und 2 DSG NW unterscheidet § 10 Abs. 1 i. V. m. § 11 nicht nach automatisierten und nichtautomatisierten Dateien. Demzufolge ist auch eine differenzierte Regelung der Berichtigung unrichtiger Daten in den verschiedenen Speichermedien nicht vorgesehen.

Satz 2 regelt im übrigen nur unzureichend das Verfahren, das stattzufinden hat, wenn die Richtigkeit der in Dateien gespeicherten personenbezogenen Daten von dem Betroffenen bestritten wird. Es stellt sich zwangsläufig die Frage, was passiert, wenn sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

Absatz 1 müßte daher eine ausführlichere Ausgestaltung erfahren.

11. Zu § 11 Abs. 1:

Das Verfahren, wie personenbezogene Daten, die unrichtig sind oder deren Richtigkeit vom Betroffenen bestritten wird, zu behandeln sind, ist wenig normenklar, da es nicht an § 19 DSG NW (Berichtigung, Sperrung, Löschung) orientiert ausgestaltet wurde. Es sollte daher in Absatz 1 zumindest folgender Satz 3 eingefügt werden: "Läßt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, so sind die personenbezogenen Daten zu sperren".

12. Zu § 11 Abs. 2:

Die Vorschrift macht, insbesondere auch in der Gesetzesbegründung, nicht deutlich, welche bereichspezfischen Notwendigkeiten Anlaß zu einer gegenüber § 19 Abs. 2 (Sperrung) und 3 (Löschung) DSG NW abweichenden Regelung geben. Insbesondere die nach § 19 Abs. 2 Satz 2 DSG NW gebotene Aufzeichnung der Gründe für eine weitere Speicherung fehlt.

13. Zu § 12 Abs. 1:

Ein klarstellender Hinweis wäre angebracht, daß auch Dateien nach § 13 unter Absatz 1 fallen.

Es ist nicht nachvollziehbar, aus welchen Gründen in § 12 Abs. 1 für eine Dateianordnung ein anderer Inhalt als in § 8 DSG NW für eine Dateibeschreibung festgelegt wird. Bereichspezifische Besonderheiten, die ein Abweichen von § 8 DSG NW erfordern könnten, sind nicht erkennbar, wie auch ein Vergleich mit § 15 VSG SH verdeutlicht.

Ich gehe daher davon aus, daß wegen § 28 die Regelungen der §§ 23 und 8 DSG NW neben § 12 Geltung haben, die Verfassungsschutzbehörde also verpflichtet ist, dem Landesbeauftragten für den Datenschutz die Beschreibung aller automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert sind, mit den Angaben der Dateibeschreibung nach § 8 Abs. 1 DSG NW vorzulegen.

14. Zu § 13:

Es sollte entweder, wie zu § 12 Abs. 1 ausgeführt, dort oder ansonsten in § 13 klargestellt werden, daß Dateibeschreibungen/-anordnungen auch für die Verbunddateien zu erstellen sind, da für ihre Daten speichernde Stelle die Verfassungsschutzbehörde Nordrhein-Westfalen ist.

15. Zu § 14 Abs. 1:

In Ermangelung einer bereichspezifischen Auskunfts-/Akteneinsichtsregelung im Verfassungsschutzgesetz Nordrhein-Westfalen in der derzeit gültigen Fassung richtet sich das **Recht des Betroffenen auf Auskunft und Akteneinsicht** z. Z. nach § 18 DSG NW in der Fassung vom 15.03.1988. Die darin enthaltene inhaltliche und verfahrensmäßige Ausgestaltung des Auskunfts-/Akteneinsichtsrechts läßt nach den Erfahrungen in der Praxis durchweg einen angemessenen Ausgleich

der Interessen von Betroffenen und der Verfassungsschutzbehörde zu.

Insbesondere die in § 18 Abs. 3 DSG NW vorgesehene Möglichkeit der Auskunftsbeschränkung und die flankierenden Maßnahmen nach § 18 Abs. 4 und 5 DSG NW tragen dazu bei, daß grundsätzlich soweit Auskunft erteilt werden kann, als Sicherheitsinteressen nicht berührt sind. Auskünfte in vollem oder eingeschränktem Umfang sind demnach genauso möglich wie eine generelle Auskunftsverweigerung unter Hinweis auf § 18 Abs. 3 DSG NW, verbunden mit dem Hinweis, daß daraus nicht der Schluß gezogen werden kann, Daten seien über den Auskunftsbegehrenden gespeichert oder nicht gespeichert. Selbst nach der Rechtslage des Datenschutzgesetzes Nordrhein-Westfalen in der Fassung vom 19.12.1978 (vgl. §§ 16 i. V. m. 15 Abs. 2 Nr. 1, die auf Polizei und Verfasungsschutz keine Anwendung fanden) hat die Verfassungsschutzbehörde im Hinblick auf Artikel 4 Abs. 2 Landesverfassung NW bereits vor Inkrafttreten des Datenschutzgesetzes Nordrhein-Westfalen vom 15.03.1988 in diesem Sinne Auskunft erteilt.

Auf Grund der Praxis der zurückliegenden Jahre ist die Erforderlichkeit der Regelung zur Auskunft und Akteneinsicht, wie sie in § 14 vorgenommen werden soll, in Frage zu stellen, wenn Absatz 1 nunmehr bereits von vornherein den Auskunftsanspruch im Gegensatz zu § 18 Abs. 1 Nr. 2 und 3 DSG NW auf die zur Person des Betroffenen gespeicherten Daten, den Zweck und die Rechtsgrundlage der Speicherung beschränkt und nicht einmal eine Prüfung vorsieht, ob nicht auch die Herkunft der Daten und Empfänger von Übermittlungen mitgeteilt werden können. Ein sachlicher Grund für eine derart weitgehende, unbedingte Geheimhaltung ist nicht erkennbar, zumal mit § 14 Abs. 2 ein Korrektiv verbleibt, die Auskunftserteilung und Akteneinsicht einzuschränken und den Sicherheitsinteressen ausreichend Rechnung zu tragen. Gleiches müßte gelten, sollte mit § 14 auch das Akteneinsichtsrecht des § 18 DSG NW von vornher-

ein ausgeschlossen werden, was wegen § 28, der das Datenschutzgesetz Nordrhein-Westfalen für anwendbar erklärt, wohl nicht der Fall sein dürfte. Sicherlich käme ein solches Akteneinsichtsrecht in der Praxis im Ergebnis nur als Ausnahme in Betracht; dann jedoch sollte es auch gewährt werden.

16. Zu § 14 Abs. 2:

In Nummer 1 sollte dargelegt werden, wessen Aufgabenerfüllung gefährdet sein soll.

17. Zu § 14 Abs. 3:

Die Vorschrift ist ersatzlos zu streichen (siehe Ausführungen zu § 14 Abs. 1).

18. Zu § 14 Abs. 4 Satz 6:

Soweit in Satz 6 die Offenbarung der Personalien eines Betroffenen, dem Vertraulichkeit besonders zugesichert worden ist, gegenüber dem Landesbeauftragten für den Datenschutz ausgeschlossen wird, ist nicht verständlich, wann diese Beschränkung greifen soll. Liest man Satz 6 im Zusammenhang mit den vorhergehenden Regelungen, so erscheint diese Beschränkung wenig einleuchtend.

Es bedürfte zudem einer umfassenden Regelung darüber, auf welchen Kreis die Kenntnisse beschränkt werden, wenn einem Betroffenen Vertraulichkeit besonders zugesichert worden ist (z. B. Kontrollgremium, Landesrechnungshof). Durch die Verwendung des Begriffs "Betroffener" besteht bei entsprechender Auslegung durchaus die Möglichkeit, die Kontrollbefugnis des Landesbeauftragten für den Datenschutz in weiten Bereichen durch einseitige Vertraulichkeitszusicherungserklärung der Verfassungsschutzbehörde auszuschließen. Die Notwendigkeit für eine solche Regelung hat sich schließlich in der Vergangenheit nicht ergeben.

19. Zu § 16 Abs. 1:

Die Regelung in § 16 Abs. 1 Satz 2, 2. Halbsatz, wonach die in Satz 1 genannten Behörden, Einrichtungen und juristischen Personen mit Ausnahme der Staatsanwaltschaften und Polizeibehörden Übermittlungen der ihnen bekannten Tatsachen über Bestrebungen und Tätigkeiten im Sinne des § 3 Abs. 1 vornehmen können, sollte überdacht werden.

Der Umstand, daß diese Datenübermittlung zu Tatsachen über Bestrebungen und Tätigkeiten im Sinne des § 3 Abs. 1 ins Belieben der in Satz 1 genannten Behörden, Einrichtungen und juristischen Personen, ausgenommen Staatsanwaltschaften und Polizei, gestellt wird, läßt Zweifel an der Erforderlichkeit solcher Übermittlungen entstehen. Die Befugnis fordert geradezu einen Fluß von Informationen heraus, die für die rechtmäßige Aufgabenerfüllung der Verfassungsschutzbehörde häufig unbrauchbar sein dürften. Während bei Staatsanwaltschaften und Polizei zumindest behördenintern sichergestellt werden kann, daß qualifiziert bewertete Informationen an die Verfassungsschutzbehörde übermittelt werden, dürfte dies bei anderen Behörden und Stellen nicht der Fall sein. Diese Art der Mitarbeit seitens anderer Behörden sollte deutlich eingeschränkt werden. Zudem könnte die Vorschrift als Grundlage eines alle öffentlichen Stellen **umfassenden Informationssystems des Verfassungsschutzes** mißverstanden werden.

20. Zu § 16 Abs. 3:

Die Norm bedeutet einen sachlich nicht zu begründenden **Rückschritt** gegenüber § 4a VSG NW in der derzeit gültigen Fassung. Sowohl in formeller als auch in materieller Hinsicht sind datenschutzrechtliche Verschlechterungen vorgesehen, die nicht nachvollziehbar, weil nicht argumentativ belegt sind. Meine Bedenken gegen die Fassung des § 4a VSG NW bleiben unabhängig hiervon bestehen (vgl. Vorlage 10/114 vom 15. Oktober 1985).

Unter formellen Aspekten ist die Entscheidungsbefugnis vom Innenminister oder seinem ständigen Vertreter auf den Leiter der Verfassungsschutzabteilung übergegangen (§ 16 Abs. 3 Satz 2). Lediglich die Anordnung der Benutzung von Registern oder Teilen davon zum Zwecke des automatisierten Abgleichs (Rasterfahndung) ist dem Minister oder seinem ständigen Vertreter vorbehalten. Eine Pflicht des Innenministers zur Unterrichtung des parlamentarischen Kontrollgremiums innerhalb von sechs Monaten über angeordnete Registereinsichten ist auf diese Fälle beschränkt worden.

Unter materiellen Aspekten kommt es nicht mehr darauf an, ob die Aufklärung unter Beachtung des Verhältnismäßigkeitsgrundsatzes auf andere Weise nicht möglich erscheint und ob besondere gesetzliche Geheimhaltungsvorschriften oder ein Berufsgeheimnis entgegenstehen. Eine ausdrückliche Zweckbindungsklausel ist für die durch die Registereinsicht gewonnenen Erkenntnisse ebensowenig vorgesehen, wie eine abschließende Aufzählung der Register, in die die Verfassungsschutzbehörde Einblick nehmen kann. Vielmehr drängt sich der Eindruck auf, daß mit der Registereinsicht der Verfassungsschutzbehörde eine spezielle Erhebungsmethode als alternative Informationserhebungsmethode zur Verfügung gestellt werden soll. Dies muß um so mehr gelten, als die Suche mit Hilfe bestimmter Rasterkriterien nicht ausdrücklich zu Gunsten der Einholung einer Auskunft über einzelne Personen ausgeschlossen ist. Hierbei ist im übrigen auch nicht sichergestellt, daß der registerführenden Stelle die Tatsache der Ermittlung gegen diese Person verborgen bleibt.

21. Zu § 16 Abs. 5:

Anders als § 23 Abs. 3 VSG SH enthält Absatz 5 keine Regelung für die Übermittlung personenbezogener Daten, die auf Grund anderer strafprozessualer Zwangsmaßnahmen als der Maßnahmen nach § 100a Strafprozeßordnung bekanntgeworden sind.

22. Zu § 17 Abs. 1:

Absatz 1 ist in dieser Form zu weit und damit nicht hinreichend klar gefaßt. Empfehlenswert wäre, die Voraussetzungen für die Datenübermittlung im einzelnen in einem Katalog ähnlich § 19 Abs. 2 VSG SH aufzulisten.

23. Zu § 17 Abs. 2:

Mit dem Verweis auf Artikel 3 des Zusatzabkommens zum NATO-Truppenstatut wird keine ausreichende Grundlage für eine Datenübermittlung geschaffen. Die dort enthaltene Zusammenarbeitsklausel ist derart undifferenziert, daß sie nicht einmal dem Erforderlichkeitsgrundsatz der allgemeinen Datenschutzgesetze entspricht. Im übrigen wird in dem Abkommen nicht ausreichend zwischen dem allgemeinen Informationsaustausch und der Verarbeitung personenbezogener Daten unterschieden.

24. Zu § 17 Abs. 3:

Im Hinblick auf datenschutzrechtliche Standards im Ausland ist die Übermittlungsvorschrift des Absatzes 3 Satz 1, die Übermittlungen offensichtlich ohne nähere Voraussetzungen an jede ausländische öffentliche Stelle sowie an über- und zwischenstaatliche Stellen zuläßt, zu weit gefaßt. Der Hinweis an den Empfänger, daß die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden, sowie der Hinweis auf die Bitte um Auskunft über die vorgenommene Verwendung der Daten, die sich die Verfassungsschutzbehörde vorbehält, machen deutlich, daß hier dem Datenschutzgesetz Nordrhein-Westfalen gleichwertige Datenschutzregelungen von vornherein nicht einzuhalten sind.

25. Zu § 17 Abs. 4:

Es ist bedauerlich, daß die zum inhaltsgleichen § 19 Abs. 4 Bundesverfassungsschutzgesetz bereits diskutierte Problematik der Datenübermittlung an Private bei sogenannten operativen Maßnahmen in § 17 Abs. 4 nicht in einer den Zweck der Vorschrift normenklar zum Ausdruck bringenden Weise gelöst worden ist. § 17 Abs. 4 gibt in der vorgelegten Fassung ebenso wie § 19 Abs. 4 Bundesverfassungsschutzgesetz keine Anhaltspunkte für eine Unterscheidung zwischen operativen und sonstigen Maßnahmen. Die Zustimmung des Innenministers in Person oder des von ihm Beauftragten bleibt demnach auch gemäß § 17 Abs. 4 für jede Datenübermittlung an Private erforderlich. Der anderslautende Hinweis in der Gesetzesbegründung dürfte angesichts des insoweit eindeutigen Wortlauts nichts ändern.

26. Zu § 18 Abs. 1:

Soweit in Absatz 1 neben den klassischen Staatsschutzdelikten in §§ 74a und 120 Gerichtsverfassungsgesetz sonstige Straftaten erfaßt werden, bei denen auf Grund ihrer Zielsetzung, des Motivs des Täters oder dessen Verbindung zu einer Organisation tatsächliche Anhaltspunkte dafür vorliegen, daß sie gegen die in Artikel 73 Nr. 10 Buchst. b oder c des Grundgesetzes genannten Schutzgüter gerichtet sind, ist nach den Erfahrungen mit der Staatsschutzdatei "Arbeitsdatei PIOS Innere Sicherheit (APIS)" damit zu rechnen, daß auch bei Straftaten mit nur oberflächlichem politischem Bezug Datenübermittlungen an die Polizei erfolgen. Dem sollte im vorhinein durch eine Einschränkung der Übermittlungsverpflichtung Beachtung geschenkt werden.

27. Zu § 20:

Es bleibt offen, worin der besondere Minderjährigenschutz bestehen soll. Der Empfängerkreis der zu übermittelnden Informationen wird nicht näher festgelegt.

28. Zu § 28:

Erfahrungsgemäß dürfte es im Zusammenhang mit einer derartigen Globalverweisung in der täglichen Praxis Anwendungs- und Auslegungsprobleme geben. Gerade für die Arbeit einer Verfassungsschutzbehörde wäre es ein erheblicher Fortschritt im Hinblick auf mehr Transparenz der Datenverarbeitung, wenn im einzelnen die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen mit ihrem Anwendungsumfang aufgeführt würden.

Maier-Bode

(Maier-Bode)