Humanistische Union

Die (un)heimliche Staatsgewalt: VII. Datenschutz

aus: vorgänge Nr. 55 (Heft 1/1982), S. 105-107

Ein nicht mehr zu vernachlässigender Teil unserer Bevölkerung findet das Interesse des Verfassungsschutzes, der, meistens ohne Wissen der Betroffenen, deren „Datenschatten" in seinen Akten und Dateien „abbildet". Die wenigen bekannt gewordenen Zahlen gehen von 5% der Bevölkerung beim Bundesamt für Verfassungsschutz [1] bis zu 10% beim Verfassungsschutz in Berlin [2]. Wie die eindrucksvollen Fallsammlungen von *J. Bösche* [3] über Sicherheitsüberprüfungen und *D. Damm* [4] über Mitwirkung bei Einstellungsüberprüfungen belegen, sammeln die Verfassungsschutzbehörden häufig Daten über die bloße Ausübung von Grundrechten, über Gesinnungen und Verhalten, die vom jeweils politisch Erwünschten abweichen. Solche Daten gehen den Staat nichts an. Vor allem durch die großzügige Weitergabe dieser Informationen an andere Behörden, an Arbeitgeber und sonstige Privatpersonen [5] wird grundgesetzwidrig in die Privatsphäre der Betroffenen eingegriffen, Die bisherigen Versuche von Gesetzgeber und Verwaltung, dem Bürger auch faktisch zu seinen Grundrechten zu verhelfen, reichen nicht aus. So enthalten die *Datenschutzgesetze* von Bund und manchen Ländern zu viele Generalklauseln und unbestimmte Rechtsbegriffe und schließen im Sicherheitsbereich die Kontrolle durch den Betroffenen praktisch aus. Bereichspezifische Regelungen sind nur in Verwaltungsrichtlinien festgehalten.

Deshalb ist eine *spezielle gesetzliche Datenschutzregelung* für den Verfassungsschutz zu fordern mit folgenden Schwerpunkten:

1 Einschränkung der Erfassung, Speicherung und Übermittlung von personenbezogenen Daten.

2 Löschung nach Frist.

3 Kontrolle durch Anspruch des Betroffenen auf Auskunft aus Dateien und Akten.

Selbstverständlich müssen auch die inzwischen erreichten Fortschritte der Datenschutz-Diskussion berücksichtigt werden wie etwa die kostenlose Auskunft, Schadenersatz auch für immaterielle Schäden, feste Regeln für die Errichtung und Führung von Dateien, Transparenz für den Bürger.

Erfassung und Speicherung:

Gemäß dem Datenschutzprinzip dürfen nur solche personenbezogene Daten erfasst und gespeichert werden, die für die Erfüllung der gesetzlich zugewiesenen Aufgaben unerlässlich sind. Im Sinne der mit dem vorliegendem Memorandum geforderten Beschränkung der Verfassungsschutz-Aufgaben ist nur noch die Erfassung und Speicherung von Daten über sicherheitsüberprüfte, oder der Spionage verdächtigen Personen und ggf. über Träger von „Bestrebungen" zulässig.
Bei der Sicherheitsüberprüfung werden sowohl Daten vom Betroffenen selbst als auch bei anderen, etwa bei Bekannten oder dem Arbeitgeber erhoben. Damit diese Eingriffe in die Privatsphäre minimal bleiben, sind Art und Umfang der zur Erfassung und Speicherung zugelassenen Merkmale an die unterschiedlichen Sicherheits- und Geheimhaltungsstufen anzupassen und in einer *Rechtsverordnung* festzulegen. Auf diese weise wird sowohl die nötige Transparenz für die Öffentlichkeit erreicht als auch die Möglichkeit gewährleistet, flexibel auf neuartige Sicherheitsrisiken reagieren zu können.
Die *Spionageabwehr* ist mit einer großen und weiter wachsenden Varianz von Spionage-Methoden

konfrontiert, so daß die zu erfassenden und speichernden Merkmale kaum abschließend festgelegt werden können. Deshalb ist hier eine besondere Kontrolle erforderlich: Der Amtschef hat im Einzelfall festzustellen, ob tatsächliche Anhaltspunkte für die Agententätigkeit die Sammlung und Speicherung personenbezogener Daten rechtfertigen.
Werden Bewertungen über Betroffene gespeichert, muss erkennbar sein, wer die Bewertung vorgenommen hat und wo die Informationen gespeichert sind, die der Bewertung zugrunde liegen [6].

Übermittlung:

Analysen der gegenwärtigen Situation, z.B. die von *R. Riegel* [7], zeigen übereinstimmend, daß die Verfassungsschutz- und die Datenschutzgesetze lückenhaft und unbestimmt sind und daß die Richtlinien, die versuchen, diese Lücken zu füllen, durch gesetzliche Regelungen ersetzt werden müssen. Beispielhaft seien hier genannt die Übermittlungspflichten in den „Richtlinien für die Zusammenarbeit der Verfassungsschutzbehörden, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes, der Polizei und der Strafverfolgungsbehörden in Staatsschutzangelegenheiten [8]. Zur Begründung wird auf das Kapitel „Amtshilfe" verwiesen, Stichworte: Gesetzliche Grundlage für Eingriffe, keine „Einheit der Staatsgewalt", sondern Kompetenzverteilung. Gegen diesen zuletzt genannten Grundsatz verstoßen mehrere Landes-Verfassungsschutzgesetze [9], indem sie alle Gliederungen der Verwaltung verpflichten, unaufgefordert alle relevanten „Tatsachen und Unterlagen" den Verfassungsschutzbehörden zu übersenden, also alle Bedienstete der Verwaltung zu V-Leuten dienstverpflichtet.

Aufgrund der mit diesem Memorandum geforderten Aufgabenbegrenzung des Verfassungsschutzes ist die Übermittlung von personenbezogenen Informationen an andere Stellen auf folgende vier Fälle zu begrenzen:

1 Übermittlung von Informationen über Straftaten nach § 138 Strafgesetzbuch an die Strafverfolgungsbehörden;

2 Übermittlung von Informationen über die Gefährdung der in der Bundesrepublik stationierten NATO-Truppen an die zuständigen Behörden des betroffenen Staates;

3 Übermittlung des Ergebnisses einer Sicherheitsüberprüfung an den Arbeitgeber, aber nur mit Einverständnis des Betroffenen;

4 Übermittlung von tatsächlichen Anhaltspunkten für eine Agententätigkeit an andere Stellen, sofern der Innenminister eingewilligt hat.

Wie im Kapitel „Amtshilfe" begründet wurde, ist die Übermittlung von Informationen zwischen dem Verfassungsschutz und dem Bundesnachrichtendienst sowie dem Militärischen Abschirmdienst gegenwärtig rechtswidrig.
Zwischen den Informationssystemen des Verfassungsschutzes und denen der zugelassenen Empfänger darf weder ein Dateiverbund bestehen noch ein Dateienabgleich durchgeführt werden.
Entsprechend der Regelung im *Melderechtsrahmengesetz* [10] sind in allen Fällen der Übermittlung der Name und die Anschrift des Betroffenen unter Hinweis auf den Anlass der Übermittlung aufzuzeichnen. Diese Aufzeichnungen sind gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Erstellung der Aufzeichnung folgt, zu vernichten.

Löschung:

Die Frage der Aufbewahrungsfristen für Daten ist u.a. auch durch mehrere bekannt gewordene Fälle der Speicherung von „Jugendsünden" in den Vordergrund gerückt worden. Diese Diskussion hat verdeutlicht, das sich Einstellung und Verhalten eines Menschen im Laufe seines Lebens ändern und das sein „Abbild" in den Datensammlungen entsprechend veraltet. Aus dieser Erkenntnis entstand das Modell des „programmierten Vergessens" (*S. Simitis*), wonach bereits bei der Dateneingabe in automatisch geführte Dateien die automatische Sperrung oder Löschung nach Ablauf bestimmter Fristen initiiert wird. Dieses Modell wurde, wenn auch äußerst zaghaft, in die im März 1981 in kraft gesetzten Dateirichtlinien des Bundeskriminalamts übernommen. Im Gegensatz zu den oben behandelten Zusammenhängen liegen ganz eindeutige Anlässe für die Löschung von Daten vor, wenn ein Arbeitnehmer auf einen Arbeitsplatz mit niedriger Sicherheitsstufe wechselt oder aus dem Arbeitsverhältnis ausscheidet.

In die Verfassungsschutz-Gesetze sind somit folgende Löschungsprinzipien aufzunehmen:

1 Festlegung von Aufbewahrungsfristen, die an die Bedeutung der Daten angepaßt sind.

2 Unterlagen sind zu vernichten und Daten zu löschen, wenn die Gründe, die zur Aufbewahrung der Daten geführt haben, nicht zutreffen. Im letzten Fall müssen die Daten auch bei denjenigen Stellen gelöscht werden, an die sie übermittelt wurden.

3 Bei automatisch geführten Dateien ist bereits bei der Dateneingabe die automatische Sperrung oder Löschung nach Ablauf bestimmter Fristen vorzusehen.

Verweise

1 J. Bölsche, DerWeg in den Überwachungsstaat, Reinbeck,1979, S 37.
2 3. Internationales Russell-Tribunal, Band 4, Berlin, 1979, S 104.
3 J.. Bölsche, aaO, S 155 ff.
4 P. Brückner, D. Damm, J. Seifert, 1984 schon heute?, Frankfurt, 1977.
5 Süddeutsche Zeitung vom 19.10.79, S. 21: Der Bayerische Innenminister Seidl gibt Verfassungsschutz-Daten über „mißliebige" Bürger an Parteifreunde weiter.
6 A. Podlech, Das umfassenste Mittel staatlicher Herrschaft, in: DAS PARLAMENT, 26.8.78, S 2.
7 R. Riegel, Datenschutz bei den Sicherheitsbehörden, Köln, Berlin, Bonn, München, 1980.
8 Richtlinien für die Zusammenarbeit der Verfassungsschutzbehörden, des Bundesnachrichtendienstes (BND), des Militärischen Abschirmdienstes (MAD), der Polizei und der Strafverfolgungsbehörden in Staatssschutzangelegenheiten (Zusammenarbeitsrichtlinien) von 1973, in: Frankfurter Rundschau vom 7.11.79, S 5.
9 Hier handelt es sich um die Verfassungsschutzgesetze von Bayern, Berlin, Hessen, Rheinland-Pfalz, Saarland, Schleswig-Holstein. In Baden-Württemberg und Niedersachsen sind diese Mitteilungspflichten sehr eng begrenzt.
10 Melderechtsrahmengesetz (MRRG) vom 16.8.80, § 18, Absatz 3, Sätze 2 und 3, BGBL Teil I, Nr. 54, S 1433.
11 Richtlinien für die Errichtung und Führung von Dateien über personenbezogene Daten beim Bundeskriminalamt, Punkt 7, Gemeinsames Ministerialblatt, 1981, S. 114.
