Sicherheit und Datenschutz - ein Widerspruch?

Bürgerfreiheit und Sicherheitsvorsorge nach dem 11. September 2001

Vortrag anlässlich des Festakts zum 200. Stiftungsfest der Baruthia

Hohe Festversammlung, meine sehr geehrten Damen und Herren,

.....

Ich habe es deshalb gerne übernommen, heute vor Ihnen zum Thema Bürgerfreiheit und Innere Sicherheit zu sprechen.

Datenschutz ist ein wesentlicher Teil der Bürgerfreiheit. Das Recht auf Datenschutz bedeutet in erster Linie das Recht, dass Sie selbst bestimmen, wer was über Sie weiß und was er mit diesem Wissen anfängt.

Der Satz "Wissen ist Macht" leuchtet jedem ein. Wer alles über mich weiß, kennt meine Stärken, er kennt aber auch meine Schwächen. Er hat mich informationell in der Hand. George Orwell hat die Auswirkungen und die Missbrauchsmöglichkeiten einer totalen Kontrolle des Einzelnen durch den Staat in seinem Roman "1984" sehr eindringlich beschrieben.

Der Satz "von mir kann jeder Alles wissen" sagt sich leicht dahin. Ganz anders sehen die Dinge dann aber aus, wenn jemand ganz konkret betroffen ist: Z.B. wenn er als Verdächtiger in einer polizeilichen Datei auch dann noch gespeichert ist, wenn ein Ermittlungsverfahren gegen ihn mangels hinreichendem Tatverdachts eingestellt. Es wird sich auch niemand darüber freuen, wenn seine Unterhaltung mit Freunden im Lokal eines Wirtes belauscht wird, gegen den z.B. wegen gewerbsmäßiger Hehlerei ermittelt wird.

Natürlich müssen die Meldeämter Namen und Adressen von Einwohnern speichern, natürlich muss die Polizei Daten über Straftäter, in bestimmtem Umfang auch Daten über Verdächtige speichern können.

Diese Speichermöglichkeiten müssen im Interesse des Bürgers aber gesetzlich begrenzt sein, sie dürfen nicht über das hinausgehen, was zur Erfüllung der Aufgaben der jeweiligen Dienststellen erforderlich ist.

Sie müssen auch verhältnismäßig zur Eingriffstiefe sein. Wegen einer Übertretung oder einer Straftat des mittleren Bereichs dürfen keine Telephone abgehört oder Wohnungen belauscht werden. Die ständige Erweiterung des Straftatenkatalogs in § 100a StPO – Telephonabhören zur Strafverfolgung – erfüllt mich deshalb mit Sorge.

Andererseits müssen diese Bestimmungen auch die erforderliche und verhältnismäßige Datenverarbeitung durch die Sicherheitsbehörden ermöglichen. Auch die Sicherheit des Staates und die Sicherheit seiner Bürger stellen Verfassungswerte dar.

Dem Satz "keine Freiheit ohne Sicherheit" kann ich auch als Datenschützer zustimmen. Ich hebe aber ebenso hervor: Ein Leben in Sicherheit, aber ohne Freiheit wäre genauso wenig lebenswert.

Es gilt deshalb einen sachgerechten Ausgleich zwischen den Anforderungen der Sicherheit und den Grundgeboten der Freiheit zu finden. Dabei sehe ich keinen diametralen Widerspruch zwischen Datenschutz und Polizei: Beide haben die Aufgabe, Teile unserer Verfassungsordnung zu schützen, beide haben die Aufgabe, den Bürger zu schützen.

Konflikte sind aber vorgegeben. Von seiner Zielsetzung her intendiert das Recht auf Freiheit auf Begrenzungen der Datenverarbeitungsmöglichkeiten; im Gegensatz dazu werden Sicherheitsbehörden möglichst viel wissen wollen und dieses Wissen möglichst lange vorhalten und möglichst umfangreich verarbeiten wollen.

Hier ist gegenseitiger Respekt vor der Aufgabe der jeweils anderen Stelle erforderlich; genauso die Bereitschaft, aufeinander zuzugehen. Es stellt diese Aufgabe aber nichts

grundsätzlich ungewöhnliches dar; sie ist bei widerstreitenden Grundrechten unter der Rechtsfigur der "Praktischen Konkordanz" bekannt.

Was soll diesen Ausgleich gewährleisten? Das sind beispielsweise die Vorschriften des Verfassungsschutzrechtes, die Polizeigesetze, die Strafprozessordnung und die Datenschutzgesetze.

Sie enthalten Befugnisse zur Datenerhebung und Datenverarbeitung, bestimmen aber gleichzeitig die Grenzen dieser Befugnisse. Sie stellen damit – so widersprüchlich das klingen mag - auch Datenschutzvorschriften dar.

Es gehört zu den Aufgaben des Datenschutzbeauftragten, auch über deren Einhaltung zu wachen.

Waren diese Gesetze zu einseitig am Datenschutz orientiert? Ich sage nein!

Diese Bestimmungen ermöglichten schon vor dem 11. September 2001 eine umfangreiche Zusammenarbeit der verschiedenen Dienste. Es war einfach nicht wahr, dass die Datenschutznormen eine effektive Zusammenarbeit der Sicherheitsbehörden verhindert hätten.

Der Verfassungsschutz konnte Daten an die Polizei übermitteln und umgekehrt; die Ausländer- und Asylbehörden konnten in Kontakt mit den Nachrichtendiensten und der Polizei treten.

Es war deswegen sehr bedrückend, dass der "Datenschutz" umgehend zum Sündenbock für Mängel bei der Terrorismusbekämpfung gemacht wurde mit Sätzen wie "die Datenschutzvorschriften müssen jetzt insgesamt auf den Prüfstand" und "Es muss auch über den Datenschutz grundsätzlich nachgedacht werden"

Mit dieser Formulierung wurde tiefgehendes Misstrauen gegenüber dem Datenschutz zum Ausdruck gebracht, wenn nicht sogar eine grundsätzliche Ablehnung.

Diese Auffassungen sind unberechtigt und sie sind gefährlich: Sie sind unberechtigt, weil Datenschutz auch schon bisher die Datenverarbeitung im Sicherheitsbereich nicht verhindert hat.

Die Forderung nach *"grundsätzlichem Nachdenken über den Datenschutz"* ist aber auch gefährlich: Sie geht an den Kern des Grundrechts. Sie birgt die Gefahr, dass das Grundrecht auf informationelle Selbstbestimmung als beliebig fungible Größe angesehen wird, die ebenso beliebig eingeschränkt werden kann.

Diese Möglichkeit besteht nicht: Grundrechte dürfen in ihrem Kern nicht angetastet werden.

Nach dem 11. September 2001 begann eine hektische Gesetzgebungsarbeit. Innerhalb weniger Monate wurden zwei Gesetzgebungspakete verabschiedet, bekannt unter dem Namen "Otto – Katalog I" und "Otto-Katalog II" . Wir Datenschutzbeauftragten hatten uns intensiv in die Diskussion eingeschaltet.

Wir haben uns erfolgreich dafür eingesetzt, dass in die neuen Vorschriften sachliche Begrenzungen, verfahrensmäßige Sicherungen und zeitliche Limitierungen und damit rechtsstaatliche Sicherungen eingebaut wurden. Sie ermöglichen einen sachgerechten Ausgleich zwischen den Interessen der Sicherheitsbehörden und der Gewährleistung der Bürgerrechte.

Dieser Ausgleich ist notwendig. Klare Beschreibungen und Begrenzungen von Eingriffsbefugnissen in Grundrechte sind erforderlich. Von den Auskunfts- und Ermittlungsbefugnissen der Sicherheitsbehörden kann jeder Bürger betroffen sein, nicht nur Gangster und Terroristen.

Was sind das nun für Befugnisse, was ist daran neu?

Ausdrücklich ist nunmehr bestimmt, dass die Verfassungsschutzbehörden von Fluggesellschaften und Finanzdienstleistern Auskünfte einholen können.

Hierin sehe ich nichts sensationell neues, weil die Verfassungsschutzbehörden dieses Recht auch bisher schon hatten und zwar durch die allgemeine Datenerhebungsbefugnis zur

Erfüllung ihrer Aufgaben. Durch die nunmehrige ausdrückliche und konkrete Regelung wird diese Berechtigung aber sozusagen verdichtet, sie wird verdeutlicht.

Weiter wurden Auskunftsbefugnisse gegenüber Post – Telekommunikations- – und Teledienstunternehmen geschaffen, die es in dieser Form bisher nicht gab.

Bisher konnten die Verfassungsschutzbehörden des Bundes und der Länder allein nach dem Gesetz zur Ausführung von Art. 10 Grundgesetz, dem sogenannten G-10 Gesetz, Telekommunikationsvorgänge abhören und aufzuzeichnen; das aber nur für die Zukunft. Regelungen in Bezug auf die Vergangenheit und in Bezug auf Teledienstunternehmen, also z.B. Anbieter von Internetdienstleistungen, gab es bisher nicht.

Nach dem neuen Recht sind solche Eingriffe durch die Verfassungsschutzbehörden nunmehr auch gegenüber Teledienstunternehmen und für die Vergangenheit möglich.

Insoweit enthält das Terrorismusbekämpfungsgesetz zusätzliche Eingriffe in das Grundrecht aus Art. 10 Grundgesetz, das Post und Telekommunikationsgeheimnis.

Diese neuen Befugnisse stehen aber ebenfalls unter den strengen Voraussetzungen des G-10 Gesetzes – Verhinderung von bestimmten schweren Straftaten - und unter Schutzmechanismen durch Verfahren, die ebenfalls an die Modelle des G-10-Gesetzes angelehnt sind:

Der Präsident des BfV oder sein Vertreter muss einen schriftlichen Antrag stellen, das Ministerium muss entscheiden; die G-10-Kommission ist grundsätzlich vor der Maßnahme zu unterrichten; sie überprüft die Berechtigung der Maßnahme, diese ist bei negativem Votum der G-10-Kommission aufzuheben.

Es besteht die Verpflichtung, die parlamentarische Kontrollkommission mindestens halbjährlich zu unterrichten; schließlich ist ein jährlicher und nach drei Jahren ein zusammenfassender Bericht dieser Kommission an den Bundestag vorgesehen. Dadurch soll im Lichte der Erfahrungen die Notwendigkeit der Bestimmungen überprüft werden.

Schließlich berechtigt das Gesetz nunmehr auch den Verfassungsschutz, den sogenannten IMSI-Catcher einzusetzen. Mit diesem Gerät können die Karten- und die Gerätenummer, aber auch der Standort eines Mobiltelephons festgestellt werden.

Die Strafprozessordnung ermöglicht schon bisher den Einsatz dieser Geräte zur Strafverfolgung, allerdings ohne Beachtung des Zitiergebots des Grundgesetzes. Danach hätte das eingeschränkte Grundrecht in der Strafprozessordnung genannt werden müssen.

Das neue Gesetz sieht nunmehr den Einsatz des IMSI-Catchers auch durch die Verfassungsschutzbehörden vor. Im Gegensatz zur Strafprozessordnung wird hier das Zitiergebot beachtet.

Es werden die gleichen Voraussetzungen wie in dem G-10-Gesetz verlangt, es muss die Gefahr bestimmter schwerer Straftaten bestehen und der IMSI-Catcher darf nur als letztes Mittel eingesetzt werden, nur wenn die Ermittlungen sonst aussichtslos oder wesentlich erschwert wären.

Das Gesetz legt weiter ein absolutes Verwendungsverbot für Randerkenntnisse über Nichtbetroffene fest, sowie ebenfalls die Schutz- und Kontrollmechanismen Präsidentenantrag und Ministeriumsentscheidung.

Die neuen Befugnisse sind auf 5 Jahre befristet.

Im Pass- und Personalausweisgesetz wurde die grundsätzliche Möglichkeit aufgenommen, dass die Ausweise neben Unterschrift und Bildern auch weitere biometrische Merkmale von Fingern, Händen und Gesicht enthalten dürfen. Die Merkmale dürfen nur zur Identifizierung benutzt werden. Die Speicherung in einer bundesweiten Date ist ausgeschlossen.

Wie sehe ich das alles nun als Datenschützer?

Der Gesetzesbeschluss zum Terrorismusbekämpfungsgesetz war der Abschluss einer intensiven Diskussion von ursprünglichen Absichten und Vorhaben des

Bundesinnenministeriums. Wir Datenschutzbeauftragten hatten uns unter der Federführung des Bundesbeauftragten für den Datenschutz intensiv in diese Diskussion eingeschaltet.

Die ursprünglichen Vorstellungen des Bundesinnenministeriums gingen in Teilbereichen wesentlich über das hinaus, was schließlich Gesetz geworden ist. Die Begrenzungen und die Schutz- und Kontrollmechanismen beruhen wesentlich auf unseren Vorschlägen.

Ich sehe die konkretisierten Auskunftsbefugnisse im Hinblick auf die gesetzlichen Begrenzungen, die vorgesehenen Schutzmechanismen sowie die zeitliche Limitierung als durchaus vertretbar an.

Neue Erhebungsbefugnisse gegenüber Post, Telekommunikations- und Teledienstunternehmen halte ich dagegen grundsätzlich für problematisch. Sie greifen in den Schutzbereich von Art. 10 Grundgesetz ein.

Im Hinblick auf die Bedrohungssituation und wegen der gesetzlichen Eingrenzungen und Schutzmechanismen des G-10-Gesetzes, halte ich aber diese Befugnisse aus Datenschutzsicht für ebenfalls hinnehmbar.

Ihre Auswirkungen auf nicht Betroffene und ihre Effektivität müssen aber genau beobachtet werden. Hier kommt der vorgeschriebenen Berichterstattung an den Dt. Bundestag eine besondere Bedeutung zu.

Die Verwendung des IMSI-Catchers wird von den Datenschutzbeauftragten wegen der unvermeidbaren Betroffenheit Dritter ebenfalls grundsätzlich als problematisch angesehen. Ich begrüße es deshalb ausdrücklich, dass hinsichtlich der unvermeidbaren Randerkenntnisse über nicht Betroffene eine sofortige Verpflichtung zur Löschung und ein absolutes Verwendungsverbot vorgesehen ist.

Heftig diskutiert wurden die biometrischen Merkmale in den Ausweisen. Das Ausführungsgesetz gibt es noch nicht. Für mich wesentlich ist der von uns geforderte Ausschluss der bundesweiten Zentraldatei und die klare Zweckbegrenzung auf die Erleichterung der Identifizierung.

Ich kann deshalb feststellen, dass in den Sicherheitsgesetzen nach dem 11. September wesentliche Forderungen von Seiten der Datenschützer nach Begrenzungen und Schutzmechanismen berücksichtigt wurden.

Was ich gleichwohl befürchte, ist das schrittweise Abgehen von diesen Begrenzungen, ist eine gewisse Salamitaktik, mit der immer noch ein Schritt in eine weitere Überwachung im Vorfeld von Straftaten gegangen wird.

Die Berechtigung dieser Befürchtungen zeigen jüngste Überlegungen in Bayern zur Einführung einer eigenen Telephonüberwachungsbefugnis für die Polizei.

Die Polizei konnte schon bisher zur Strafverfolgung unter der Leitung der Staatsanwaltschaft unter bestimmten Voraussetzungen Telephone abhören. Nunmehr soll die Polizei in Bayern Telephone auch zur Verhinderung von Straftaten abhören können.

Man könnte nun sagen, "ja und, das ist doch gut so". Aber so einfach sind die Dinge nicht. Anders als beim Abhören zur Strafverfolgung gibt es keinen feststehenden Anlass – wie eine bereits begangene Straftat. Es gibt vielmehr nur Vermutungen und Befürchtungen. Es ist auch nicht so, dass nur der zukünftige Straftäter abgehört werden soll. Auch das Umfeld, ja auch nur weitläufige Bekannte können davon betroffen sein.

Andererseits zeigt das Beispiel auch die Komplexität der Aufgabe des Datenschutzes: Es gibt durchaus auch Gründe, die für die Einführung dieser neuen Möglichkeit sprechen: Die Polizei hört aus zuverlässiger Quelle, dass eine schwere Straftat geplant ist, die Planung selbst ist aber noch keine Straftat, auch fällt der Vorgang nicht unter den Tatbestand der Strafbarkeit der Nichtanzeige bestimmter Straftaten.

Soll sie mit dem Aufklärungsmittel der Telephonüberwachung warten müssen, bis die Straftat begangen wird? Ich meine Nein.

Notwendig ist aber, dass solchen Befugnissen klare Grenzen gezogen werden.

Notwendig ist auch, dass im Hinblick auf die Schwere des Grundrechtseingriffs die Befugnisse immer auch verhältnismäßig sind. Sie dürfen deswegen nur zur Verhinderung

bestimmter schwerer Straftaten in Betracht kommen. Es dürfen auch nicht nur bloße Vermutungen und Befürchtungen bestehen, sondern es müssen bestimmte Tatsachen sein, die für die bevorstehende schwere Straftat sprechen.

In diesem Sinn hatte ich mich zu dem Gesetzentwurf der CSU-Fraktion im Bayerischen Landtag geäußert. Dieser ist bekanntlich inzwischen zurückgezogen worden.

Mit Befriedigung habe ich einer Pressemitteilung des Innenministeriums entnommen, dass Innenminister Beckstein diese Forderungen nunmehr aufgreifen will.

Nach der Sommerpause wird über einen neuen Gesetzentwurf noch intensiv diskutiert werden müssen. In diese Diskussion werden auch die vielfältigen Anregungen einfließen, die in der kürzlichen Anhörung vor dem Bayerischen Landtag, z.B. von der Deutschen Polizeigewerkschaft, erhoben wurden. Auch die Deutsche Polizeigewerkschaft hielt den Entwurf für zu weitgehend.

Meine sehr verehrten Damen und Herren, Hohe Festversammlung, ich durfte Ihnen einige wesentliche Punkte meines Arbeitsbereichs vorstellen.

Mein Bestreben ist es einen Beitrag zur Wahrung der Bürgerrechte auf Privatheit zu leisten. Ich möchte verdeutlichen, dass auch im Sicherheitsbereich Datenschutz Grundrechtsschutz ist.

Wichtig ist es das richtige Maß zu finden. Die Leitlinie muss lauten Sicherheit und Effektivität ja, aber nur nach Maßgabe der Grundrechte. Hier die Stimme zu erheben, ist Aufgabe der Datenschutzbeauftragten.
Benjamin Franklin hat gesagt:

"Wer bereit ist, grundlegende Freiheiten aufzugeben, um sich kurzfristig Sicherheit zu schaffen, der hat weder Freiheit noch Sicherheit verdient".

Bedenken wir diese Mahnung.

Ich danke Ihnen für Ihre Aufmerksamkeit

Reinhard Vetter, Fassung 18.07.03