

PRESSEINFORMATION

Kiel, den 22.01.2003

Silke Hinrichsen

Es gilt das gesprochene Wort

„Wir müssen heute die nötige Distanz haben, um die Sicherheitsmaßnahmen nach dem 11. September einer neuerlichen Bewertung zu unterziehen.“

TOP 8 Datenschutzpolitik in Schleswig-Holstein (Drs. 15/2287)

In Schleswig-Holstein lässt es sich gut leben. Das gilt auch – und nicht zuletzt – für den Datenschutz. Sollte es denn noch eines Beweises bedurft haben, so zeigt die Antwort der Landesregierung auf die Große Anfrage zur Datenschutzpolitik in Schleswig-Holstein, dass unsere Bürgerinnen und Bürger sich hier auf den Staat verlassen können. Er sorgt soweit möglich dafür, dass ihre Persönlichkeitsrechte gewahrt bleiben und er zeigt auf, dass Datenschutz nicht im Widerspruch zur modernen Kommunikationsgesellschaft und zur inneren Sicherheit stehen muss.

Je mehr wir uns in allen Bereichen des Lebens auf datenverarbeitende Technologien einlassen desto wichtiger wird der Blick auf die persönlichen Daten des Einzelnen. Wir alle hinterlassen täglich Datenspuren und wir müssen uns darauf verlassen können, dass diese vertraulich behandelt werden - und schon gar nicht in die Hände von Unbefugten geraten.

Das gilt natürlich insbesondere für den Bereich der Sicherheitsbehörden, die ja gerade das Ziel haben, vertrauliche Informationen zu gewinnen und auszuwerten. Dies ist insbesondere nach den Attentaten vom 11. September 2001 deutlich geworden, wo der Schutz der Grundrechte des Einzelnen gegenüber den politisch bestimmten Sicherheitsbedürfnissen der Bevölkerung noch einmal deutlich an Gewicht verloren hat.

Es ist klar, dass direkt nach dem 11. September die Vorschläge zur Änderung der Gesetze durch dieses erschütternde Erlebnis geprägt waren. Allerdings müssen wir heute auch die nötige Distanz haben, um diese Vorschläge einer neuerlichen Bewertung zu unterziehen. Sicherlich hat die Landesregierung Recht, wenn sie sagt, dass die Sicherheitslage heute nach wie vor angespannt ist. Es muss aber trotzdem erlaubt sein, Fragen zu stellen. Wenn die Presseberichte wirklich zutreffen, wonach mehrere der Täter des 11. September schon lange davor vom Verfassungsschutz beobachtet wurden, dann frage ich mich schon: Sind die Voraussetzungen für die Rasterfahndung heute noch gegeben? Wir haben diesem Instrument im Herbst 2001 nur deshalb zugestimmt, weil damit die terroristischen „Schläfer“ aufgedeckt werden sollten, die bisher keiner gesehen hatte. Mit der Rasterfahndung geraten aber auch viele unbescholtene Menschen ins Visier der Sicherheitsbehörden. Deshalb muss sie auch etwas leisten, was wir mit anderen Mitteln nicht erreichen können. Wenn der Verfassungsschutz die Schläfer selber finden kann, dann brauchen wir nicht die Risiken und Nebenwirkungen der Rasterfahndung in Kauf zu nehmen. Denn am Ende der Rasterung steht ja auch nur die Überwachung durch die Sicherheitsbehörden.

Zusammenfassend möchte ich für den Bereich der inneren Sicherheit feststellen: In Verbindung mit der ausgiebige Darstellung der Sicherheitspolitik nach dem 11. September vermischen wir eine ebenso detaillierte Bewertung der datenschutz-relevanten Aspekte der IMK-Beschlüsse. Es scheint fast, als hätte sogar diese Landesregierung trotz gegenteiliger Bekundungen nach dem 11. September den Datenschutz etwas aus den Augen verloren.

In einer Reihe von Bereichen teilen wir die Auffassung der Landesregierung und begrüßen ihr konsequentes Engagement für den Datenschutz. Das gilt zum Beispiel für die Positionen, dass ein Lauschangriff ausschließlich auf Anordnung eines Richters möglich sein sollte oder dass Daten nur in Drittländer mit einem Mindestmaß an Datenschutz weitergegeben werden sollten. In anderen Bereichen sehen wir die Standpunkte aber etwas skeptischer und würden im Ausschuss gern noch mit der Landesregierung über Details sprechen - zum Beispiel was die

Praxis der nachträglichen Aufklärung von abgehörten Personen oder die Notwendigkeit einer richterlichen Anordnung bei der Speicherung von DNA-Profilen in der Gen-Datei betrifft.

Mann muss aber gar nicht ins Visier der Sicherheitsbehörden geraten, damit tief in die Privatsphäre eingedrungen wird. Denn häufig liegt es in unserem eigenen Interesse, unsere intimsten Daten herzugeben. Wer zum Arzt geht will eine optimale, individuelle Behandlung, die ohne persönliche Daten gar nicht möglich ist. In Zukunft sollen diese Daten einem weit größeren Kreis von Menschen zur Verfügung stehen, um eine noch optimalere medizinische Versorgung zu gewährleisten. Dagegen kann auch gewiss niemand etwas einzuwenden haben. Es dient schließlich nur zu unserem Vorteil, wenn die Anbieter des Gesundheitswesens mit Computern vernetzt werden und über eine persönliche Chipkarte einen schnellen Zugriff auf wichtige – manchmal sogar lebenswichtige – Daten haben. Uns bleiben Doppeluntersuchungen erspart, die sinnlose Medikamentengabe wird verhindert und bei der Notfallkarte können die wichtigsten Daten des Patienten sofort abgerufen werden. In Flensburg läuft zur Zeit ein Modellversuch mit dem Ziel, Erfahrungen zu gewinnen. Es wird untersucht, wie im Netzwerk elektronische Krankenakten und Notfall-Chipkarten sinnvoll genutzt werden können.

Aber auch wenn die Ziele durchweg gut sind: Auch im Gesundheitsbereich ist ein Missbrauch nicht ausgeschlossen. Es können persönliche Daten gespeichert werden, die für die Behandlung nicht relevant sind oder relevante Daten können in falsche Hände geraten. Dieses intime Wissen ist für viele Menschen abrufbar, ohne dass der Patient immer darüber entscheiden kann, ob er diese Daten weitergeben möchte. Schon bei einer Notfallkarte mit den wichtigsten Daten streiten sich die Gelehrten darüber, was gespeichert werden muss. Außerdem gibt es noch keinen internationalen Standard für derartige Systeme, so dass die Vorteile einer solchen Karte nur in einem Land bestünden. Hier wären Überlegungen und Vereinbarungen im europäischen Raum hilfreich, damit nicht jeder alleine für sich damit arbeitet.

Man muss aber gar nicht die Zukunftsvisionen für das Gesundheitswesen bemühen, um die Datenschutz-Probleme im Gesundheitswesen zu erkennen. Bereits die jetzigen Daten geben schon genügend Möglichkeit zum Missbrauch, wie aktuelle Fälle zeigen. Zum einen bieten die Krankenversichertenkarten keinerlei Schutz. Zwar haben die Lesegeräte und die elektronische Datenverarbeitung einen Datenschutz-Standard, aber ein PC-Programm reicht schon aus, um die heutigen Sicherungsmaßnahmen zu umgehen. Die aktuellen Skandale um gefälschte Ärzte-Abrechnungen machen auch deutlich, dass die beste Technik nicht ausreichend ist, wenn die zuständigen Stellen im datenschutzrechtlichen Dornröschenschlaf schlummern oder sogar wegsehen. Kein Patient wird wohl freiwillig eine noch umfassendere Chipkarte nutzen wollen, wenn die Kontrollinstanzen Auffälligkeiten einfach ignorieren. Technische Maßnahmen allein werden kaum das notwendige Vertrauen schaffen können.

Vertrauen ist ein Schlüsselwort, wenn es um Daten geht. Das gilt nicht nur für das Glauben darin, dass der Staat personenbezogene Informationen schützt. Um dieses Vertrauen zu gewinnen, muss der Staat auch offen mit den anderen Daten umgehen, die ihm zur Verfügung stehen. Deshalb freut es uns natürlich, dass die Landesregierung mittlerweile erkannt hat, wie fortschrittlich das Informationsfreiheitsgesetz ist, dem sie ja noch vor einigen Jahren nicht ganz so aufgeschlossen gegenüber stand.

Um Vertrauen zu schaffen brauchen wir auch endlich ein Verbraucherinformationsgesetz. Es entbehrt wirklich nicht einer gewissen Ironie: Diejenigen, die immer eine freie Marktwirtschaft predigen, wehren sich mit Händen und Füßen dagegen. Zu einem freien Markt gehören aber auch aufgeklärte Verbraucher, die eine gut informierte Kaufentscheidung treffen. Es ist schon verwunderlich, dass die Wirtschaft so wenig Vertrauen in ihre eigenen Produkte hat, dass sie sich einer Stärkung der Verbraucherinnen und Verbraucher so vehement widersetzt.