

**Parlamentarischer  
Geschäftsführer  
Heinz Maurus**

Landeshaus  
24100 Kiel  
Telefon 0431-988-1440  
Telefax 0431-988-1444  
Internet: <http://www.cdu.ltsh.de>  
e-mail: [info@cdu.ltsh.de](mailto:info@cdu.ltsh.de)

## **PRESSEMITTEILUNG**

**Nr. 24/03 vom 22. Januar 2003**

Innenpolitik

### **TOP 8**

## **Thorsten Geißler: Individuelle Entfaltungschancen des Einzelnen dürfen nicht beeinträchtigt werden Datenschutz deshalb weiter wichtige Aufgabe**

Mit dem Landesdatenschutzgesetz, das am 1. Juni 2000 in Kraft getreten ist und in diesem Hohen Hause einstimmig beschlossen wurde, verfügt das Land Schleswig-Holstein über eine Rechtsvorschrift, mit der nicht nur die europäische Datenschutzrichtlinie umgesetzt wurde, sondern die auch gewährleistet, dass das Grundrecht auf informationelle Selbstbestimmung in Schleswig-Holstein verwirklicht wird.

Die gesetzliche Verpflichtung der Behörden zur Datenvermeidung und Datensparsamkeit, die Privilegierung der Verarbeitung anonymisierter oder pseudonymisierter Daten, die Förderung datenschutzfreundlicher Produkte sowie die Verschlüsselung von Daten bei einer Bearbeitung aus der Dienststelle seien dazu beispielhaft genannt.

Bewährt hat sich auch die Service- und Beratungstätigkeit des Unabhängigen Landeszentrums für Datenschutz. Dessen jährliche Berichte zeigen zwar immer auch wieder Verstöße gegen datenschutzrechtliche Bestimmungen auf. Zugleich wird aber deutlich, dass immer mehr Behörden und teilweise auch nicht-öffentliche Stellen sensibel sind gegenüber den Belangen des Datenschutzes.

Diese Berichte werden in Fachausschüssen des Landtages stets sehr sorgfältig beraten. Es wäre aus meiner Sicht aus wünschenswert, den Bericht auch – so wie es früher üblich war – im Plenum zu diskutieren.

Bewährt hat sich die Zusammenlegung der Aufsicht für den öffentlichen und nicht-öffentlichen Bereich. Die damit einhergehende Bündelung ermöglicht eine effektive Aufgabenerledigung durch das ULD.

Ebenso richtig war die Einführung eines Datenschutzaudits. Es ist ein wirksames Instrument zur Verbesserung des Datenschutzes und das die Datensicherheit. Erst vor wenigen Tagen wurden dem Herrn Landtagspräsidenten die Urkunden des ULD über die Auditierung des über das Parlanet bereitgestellten Informationsangebots und des sorgsamem Umgangs mit Petitionsdaten. Diese Auditierung wurde vorgenommen aufgrund einer Anregung des Datenschutzgremiums des Landtages, und ich glaube, wir haben alle Anlass zur Freude, wenn der Landesdatenschutzbeauftragte, Herr Dr. Bäumler, in einer Presseerklärung dazu vorgestellt hat, dass der Landtag in Sachen Datenschutz eine Vorbildstellung nicht nur unter den öffentlichen Stellen, sondern auch gegenüber privaten Anbietern hat.

Dennoch – die Antwort der Landesregierung auf die Große Anfrage der SPD-Fraktion macht dies deutlich, gibt es im Bereich der Datenschutzpolitik einige große Problembereiche, von denen auch Schleswig-Holstein betroffen ist. Der Bundesgeber hat sich mit seiner weit verspäteten Umsetzung der EU-Datenschutzrichtlinie alles andere als vorbildlich verhalten. Auch ist das neue Bundesdatenschutzgesetz an einigen Stellen wenig übersichtlich und wenig anwenderfreundlich. Probleme ergeben sich insbesondere auch bei den Regelungen für die Übermittlung personenbezogener Daten ins Ausland. Auch in der globalen Informations- und Kommunikationsgesellschaft muss es beim internationalen Datentransfer Standards für Datenschutz und Datensicherheit geben. Dies gilt gerade auch, weil im Interesse einer effektiven Kriminalitätsbekämpfung die Übermittlung sensibler Daten alltägliche Praxis ist. Unzureichende Datensicherheit, die den unberechtigten Zugriff auf alle Daten ermöglicht, beeinträchtigt nicht nur das Grundrecht auf informationelle Selbstbestimmung, sie gefährdet auch die Erfolgsaussichten bei der Bekämpfung dieser Kriminalität.

Die Erweiterung der Europäischen Union wird ein angemessenes Datenschutzniveau auch in denjenigen Beitrittsländern gewährleisten, die anders als beispielsweise Ungarn in diesem Bereich derzeit noch Defizite aufweisen. Probleme ergeben sich aber bei der Übermittlung personenbezogener Daten in Nicht-EU-Länder. Hier werden weitere internationale Vereinbarungen erforderlich sein.

Dies gilt gerade auch im Zeitalter globaler terroristischer Bedrohung. Spannungsfelder zwischen einzelnen Grundrechten oder zwischen Grundrechten und einer effektiven polizeilichen Kriminalitätsbekämpfung und der Abwehr terroristischer und anderer Gefahren sind nicht Ungewöhnliches. Die angemessene Antwort eines freiheitlichen und demokratischen Staates ist nicht die Abschaffung oder Aushöhlung von Grundrechten, auch nicht des Grundrechts auf informationelle Selbstbestimmung, sondern es gilt, im Wege der praktischen Konkordanz Lösungen zu finden, die sowohl einen effektiven Grundrechtsschutz als auch eine effektive Kriminalitätsbekämpfung und Abwehr terroristischer Gefahren ermöglichen.

Unser Gefahrenabwehrrecht kennt eine Reihe verdeckter Datenerhebungsmittel, die sich – hier teile ich die Einschätzung der Landesregierung – positiv bewährt haben.

Zu meiner Überraschung habe ich auf Seite 29 der Antwort gelesen, dass die Landesregierung zu den besonderen Mitteln der Datenerhebung nach dem Landesverwaltungsgesetz auch den Einsatz verdeckter Ermittler zählt. Ich darf darauf aufmerksam machen, dass unser Landesverwaltungsgesetz verdeckte Ermittler überhaupt nicht vorsieht. Richtig ist, dass meine Fraktion die Aufnahme einer entsprechenden Bestimmung immer gefordert hat. Sollte sich hinter der Formulierung die Ankündigung einer Gesetzesinitiative verbergen, haben Sie, Herr Minister, die Unterstützung der CDU-Fraktion.

Wenn verdeckte Datenerhebungsmittel nicht nur aufgrund des hohen Personal- und Zeitaufwandes nicht massenhaft durchgeführt werden, so - und auch hier teile ich die Einschätzung der Landesregierung – kann damit nicht auch auf die Entbehrlichkeit dieser Instrumente geschlossen werden. Gleiches aber gilt auch für die akustische Wohnraumüberwachung gemäß Artikel 13 Absatz 3 Grundgesetz bzw. § 110 Absatz 1 Nummer 3 der Strafprozessordnung. Auch hier gilt, dass die verhältnismäßig geringe Anzahl durchgeführter Maßnahmen nicht die Entbehrlichkeit dieses Instrumentes belegt, sondern vielmehr den verantwortungsvollen Umgang der Behörden mit diesem sensiblen Eingriffsrecht.

Der Bericht des Innenministers über erste Erfahrungen mit der sogenannten Rasterfahndung zeigt auch, dass dieses Instrument erforderlich war. Meine Fraktion hatte es lange vorher angemahnt und das beschlossene Gesetz zeigt, dass es durchaus möglich ist, effektive Kriminalitätsbekämpfung und effektiven Datenschutz miteinander zu vereinbaren.

Pragmatische Lösungen sind auch gefordert im Bereich des Einsatzes von Videotechnik an Kriminalitätsbrennpunkten. Um es klar zu stellen: Niemand möchte britische Verhältnisse. In London beispielsweise wird ein Passant mindestens alle 5 Minuten von einer Kamera erfasst. Mit Hilfe der Vernetzung kann die Polizei Bewegungsbilder auch sich rechtstreuverhaltender Personen erstellen.

Wenn aber auch die Landesregierung es für erforderlich hält, am Flensburger ZOB als einem erkannten Gefahren- bzw. Deliktsschwerpunkt eine offene Videoüberwachung durchzuführen, so zeigt das, dass dies Instrument im Einzelfall durchaus geeignet sein kann, zur Prävention, aber auch zur Aufklärung begangener Straftaten eingesetzt zu werden.

Es ist bemerkenswert, dass die Landesregierung nun einen Beschluss der Innenministerkonferenz vom 5. Mai 2000, der genau dies feststellt, nunmehr uneingeschränkt unterstützt.

Lassen Sie mich zu einigen weiteren rechtspolitischen Fragen Stellung beziehen.

1. Ich halte das DNA-Identitätsfeststellungsgesetz vom 7. September 1998 für novellierungsbedürftig, gerade angesichts immer wieder vorkommender, das Sicherheitsgefühl der Bevölkerung zutiefst beeinträchtigenden und schwere Sexualstraftaten wäre dies dringend erforderlich. Ich verweise auf eine entsprechende Initiative meiner Fraktion.
2. Durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 wurde der Einsatz von biometrischen Merkmalen in verschiedenen Bereichen ermöglicht. Ich teile die Auffassung der Landesregierung, dass die Verwendung biometrischer Verfahren eine geeignete Möglichkeit zur Überprüfung der Authentizität von Dokumenten und zur Identitätsfeststellung von Personen darstellt.

Richtig ist andererseits auch, dass es datenschutzrechtliche Risiken gibt etwa durch die mögliche Manipulation der Merkmale oder deren missbräuchliche Verwendung. Sicher zu stellen ist auch, dass biometrische Merkmale nicht für gänzlich andere Zwecke verwendet werden, als die soeben dargestellten. Dies wäre datenschutzpolitisch in ebenso hohem Maße bedenklich wie eine Speicherung, die es ermöglichen würde, detaillierte Bewegungsbilder sich völlig

rechtstreu verhaltener Bürgerinnen und Bürger zu erstellen.

3. Die Antwort der Landesregierung geht in einem Abschnitt auch auf das Stichwort „Internet“ ein. Ich möchte darauf, weil dieses Thema erhebliche datenschutzrechtliche Fragen berührt, an dieser Stelle eingehen. Das Internet erleichtert nicht nur zahlreiche Arbeitsabläufe, es ermöglicht auch breitesten Bevölkerungsschichten, sich frei und uneingeschränkt und auch grenzüberschreitend über die unterschiedlichsten Probleme zu informieren und sich damit auch die Grundlagen zu verschaffen, an politischen Entscheidungsprozessen partizipieren zu können. Das Internet ist der Alptraum jedes Diktators oder autoritären Staatslenkers.

Aber das Internet wird auch missbraucht von Terroristen, die es nutzen, um ihre Anschläge vorzubereiten, von Rechts- und Linksextremisten, aber auch von Menschen, die mit Kinderpornographie oder anderer Form sexueller Ausbeutung Handel treiben.

Die Bekämpfung solcher Kriminalitätsphänomene wird wesentlich dadurch erschwert, dass sich die Strafverfolgungsbehörden stets an neue technische Entwicklungen anpassen müssen. Es gilt der Grundsatz, dass die Strafverfolgungsbehörden in rechtlicher, technischer und personeller Hinsicht in die Lage versetzt werden müssen, ihrem staatlichen Strafverfolgungsauftrag gerade auch im Hinblick auf die Internet-Kriminalität nachkommen zu können. Die beispielsweise von der Zentralstelle zur anlaßunabhängigen Recherche in Datennetzen im Bundeskriminalamt deliktübergreifend durchgeführten Recherche in allen Internetdiensten sind geeignet, entsprechend strafbare Inhalte im Internet zu erkennen. Gleiches gilt für entsprechende Dienststellen in einzelnen Bundesländern. Schleswig-Holstein nimmt hier bedauerlicherweise alles andere als eine Spitzenstellung ein. Gleichzeitig ist es aber erforderlich, eine Überwachung unverdächtiger, sich vollkommen rechtstreu verhaltender Bürger zu vermeiden. Es ginge ein gutes Stück an Unbefangenheit verloren, wenn auch der rechtstreu Bürger in dem Bewusstsein leben müsste, dass die Internetseiten, die er aufruft, protokolliert werden und dass aus dem Nachvollziehen seines Surfverhaltens Rückschlüsse gezogen werden könnten in Hinblick auf seine politischen Ansichten, seine Konsumgewohnheiten, sein Gesundheitszustand, sein Intimverhalten und über zahlreiche andere Dinge, die der Privatsphäre zuzuordnen sind.

Nicht zuletzt deshalb hat sich daher auch der Innenausschuss unseres Landtages im Januar 2001 nachdrücklich gegen die Einführung einer entsprechenden Speicherverpflichtung für Internet-Serviceprovider ausgesprochen.

Dabei bin ich mir darüber im klaren, dass Gefahren für das Recht auf Anonymität heute in erster Linie von denjenigen ausgehen, die durch das Nutzen vorhandenen technischen Möglichkeiten versuchen, gezielt Persönlichkeitsprofile von Internetnutzern anzulegen, um sie für eigene wirtschaftliche Zwecke zu nützen oder sie an andere zu verkaufen, also nicht vom öffentlichen Sektor.

Wichtig ist die Aufklärung über Schutzmöglichkeiten. Wichtig ist ebenfalls die Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmung auch im Bereich der privaten Wirtschaft. Im Volkszählungsurteil von 1993 heißt es: Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa

die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf einer Ausübung seiner entsprechenden Grundrechte verzichten.

Man könnte auch formulieren: Wer sicher ist, dass abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergeben werden wird, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer weiß, dass sein Internetsurfverhalten behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten. Wir werden dies zu berücksichtigen haben, wenn wir vor Entscheidungen stehen, die dazu führen sollen, dass unsere Bürger in Sicherheit und ohne Furcht vor Kriminalität leben können und damit auch in Freiheit von Kriminalitätsfurcht leben können. Dabei werden wir auch sicherstellen müssen, dass wir keine Entscheidungen treffen, die, wie es das Bundesverfassungsgericht formuliert hat, nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.