

Sabine Leutheusser-Schnarrenberger, MdB

„Vertrauensschutz – Datensicherheit – informationelle
Selbstbestimmung: das Arzt-Patienten-Verhältnis im Zeitalter
der Informationstechnologie“

Impulsreferat

Berlin, den 14.11.2008

Es gilt das gesprochene Wort

Anrede,

ich freue mich, heute das Impulsreferat auf Ihrer Bundeshauptversammlung halten zu dürfen.

Kein Zweifel: Die Bedeutung des Schutzes der Privatsphäre, der Vertraulichkeit der Kommunikation und des informationellen Selbstbestimmungsrechts werden von immer mehr Menschen geschätzt.

Dazu haben leider gerade negative Ereignisse beigetragen, wie die in der breiten Öffentlichkeit berichteten Datenmissbräuche im nicht-öffentlichen Bereich, der Verlust von Millionen Sozialdaten in Großbritannien, der Fund von Datenträgern mit höchstpersönlichen Daten. Das alles hat sehr viel mehr Bürgerinnen und Bürger wachsam und bewusster gemacht.

Eine aktuelle Entscheidung des Bundestages in dieser Woche hat leider diese berechtigten Befindlichkeiten nicht berücksichtigt. Der Bundestag hat diese Woche den Umbau des Bundeskriminalamtes zu einer Art deutschem FBI beschlossen – trotz heftigen Widerstandes.

Mit dem Gesetz erhält das BKA neue Aufgaben und neue Befugnisse, die weit im Vorfeld terroristischer Bedrohungen liegen. Als Beispiel darf ich nur die weit gefasste polizeiliche Rasterfahndung, die präventive Telefonüberwachung und die optische und akustische Überwachung von Wohnungen sowie die heimliche Online-Durchsuchung nennen. Das Bundeskriminalamt bekommt damit Befugnisse, die in dieser Konzentration nicht den Landespolizeibehörden zustehen, die bisher richtigerweise vorwiegend die Gefahrenabwehr als ihre Aufgabe wahrgenommen haben.

Dass diese neue Konstruktion der Sicherheitsarchitektur installiert wird, stößt auf weiteren heftigen Widerstand der FDP in Bund und Ländern. Wir behalten uns auch eine umfassende verfassungsrechtliche Prüfung vor, weil durch die Neuregelung des BKA vielfach rechtsstaatliche Prinzipien verletzt werden – nicht nur bei der heimlichen Online-Durchsuchung.

Es gibt keine Notwendigkeit, die bisher funktionierende Sicherheitsarchitektur ohne Not zu ändern. Erfreulicherweise sind ja wegen der hervorragenden Arbeit der Polizei von Bund und Ländern einige Anschläge verhindert worden. Aus gutem Grund ist bei

der Gründung der Bundesrepublik die Polizeihöhe in die Hände der Länder gelegt worden, weil man aus den historischen Erfahrungen heraus keine zentrale Polizeigewalt haben wollten.

Die beabsichtigte Aufhebung der Trennung zwischen ordentlicher Polizei und Geheimdienst muss jeden Bürger beunruhigen, insbesondere weil bei den Bürgern bei Polizeimaßnahmen immer die vollständige juristische Kontrolle bleiben muss. Wir brauchen in Deutschland keinen Umbau des BKA, das einem ausufernden Präventionsstaat Tür und Tor öffnet.

Durch den gesamten Gesetzentwurf zieht sich eine Missachtung des verfassungsrechtlich gebotenen Schutzes des Kernbereichs privater Lebensgestaltung. Die unantastbare Würde des Menschen gebietet, dass es einen absolut geschützten Bereich geben muss, der frei von staatlicher Einsichtnahme bleibt. Mit dem beschlossenen Gesetzentwurf wird der Kernbereichsschutz so stark reduziert, dass es kaum zu einem Unterbleiben des Eingriffs kommen wird, sondern allenfalls ein nachträgliches Verwertungsverbot zu Unrecht erhobener privater Erkenntnisse geben wird. Das liegt nicht in der Intention der Rechtssprechung des Bundesverfassungsgerichts.

Meine Damen und Herren, ich erwähne den Umbau des BKA gleich zu Beginn, weil er auch unmittelbare Auswirkungen auf das Verhältnis von Arzt und Patienten haben wird.

Tritt die BKA-Novelle in Kraft, wird künftig der Lauschangriff sogar auf Kontakt- und Begleitpersonen ausgeweitet.

Meine Damen und Herren, was das für die Ärzteschaft bedeutet, liegt auf der Hand: Der Schutz von besonderen Vertrauensverhältnissen, die gerade das Verhältnis von Arzt und Patient prägen, wird durch den Umbau des BKA weiter ausgehöhlt.

Für Liberale ist völlig unstrittig, dass ein absoluter Schutz der Gesprächspartner von Berufsgeheimnisträgern vor heimlichen Ermittlungsmaßnahmen genauso wichtig ist wie der absolute Schutz für Berufsgeheimnisträger selbst.

Es ist eine Grundüberzeugung unserer Rechtsordnung, dass nicht mit jedem Mittel jede nur mögliche Information gewonnen werden darf. Von daher sieht auch die Strafprozessordnung, das angewandte Verfassungsrecht, seit jeher vor, dass es einen Schutz von Personen vor heimlichen Ermittlungsmaßnahmen geben muss, weil sie sonst nicht in der Lage sind, ihren Beruf mit der Wahrung der notwendigen Vertrauensbeziehungen auch auszuüben.

Diese Berufsgeheimnisträger wie Ärzte und viele andere müssen absoluten Schutz genießen. Es geht hier nicht um ein Privileg der Berufsgeheimnisträger, sondern um den Schutz der Privatsphäre der Bürgerinnen und Bürger, der Patienten oder der Mandanten.

Wird erst einmal das Vertrauensverhältnis zu Ärzten relativiert, ist das Ende der vertraulichen Gespräche mit den Vertretern dieser Berufsgruppen vorhersehbar. Aus

Angst vor polizeilichen Lauschangriffen werden auch solche Bürgerinnen und Bürger, die weit davon entfernt sind, jeweils in die Nähe terroristischer Aktivitäten zu geraten, sich den Berufsgeheimnisträgern weniger oder nicht mehr anvertrauen.

Anrede,

nach Ansicht der Liberalen ist der demokratisch verfasste Rechtsstaat auf kommunikative Freiräume angewiesen. Sie für Lausch- und Spähangriffe zu öffnen, ist für das Ziel, den internationalen Terrorismus zu bekämpfen, weder geeignet noch erforderlich und schon gar nicht verhältnismäßig.

Mit Sorge betrachte ich besonders die Aufweichung des Vertrauensschutzes von Ärzten und Patienten, wie sie durch die von Union und SPD geänderte Strafprozessordnung vorgenommen wurde und seit Anfang des Jahres gilt. Unter anderem wurde in die StPO ein neuer Paragraf 160a eingeführt. Er enthält Schutzvorschriften vor verdeckten staatlichen Ermittlungsmaßnahmen für Berufsgeheimnisträger, die sich nach §§ 53, 53a StPO auf Zeugnisverweigerungsrechte berufen können.

Nach § 160a StPO Abs. 1 ist eine Ermittlungsmaßnahme, die sich gegen Geistliche (§ 53 Abs. 1 Nr. 1 StPO), Strafverteidiger (§ 53 Abs. 1 Nr. 2 StPO) und Abgeordnete (§ 53 Abs. 1 Nr. 4 StPO) richtet „und voraussichtlich Erkenntnisse erbringen würde, über die diese Person das Zeugnis verweigern würde, unzulässig“.

Die übrigen von § 53 Abs. 1 StPO erfassten Berufsgeheimnisträger sind von diesem generellen Schutz vor verdeckten Ermittlungsmaßnahmen des Staates ausgenommen.

Für sie bestimmt § 160a Abs. 2 StPO lediglich, dass bei Ermittlungsmaßnahmen, durch die Rechtsanwälte, Ärzte u.a. (§ 53 Abs. 1 Satz 1 Nr. 3 bis 3b StPO) oder Journalisten (§ 53 Abs. 1 Nr. 5 StPO) betroffen wären „... und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Personen das Zeugnis verweigern dürften, dies im Rahmen der Prüfung der Verhältnismäßigkeit besonders zu berücksichtigen (ist)“.

Während also gegen Geistliche, Strafverteidiger und Abgeordnete gerichtete verdeckte Ermittlungsmaßnahmen des Staates generell unzulässig sind, wenn mit ihnen voraussichtlich dem Recht auf Zeugnisverweigerung unterfallende Erkenntnisse erlangt werden, sind verdeckte Ermittlungsmaßnahmen von denen Ärzte, Rechtsanwälte und Journalisten betroffen sind, generell zulässig, wenn die Bedeutung der Straftat, wegen der ermittelt wird, das Gewicht des Berufsgeheimnisschutzes überwiegt. Als Auslegungshilfe für die insoweit geforderte Einzelfall-Abwägung führt § 160a Abs. 2 StPO aus, dass in der Regel dann nicht von einem überwiegenden Strafverfolgungsinteresse auszugehen ist, wenn sich das Ermittlungsverfahren auf Straftaten von nicht erheblicher Bedeutung bezieht.

Gegen diesen unterschiedlichen Schutz der von § 53 StPO erfassten zeugnisverweigerungsberechtigten Berufsgeheimnisträger vor verdeckten Ermittlungsmaßnahmen der Strafverfolgungsbehörden sind im Verlaufe des Gesetzgebungsverfahrens triftige Einwände vorgebracht worden. Sie wurden von der

Regierungsmehrheit des Deutschen Bundestages nicht beachtet. Auch lehnte die Mehrheit des Bundesrates den vom Land Berlin eingebrachten Antrag ab, wegen der als problematisch angesehenen Regelung des § 160a StPO den Vermittlungsausschuss anzurufen.

Schlüssige, nachvollziehbare Argumente für die vorgenommene Abschichtung des Schutzes zeugnisverweigerungsberechtigter Personen vor verdeckten Ermittlungsmaßnahmen werden von der Bundesregierung nicht vorgebracht. So muss es unverständlich bleiben, dass die Bundesregierung ausweislich der Gesetzesbegründung mit Verweis auf die Rechtsprechung des Bundesverfassungsgerichts zwar konzidiert, dass die vertrauliche Kommunikation von Arzt und Patient verfassungsrechtlich dem Zugriff des Staates entzogen, um dann dennoch gerade diesen Berufsgruppen einen nur beschränkten Schutz vor verdeckten Ermittlungsmaßnahmen zuzubilligen.

Ebenso unverständlich ist es, wenn die Bundesregierung den Vorschlag des von ihr in Auftrag gegebenen Forschungsgutachtens, demzufolge nicht nur für Verteidiger und Angeordnete, sondern auch für Journalisten ein absolutes Überwachungsverbot vorzusehen wäre, zwar als unbegründet ablehnt, ihrerseits aber auf einer gleichermaßen unbegründeten Differenzierung des Schutzes vor staatlichen Ermittlungsmaßnahmen besteht. Auch ist nicht nachzuvollziehen, warum die Bundesregierung auf die Kernbereichsrechtsprechung des Bundesverfassungsgerichts verweist, wonach ein genereller Vorrang der schutzwürdigen Interessen von Journalisten und Abgeordneten vor dem Strafverfolgungsinteresse des Staates verfassungsrechtlich nicht begründet ist, um ihrerseits daraus zu folgern, dass Journalisten und Abgeordnete hinsichtlich des Schutzes vor Ermittlungsmaßnahmen unterschiedlich zu behandeln sind.

Alles in allem ist die in dem Gesetz vorgesehene Differenzierung des Schutzes zeugnisverweigerungsberechtigten Personen vor verdeckten Ermittlungsmaßnahmen willkürlich. Letztlich erschöpft sich die Begründung der Differenzierung in der dezisionistischen Behauptung, dass – anders als bei Geistlichen, Verteidigern und Abgeordneten - dem konzidierten verfassungsrechtlich gebotenen besonderen Schutz von zeugnisverweigerungsberechtigten Ärzten, Anwälten, und Journalisten durch das in § 160a Abs. 2 aufgenommene Abwägungsgebot genügend Rechnung getragen sei.

Dem kann nicht gefolgt werden. Vielmehr ist aus § 53 Abs. 1 StPO, der die Kommunikationsbeziehungen aller dort erfassten Berufsheimnisträger zu den bei ihnen Schutz und Hilfe suchenden Bürgern unterschiedslos einer besonderen Vertraulichkeit unterstellt, kein Spielraum für eine hinsichtlich des Vertraulichkeitsschutzes differenzierende Regelung herzuleiten.

Differenzierende Regelungen, wie sie die Abs. 1 und 2 des neuen § 160a StPO vorsehen, höhlen demnach den gesetzgeberischen Zweck des § 53 StPO aus und führen zu Wertungswidersprüchen sowohl in § 53 Abs. 1 StPO als auch in § 203 StGB, der die Preisgabe von Informationen, auf die sich ein Zeugnisverweigerungsrecht bezieht, das heißt, die Verletzung von Privatheimnissen unter Strafe stellt.

Eine Abstufung des Vertrauensschutzes lässt sich ebenfalls nicht aus dem unterschiedlichen Bezug zum Kernbereich privater Lebensgestaltung der verschiedenen zeugnisverweigerungsberechtigten Berufsheimnisträger oder aus anderen Grundrechten ableiten. So ist es z.B. nicht plausibel, dass die Informationen, auf die sich das Zeugnisverweigerungsrecht z. B. des Geistlichen bezieht, a priori stärkeren Bezug zum Kernbereich aufweisen sollte, als die körperlichen oder seelischen Offenbarungen eines Patienten seinem Arzt oder Psychiater gegenüber.

Die Regelung in § 160a Abs. 2 StPO verkennt die hinsichtlich des Vertraulichkeitsschutzes herausgehobene Stellung des Arzt-Patienten-Verhältnisses. Angaben des Arztes zu Anamnese, Diagnose und Therapie betreffen zwar nicht unbedingt und nicht in jedem Falle die unantastbare Intimsphäre, wohl aber den privaten Bereich des Patienten. Damit nehmen sie Teil am Persönlichkeitsschutz, den das Grundrecht aus Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG dem Einzelnen vor dem Zugriff der staatlichen Gewalt gewährt.

Dabei kommt es nicht darauf an, ob derartige Feststellungen sich auf Krankheiten, Leiden oder Beschwerden beziehen, deren Offenbarung den betroffenen Patienten mit dem Verdacht einer Straftat belasten oder ihm in anderen Hinsichten peinlich oder seiner sozialen Geltung subjektiv oder objektiv abträglich sind.

Vielmehr verdient ganz allgemein der Wille des Einzelnen Achtung, höchstpersönliche Sachverhalte, wie die Beurteilung seines Gesundheitszustandes durch den Arzt, vor fremder Kenntnisnahme zu bewahren. Wer sich in ärztliche Behandlung begibt, muss und darf erwarten, dass alles, was der Arzt im Rahmen seiner Berufsausübung über seine körperliche oder psychische Verfassung erfährt, geheim bleibt und ohne seine ausdrückliche Einwilligung nicht zur Kenntnis Dritter gelangt. Das allgemeine Persönlichkeitsrecht schützt daher grundsätzlich vor der Erhebung und Weitergabe von Befunden über den Gesundheitszustand, die seelische Verfassung und den Charakter.

Die im Einzelfall vorzunehmende Verhältnismäßigkeitsprüfung gemäß § 160a Abs. 2 StPO führt dazu, dass das grundrechtlich geschützte Vertrauensverhältnis zwischen Arzt und Patient nicht in jedem Falle gewährleistet werden kann.

Anrede,

so wichtig ein handlungsfähiger Staat beim Vorgehen gegen internationalen Terrorismus und organisierte Kriminalität ist, so wichtig ist der Erhalt des demokratisch verfassten Rechtsstaats mit seinen Grundrechtsgarantien. Der Gesetzgeber muss deshalb immer die richtige Balance wahren, um das Vertrauen der Bürgerinnen und Bürger in die Achtung ihrer Privat- und Intimsphäre durch staatliche Organe zu erhalten.

Nach biometrischen Merkmalen in Reisepässen und künftig auch in Personalausweisen, nach immer intensiveren Zugriff auf die Kontendaten der Bürgerinnen und Bürger, nach immer weiteren Befugnissen für Bundesnachrichtendienst, Verfassungsschutzbehörden, militärischem Abschirmdienst mit Zugriff auf umfangreiche private Datenbestände, nach einem

ständigen Anstieg der Telefonabhörmaßnahmen und schließlich nach Vorratsdatenspeicherung und Online-Durchsuchung verwundert es nicht, dass die Angst vor dem gläsernen Bürger zunimmt und die gesellschaftlichen Sorgen wachsen.

Im Bereich des öffentlichen wie nicht-öffentlichen Datenschutzes war 2008 von einer bislang ungekannten Serie an Datenschutzpannen geprägt. Sie haben sicher heute früh den Zeitungen entnommen, dass alleine der Kreis der von Telekom illegal abgehörten Personen auf 55 Personen angewachsen ist. Oder denken Sie an die Einkaufsketten, die dieses Frühjahr illegale Bespitzelungsaktionen der eigenen Belegschaft einräumen mussten.

Angesichts dieser Pleiten, Pech und Pannen im Datenschutz erlebt der Datenschutz als gesellschaftliches Thema geradezu eine Renaissance.

Der Datenschutz, wie wir ihn verstehen und kennen, ist viel mehr als ein bloßer Abwehranspruch gegen Datenerhebung und –verwendung. Es ist der auf Informationstechnologie angewandte Schutz der Menschenwürde und des Persönlichkeitsrechts. Als solcher dient der Datenschutz auch dem Schutz der Intimsphäre des Einzelnen vor der Erhebung höchstpersönlicher Daten, auf deren konkrete Auswertung und Weitergabe der Bürger im Einzelfall kaum Einfluss hat. Denn die Erhebung von – getrennt betrachtet – unerheblichen Daten kann durch deren Kombinierung und Bündelung in einem Profil zur Preisgabe von intimen Angaben über das Privatleben des Betroffenen führen.

Darüber hinaus kann der Datenschutz aber auch betrachtet werden als Schutz gegen technologische Verdinglichung.

Schon 1969 führte das Bundesverfassungsgericht im Mikrozensus-Urteil dazu aus: „Es widerspricht der menschlichen Würde, den Menschen zum bloßen Objekt im Staat zu machen. Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist.“ (Zitat Ende)

Und seit dem Volkszählungsurteil aus dem Jahre 1983 hat sich das Datenumfeld durch die Informationsgesellschaft gravierend verändert. Damals füllten Computer noch ganze Räume und beim Einkaufen wurden Rabattmarken statt Kredit- oder Kundenkarten benutzt. Heutzutage werden Kunden-, Täter-, Bewegungs- und Gesundheitsprofile erstellt, die durch Verknüpfung ein genaues Persönlichkeitsprofil ergeben können.

Übrigens: Bei der Volkszählung musste der Staat noch an die Tür der Bürger klopfen und die Daten erfragen, während heute Daten in damals unvorstellbarem Ausmaß versteckt erhoben werden, wovon der Bürger in der Regel nichts erfährt.

Stetige Aktualisierungen und Anpassungen des einfachgesetzlichen Datenschutzes werden daher immer nötig sein, um ein gleichbleibendes Schutzniveau bei weiterem informationstechnischen Fortschritt zu gewährleisten.

Daher ist es nur konsequent, dass das Bundesverfassungsgericht den grundrechtlich gebotenen Schutz der Privatsphäre (im Urteil zum Verfassungsschutzgesetz Nordrhein-Westfalen) durch die Schaffung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufgewertet und angepasst hat. In Anbetracht der neuen technischen Möglichkeiten der Ermittlungsbehörden war dies datenschutzrechtlich geboten.

So begrüßenswert dieses Urteil für die datenschutzrechtliche (Grundrechts-) Dogmatik auch ist, in der Praxis geht der Trend eher in die gegenteilige Richtung. Im Jahr 2006 war Deutschland noch Spitzenreiter der internationalen Vergleichstudie zum Datenschutz, die von der renommierten Menschenrechtsorganisation „Privacy International“ erstellt wurde. Dies ging vor allem zurück auf die verfassungsrechtlich verbriefte Rolle des Datenschutzes in Deutschland und auf das dichte Netz von Datenschutzbehörden, das zum Teil der föderalistischen Struktur der Bundesrepublik zu verdanken ist.

Die aktuelle Studie kommt zu einem anderen Ergebnis. Deutschland ist innerhalb eines Jahres ins Mittelfeld abgerutscht. Der Status der datenschutzrechtlichen Veränderung zum Vorjahr wird als „decaying“ bezeichnet, die schlechtmöglichste Kategorie, die soviel bedeutet wie ‚zerfallend‘ oder ‚zugrunde gehend‘. Diese Verschlechterung geht laut der Studie vor allem darauf zurück, dass Deutschland europaweit mit die höchste Abhör- und Überwachungsrate aufweist.

Diese Entwicklung wird sich in Anbetracht der neu gefassten Eingriffsbefugnisse wie der Onlinedurchsuchung in Zukunft wohl noch verstärken. Besonders negativ hat sich auch der Beschluss ausgewirkt, biometrische Daten in Ausweisdokumenten einzuführen. Die Folgen dieser Maßnahme sind, insbesondere in Anbetracht der weiter fortschreitenden Vernetzung der Datenbanken, noch nicht abzuschätzen.

Ich will hier nicht den falschen Eindruck erwecken, dass im Zeitalter der Informationstechnologie technologischer Fortschritt per se abzulehnen ist. Die meisten z. T. lebenswichtigen Infrastrukturen - ob Schienen-, Straßen-, Luftverkehr oder Sprach- und Datennetze, Energieversorgung oder Rettungsdienste, Banken oder Krankenhäuser - sind heute ohne Informationstechnik und Vernetzung nicht mehr funktionsfähig. In vielen Bereichen sind bereits hochgradig automatisierte IT-Systeme im Einsatz.

Trotz der Gefahrenpotenziale ist es müßig, die weitere Entwicklung und Verbreitung der IT in Frage zu stellen. Verstärkt durch die Globalisierung von Wirtschaft und Finanzwesen, ferner durch die zunehmende Privatisierung öffentlicher Infrastrukturen und von Aufgaben, die früher als hoheitlich betrachtet wurden, sind neue Technologien heute unverzichtbar.

Und der Einsatz neuer elektronischer Informations- und Kommunikationstechnologien kann im Gesundheitswesen zu Verbesserungen für alle Beteiligten führen.

Gleichwohl dürfen die Gefahren nicht weg geredet werden. Die von bewusstem Missbrauch herrührenden Gefahren einer durch und durch technologisierten Welt sind grenzenlos.

Umso mehr begrüße ich es, dass sich die Ärzteschaft immer wieder einen Grundkonsens bemüht, unter welchen Bedingungen der Einsatz neuer elektronischer Informations- und Kommunikationstechnologien ermöglicht werden soll. Und eines ist von Ihnen – und wird auch Gegenstand Ihrer Beratungen sein – immer wieder betont worden: Der uneingeschränkte Schutz der Patientendaten muss gewährleistet sein.

Das Vertrauen, das bereits beschädigt wird durch eine Aushöhlung des Vertrauensschutzes, darf nicht durch eine an falschen Effizienzgedanken orientierten Telematik weiter beschädigt werden.

Es geht nicht um die grundsätzliche Perspektiven, die die Telematik im Gesundheitswesen eröffnen kann. Die Ärzteschaft hat ja durch ihr Mitwirken in der Gesellschaft für Telematikanwendungen der Gesundheitskarte und durch die Praxistests in den Regionen gezeigt, wie sie sich konstruktiv im Sinne eines klaren Vertrauensschutzes von Ärzten und Patienten einbringt.

Und Sie beraten auf Ihrer Bundesversammlung auch ein Positionspapier zur Elektronischen Gesundheitskarte, das unmissverständliche Kritik an dem bisherigen Ergebnis des Einführungsprozesses der elektronischen Gesundheitskarte führt.

Sicher gibt es Perspektiven, die sich aus dem Einsatz der Telematik im Gesundheitswesen für eine Verbesserung der Versorgung und der Abläufe ergeben könnten. Nur wiegen die derzeitigen Gefahren wesentlich stärker. Gefahren, die sich aus der Übermittlung und Speicherung hoch sensibler Gesundheitsdaten ergeben. Diese Gefahr ist bei einem umfassenden Ansatz für die gesamte Bevölkerung, wie er der elektronischen Gesundheitskarte zugrunde liegt, besonders groß. Ich sage daher ganz offen: Ich halte wenig von dem bereits eingeschlagenen Weg. Die Einführung der elektronischen Gesundheitskarte darf nicht übereilt erfolgen. Und die ganzen Misserfolge des derzeit laufenden Projektes deuten darauf hin, das müssen selbst wohlwollende Stimmen eingestehen, dass die Kinderkrankheiten nicht geheilt worden sind.

Das bisher unzureichende Konzept im Rahmen der elektronischen Gesundheitskarte muss zurückgestellt werden, bis sichergestellt ist, dass:

- eine aktuelle Bewertung unter Einbeziehung der bisher gewonnenen Erkenntnisse ein positives Nutzen/Kosten-Verhältnis ergibt,
- weder Kostenträger, noch staatliche Stellen, Industrieunternehmen oder andere „Dritte“ Zugriff auf die sensiblen Gesundheitsdaten haben,
- die Freiwilligkeit der Nutzung aller über die Identifikation hinausgehenden Funktionen der elektronischen Gesundheitskarte für Patienten und Leistungsanbieter gewährleistet ist. Die Versicherten müssen die Verfügungsgewalt über ihre Daten haben und behalten. Sie müssen frei und unbeeinflusst entscheiden können, ob sie ihre Gesundheitsdaten auf zentralen Servern speichern lassen wollen oder nicht. Sie dürfen auch nicht durch Anreize oder Sanktionen indirekt veranlasst werden, ihre Gesundheitsdaten zur Speicherung freizugeben. Daran darf auch später nicht gerüttelt werden, wenn sich herausstellen sollte, dass die elektronische Gesundheitskarte wenn alle medizinischen Daten gespeichert werden,
- aus dem Gebrauch der elektronischen Gesundheitskarte kein erhöhter bürokratischer Aufwand resultiert, insbesondere auch beim Einlesen der Karte in Arztpraxen, Apotheken usw. sowie bei der Anwendung der PIN-Nummer,

- eine eingehende Prüfung durch unabhängige Sachverständige dahingehend stattfindet, ob moderne alternative Speicherungsmöglichkeiten wie z. B. die Speicherung auf der Gesundheitskarte selbst oder auf so genannten USB-Sticks praktikabler und sinnvoller ist als eine Speicherung auf zentralen Servern,
- eine Überprüfung der technischen Konzepte durch unabhängige Gutachter im Hinblick auf die Sicherheit der Daten erfolgt.

Benötigt wird eine Telematikinfrastruktur, die die technischen Voraussetzungen dafür schafft, dass Daten ohne Schwierigkeiten auf sicherem Weg ausgetauscht werden können.

Das Gesamtkonzept, das hinter der elektronischen Gesundheitskarte steht, geht darüber jedoch hinaus. Es sieht eine bundesweit über alle Anwendungen hinweg einheitliche Speicherung und Nutzung diverser Funktionen wie dem elektronischen Rezept oder der elektronischen Patientenakte vor. Nur dann kann sich nämlich das von der Bundesregierung behauptete positive Nutzen/Kosten-Verhältnis ergeben. Problematisch ist das insbesondere dann, wenn für fast die gesamte Bevölkerung und die Behandler eine Abwicklung des Austausches sensibler Gesundheitsdaten über die elektronische Gesundheitskarte mit einer hinterlegten zentralen Serverlösung vorgesehen wird.

Denken Sie nur an die dezentrale Struktur des Internets, die sich staatlich regulative Kontrollen, Überwachungsmaßnahmen und Eingriffen immer wieder zu entziehen versteht. Und nur wenige Stunden nach den Terroranschlägen auf das World Trade Center funktionierte das Internet dank seiner dezentralen Struktur wieder tadellos.

Ein anderer, wesentlicher Aspekt ist die Freiwilligkeit der Nutzung der neuen Funktionen der elektronischen Gesundheitskarte sowohl für die Patienten als auch für die Behandler. Nur dann, wenn diese Voraussetzung gewährleistet ist, wird die für ein solches Projekt benötigte Akzeptanz entstehen. Im Laufe der Zeit wird sich dann zeigen, welche Vor- und Nachteile mit der Nutzung der durch die elektronische Gesundheitskarte ermöglichten Anwendungen verbunden sind.

Die Einführung der elektronischen Gesundheitskarte muss zurückgestellt werden bis sichergestellt ist, dass die Voraussetzungen der Datensicherheit erfüllt sind. Das muss durch unabhängige Sicherheitsexperten überprüft sein. Die Zeit der Aussetzung ist zudem zu nutzen, um noch einmal gründlich zu prüfen, ob technische Alternativen zur Speicherung von Daten gegenüber zentralen Serverlösungen nicht der bessere Weg sind, mit solch sensiblen Daten umzugehen. Regelungsbedürftig ist auch die Frage wie das ganze Verfahren so praktikabel gemacht werden kann, dass keine Verzögerungen z. B. in den Arztpraxen entstehen. Es müssen datenschutzrechtlich unangreifbare Lösungen auch für die Fälle gefunden werden, in denen Menschen mit den Anforderungen durch die Eingabe einer PIN-Nummer nicht zurechtkommen oder aus gesundheitlichen Gründen dazu nicht in der Lage sind.

Neben diesen technischen Fragen droht in der Debatte über die Einführung der elektronischen Gesundheitskarte ein Aspekt in den Hintergrund zu geraten. Eine gute Medizin im Sinne eines Heilungserfolges lebt von der vertrauensvollen Beziehung von Patient und Arzt. Eine vertrauensvolle Beziehung kann es nur geben, wenn das Gespräch zwischen Arzt und Patient auch künftig im Mittelpunkt der Kommunikation im Gesundheitswesen steht.

Die elektronische Gesundheitskarte muss, wenn sie unter den von mir genannten Bedingungen, eines Tages kommen sollte, diesen Ansatz ausreichend berücksichtigen. Akzeptanz entsteht durch Vertrauen.

Richtig verstandener Datenschutz ist stets auch Vertrauensschutz. Kommt es zu Datenpannen, leiden darunter nicht nur Patienten, sondern das gesamte Gesundheitswesen.

Leider ist diese Sichtweise – Datenschutz als vertrauensbildende Maßnahme – in der Vergangenheit zu kurz gekommen.

Die Bundesregierung ist dabei mit besonders schlechtem Beispiel vorangegangen: Es ist scheinheilig, sich über andere aufzuregen, wenn man selbst so gut wie nichts für den Datenschutz tut. Welch geringe Wertschätzung der Datenschutz bei CDU/CSU und SPD genießt, ist im Koalitionsvertrag nachzulesen. Dort ist wiederholt vom Datenschutz als Hindernis die Rede - beim Bürokratieabbau, bei der Terrorismusbekämpfung usw.

Als erste und bisher einzige Fraktion im Deutschen Bundestag hat die FDP einen Antrag zur Verbesserung des Datenschutzes vorgelegt. Darin fordern wir eine Verbesserung der Stellung der betrieblichen Datenschutzbeauftragten, mehr Transparenz, ein angemessenes Sanktionssystem, ein Ausführungsgesetz zum Datenschutz-Audit, eine Gesamtstrategie zur Förderung datenschutzfreundlicher Technik und eine strikte Verwirklichung des Grundsatzes der Datensparsamkeit.

Vieles hiervon stieß in erster Lesung auf Zustimmung auch der anderen Bundestagsfraktionen. Vieles hiervon lässt sich bereits auf der betrieblichen Ebene verwirklichen, z. B. durch eine Beschränkung der Zugangsmöglichkeiten zu geschützten Daten, durch ein System wechselseitiger Kontrollen oder durch ein Vier-Augen-Prinzip beim Datenzugang. Eingebettet werden muss dies in eine effektive Datenschutzkontrolle. Selbstverpflichtungen alleine sind keine ausreichende Antwort. Das Versprechen, Gesetze einzuhalten, ist eine Selbstverständlichkeit und kann nicht die einzige Konsequenz aus den aktuellen Vorfällen sein.

Das Gleiche gilt für den Bereich des Arbeitnehmerdatenschutzes. Bis heute fehlen spezielle gesetzliche Regelungen. Arbeitgeber und Arbeitnehmer sind daher im Wesentlichen darauf angewiesen, sich an der Rechtsprechung zu orientieren. Auch Kennern der Materie fällt es nicht immer leicht, angesichts stetig wachsender technischer Möglichkeiten die Frage zu beantworten, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Bislang hat die schwarz-rote Bundesregierung keine erkennbaren Aktivitäten auf diesem Gebiet entwickelt, obwohl der Deutsche Bundestag dies wiederholt fraktionsübergreifend gefordert hat. Überhaupt:

Die Modernisierung und Weiterentwicklung des Datenschutzrechts kommt seit Jahren nicht recht voran. Der Abstand zwischen dem geltenden Recht und dem technologischen Fortschritt wird dadurch immer größer. Das vom Deutschen Bundestag wiederholt geforderte moderne, leicht verständliche und übersichtliche Datenschutzrecht lässt weiter auf sich warten. Das ist nicht nur aus Sicht des Datenschutzes, das ist auch aus Sicht der Wirtschaft bedauerlich. Denn ein

modernes Datenschutzrecht könnte auch ein wirtschaftlicher Standortvorteil und ein Beitrag zur Entbürokratisierung sein.

Immerhin: Es gibt Bereiche, da tut sich etwas. Das gilt für das wichtige Thema Scoring. Hier besteht gesetzgeberischer Handlungsbedarf, dem die Bundesregierung nunmehr Rechnung tragen will. Durch eine Änderung des Bundesdatenschutzgesetzes sollen die Bürger im Bereich Scoring zukünftig besser geschützt werden. Ausgestaltung und Einsatz von Scoreverfahren sollen gesetzlich geregelt werden. Die FDP-Bundestagsfraktion begrüßt dies grundsätzlich.

Anrede,

die FDP-Bundestagsfraktion bekennt sich zur Informationsgesellschaft. Freie und unkontrollierte Kommunikation sind die Basis für Freiheit, Demokratie und Rechtsstaat. Freie Kommunikation basiert auf Vertrauen. Alle sind aufgerufen, dieses Vertrauen zu gewährleisten und verloren gegangenes Vertrauen wiederherzustellen.

Wenn die elektronische Gesundheitskarte eines Tages eingeführt werden sollte, dann nur wenn der Datenschutz diesen Namen verdient und Modell werden könnte.

Die Bewahrung des Datenschutzes und eines Kernbereichs der Privatsphäre liegt nicht nur im elementaren Interesse des Einzelnen, sondern ist ein unverzichtbarer Teil unserer liberalen Rechtsordnung. Ohne die Freiheit des einzelnen Bürgers wird es auch keine gesellschaftliche Freiheit geben.

Es kommt auf die Balance zwischen Freiheitsrechten und Maßnahmen zur Erhaltung der Sicherheit an. Doch diese Balance verschiebt sich in letzter Zeit zunehmend zugunsten der Sicherheit und auf Kosten der Freiheit. Der Einsatz für Freiheitsrechte wie den Datenschutz ist heute so wichtig, weil die elektronischen Datensammlungen stetig wachsen. Dadurch wachsen auch die Begehrlichkeiten staatlicher Überwachung.

Freiheit lässt sich nicht mit deren Einschränkung verteidigen. Wie Bundespräsident Köhler am Dienstag auf dem Juristentag in Erfurt sagte: „Unser Streben nach Sicherheit darf uns nicht unsere Freiheit kosten.“

Große Datenbestände verleiten zu Missbrauch. Deshalb muss die Politik sich davon leiten lassen, das Entstehen von neuen großen Datenbeständen zu verhindern. Das gilt für alle Bereiche, natürlich auch für die Gesundheitsdaten.