Deutscher Bundestag **Drucksache 15/4725**

15. Wahlperiode 26. 01. 2005

Antwort

der Bundesregierung

auf die Große Anfrage der Abgeordneten Gisela Piltz, Ernst Burgbacher, Rainer Funke, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 15/3256 –

Überprüfung der personengebundenen datenschutzrechtlichen Bestimmungen

Vorbemerkung der Fragesteller

Ende 2003 jährte sich das Volkszählungsurteil des Bundesverfassungsgerichts zum zwanzigsten Mal. Mit diesem Urteil hat das Bundesverfassungsgericht den Grundstein für das Datenschutzrecht in Deutschland gelegt und den Datenschutz von seiner Einstufung als technische Spezialmaterie ohne gesellschaftliche Bedeutung zum informationsspezifischen Grundrecht gewandelt. Grundlegend war unter anderem die Aussage des Bundesverfassungsgerichts, dass dem Recht des Bürgers auf informationelle Selbstbestimmung Verfassungsrang zukomme. Jedem Bürger sollte damit grundsätzlich das Recht gewährleistet werden, über die Preisgabe und die Verwendung seiner persönlichen Daten selbst entscheiden zu können. Diese Grundsätze des Bundesverfassungsgerichts haben Eingang in eine Fülle von gesetzlichen Regelungen, insbesondere datenschutzrechtlichen Spezialregelungen gefunden.

Da diese so genannten bereichsspezifischen Regelungen schon für Datenschützer häufig ein undurchschaubares Regelwerk darstellen, ist es in besonderem Maße für die Bürger schwierig, ihre datenschutzrechtlichen Rechte und Pflichten wahrzunehmen. Bereiche solcher datenschutzrechtlichen Regelungen finden sich u. a. in den Gebieten der polizeilichen und staatsanwaltlichen Ermittlungstätigkeit durch DNA-Tests und deren Speicherung, Rasterfahndung sowie Videoüberwachung, in der Erfassung von gesundheitsbezogenen Daten von Patienten durch Ärzte und Krankenkassen, in der Erfassung von Kundendaten in der Wirtschaft, im Internet, in der Erfassung von persönlichen Daten durch staatliche Behörden und deren Austausch untereinander sowie im Bereich der internationalen Zusammenarbeit. Auch Ermächtigungsnormen für die Datenverarbeitung durch Wirtschaft und Verwaltung sind mit dem Datenschutz eng verknüpft.

Im Hinblick auf die Ausweitung von datenschutzrechtlich relevanten Sachverhalten und die immer weitergehende Erfassung und Speicherung von Daten infolge des technischen Fortschritts ist die Frage des Datenschutzes auf den Prüfstand zu stellen.

Im Zeitalter der Informationsgesellschaft ist der Themenkomplex des Datenschutzes gerade auch in den letzten Wochen im Hinblick auf die datenschutz-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 26. Januar 2005 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

rechtlich bedeutsamen Entscheidungen des Bundesverfassungsgerichts zum so genannten Großen Lauschangriff sowie des Bundesverwaltungsgerichts zum Speichern von Daten bei Prepaid-Karten für Handys wieder aktuell.

I. Grundsätzliches

1. Liegen der Bundesregierung Erhebungen vor, aus denen sich Art und Umfang von Datenerfassung und -organisation in der Wirtschaft und in der öffentlichen Verwaltung ergeben?

Die amtliche Statistik nimmt derartige Erhebungen nicht vor.

2. Sieht die Bundesregierung eine grundsätzliche Gefahr für den Datenschutz darin, dass mit zunehmend verfügbarer Speicherkapazität vermehrt nützliche und nicht nur notwendige Daten gespeichert werden, und wenn ja, wie begegnet die Bundesregierung solchen Gefahren, insbesondere der Gefahr einer Aushöhlung des datenschutzrechtlichen Grundsatzes der Datenvermeidung?

Die Informations- und Kommunikationstechnik ist weltweit durch stetige Leistungssteigerungen und immer kürzere Innovationsphasen gekennzeichnet, die einer Übertragung und Nutzung von Daten in Bezug auf Umfang und Zeitaufwand technisch kaum mehr eine Grenze setzen. Die dadurch entstehenden Risiken für das Recht auf informationelle Selbstbestimmung hat bereits das Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 erkannt. Deshalb hat es ausdrücklich festgestellt, dass jede natürliche Person das Recht hat, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen. Dieses Recht darf nur im überwiegenden Allgemeininteresse oder im überwiegenden Interesse Dritter eingeschränkt werden (BVerfGE 65, 1 [43 f.]; 84, 192 [194 f.]; 99, 185 [195 f.]).

Die Erhebung und Verwendung personenbezogener Daten ist deshalb nur zulässig, soweit die Betroffenen eingewilligt haben oder wenn eine Rechtsvorschrift, die den Grundsätzen der Verhältnismäßigkeit und Normenklarheit, insbesondere auch einer klaren Zweckbindung zu genügen hat, dies erlaubt (vgl. § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG)). Mit der am 23. Mai 2001 in Kraft getretenen Änderung des Bundesdatenschutzgesetzes wurden zudem in § 3a BDSG die Grundsätze der Datenvermeidung und Datensparsamkeit erstmals im allgemeinen Datenschutzrecht gesetzlich verankert.

Die Einhaltung dieser rechtlichen Vorgaben wird durch die Datenschutzbeauftragten und die für die Datenschutzkontrolle im nichtöffentlichen Bereich zuständigen Aufsichtsbehörden der Länder überwacht. Deren Kontrolle wird durch behördliche und betriebliche Datenschutzbeauftragte ergänzt, die von öffentlichen sowie von nichtöffentlichen Stellen ab einer gewissen Größe sowie, falls diese besonders sensible Daten automatisiert verarbeiten, unabhängig von der Größe zu bestellen sind (§ 4f Abs. 1 in Verbindung mit § 4d Abs. 5 BDSG). Die Wahrnehmung der dezentralen Datenschutzkontrolle durch behördliche und betriebliche Datenschutzbeauftragte hat sich bewährt. Diese haben auf die Einhaltung des Bundesdatenschutzgesetzes und anderer datenschutzrechtlicher Vorschriften hinzuwirken. Nach § 4g Abs. 1 Satz 3 Nr. 1 BDSG sind sie bereits vorab über Vorhaben der automatisierten Verarbeitung personenbezogener Daten zu unterrichten und können daher bereits bei der Konzeption entsprechender Verfahren auf die Einhaltung des Grundsatzes der Datenvermeidung und Datensparsamkeit, etwa durch eine verstärkte Anonymisierung und Pseudonymisierung personenbezogener Daten, aktiv hinwirken. Dieses Organisationsprinzip ermöglicht eine dynamische Anpassung an sich wandelnde technische Gegebenheiten.

Die Novelle des Bundesdatenschutzgesetzes aus dem Jahr 2001 hat zugunsten der Betroffenen durch die Ausweitung der gesetzlichen Benachrichtigungspflichten in den §§ 4, 19a und 33 BDSG auch die Transparenz bei der Verarbeitung personenbezogener Daten weiter erhöht. Diese rechtlichen Rahmenbedingungen tragen insgesamt den mit der Erhöhung der Verarbeitungskapazitäten einhergehenden Risiken in ausgewogener Weise Rechnung.

3. Welche Bedeutung schreibt die Bundesregierung den Datenschutzaudits für den Wettbewerb und die Förderung des Datenschutzes im privaten Bereich zu?

Die Bewertung eines bestimmten Produkts oder einer Dienstleistung als datenschutzfreundlich kann zu einer Steigerung der Nachfrage nach diesem Produkt oder nach dieser Dienstleistung und damit zu einem Wettbewerbsvorteil führen. So entsteht ein Anreiz, weitergehende Maßnahmen zur Verbesserung des Datenschutzes zu ergreifen, um diesen Wettbewerbsvorteil zu erhalten und zu steigern. Dies gilt vor allem für Bereiche, die nach dem Empfinden der Verbraucher besonders datenschutzsensibel sind wie beispielsweise der elektronische Handel.

4. Wann beabsichtigt die Bundesregierung einen Gesetzentwurf über die näheren Anforderungen an Prüfung, Bewertung und weitere Voraussetzungen für die Vergabe von Datenschutzaudits i. S. d. § 9a Bundesdatenschutzgesetz (BDSG) einzubringen?

Zu gegebener Zeit.

5. Wie begründet die Bundesregierung ihr diesbezügliches Untätigbleiben seit Einführung des § 9a BDSG vor nunmehr fast drei Jahren?

Das federführend zuständige Bundesministerium des Innern hat zahlreiche Institutionen konsultiert, die im Tätigkeitsfeld von Akkreditierung und Zertifizierung im Datenschutzbereich tätig sind. Neben einzelnen Fragen zur Struktur und zu den Kosten eines Datenschutzaudits bleibt jedoch insbesondere klärungsbedürftig, ob eine solche Regelung eine dauerhafte staatliche Subvention dieses Verfahrens verlangen würde, und ob auch aus diesem Grund eine freiwillige Selbstorganisation der Wirtschaft vorzugswürdig ist. Darüber hinaus ist zu prüfen, ob ein Datenschutzaudit-Gesetz mit den von der Bundesregierung verfolgten Zielen des Bürokratieabbaus und der Eindämmung der Normenflut im Einklang steht.

6. Welche Erkenntnisse liegen der Bundesregierung hinsichtlich Erfahrungen mit Audits in anderen Bereichen, z. B. beim Umweltschutz, und den dortigen Auswirkungen auf die Wettbewerbssituation vor, und sind diese Erkenntnisse auf Datenschutzaudits übertragbar?

Die Bundesregierung hat dem Deutschen Bundestag im Jahr 1998 über die Erfahrungen mit dem Vollzug des Umweltauditgesetzes berichtet (Bundestagsdrucksache 13/11127), das auf der Verordnung (EWG) 1863/1993 beruht. Die dort geschilderten positiven Erfahrungen mit dem Umweltaudit haben sich seitdem bestätigt. Inzwischen sind in Deutschland ca. 2 000 Standorte nach EMAS (Eco-Management and Audit Scheme) zertifiziert. EMAS beruht auf der EG-Verordnung 761/2001 über die freiwillige Beteiligung von Organisationen an einem Gemeinschaftssystem für das Umweltmanagement und die Umwelt-

betriebsprüfung. Die teilnehmenden Unternehmen setzen sich dabei Umweltziele, die es innerhalb eines von ihnen selbst festgelegten Zeitraums zu erreichen gilt, was durch staatlich zugelassene Umweltgutachter überprüft wird. Die obligatorische Prüfung der Einhaltung der Rechtsvorschriften durch Umweltgutachter, wie sie die EMAS-Teilnahme ferner vorschreibt, verleiht dem Unternehmen darüber hinaus ein größeres Maß an Rechtssicherheit. An dem weltweiten Umweltmanagementsystem ISO 14001 nehmen mehr als 4 000 deutsche Unternehmen teil.

Unternehmen, die nach EMAS oder ISO 14001 zertifiziert sind, verfügen über folgende Wettbewerbsvorteile:

– Eröffnung des Eintritts in Umweltpakte und -partnerschaften in den Ländern, Zugang zu kommunalen Netzwerken (zum Beispiel Agenda 21),

– Vorzug bei der Vergabe öffentlicher Aufträge insbesondere in den Bereichen öffentlicher Nahverkehr und Abfallentsorgung,

– Erleichterungen bei der staatlichen Überwachung im Bereich des Immissionsschutz-, Abfall- und Wasserrechts,

– teilweise geringere Versicherungsprämien.

Überdies sind in fast allen Ländern durch den Einsatz von Umweltaudits die Gebühren für immissionsschutzrechtliche Genehmigungsverfahren um 20 bis 30 % gesunken.

Audit- und auditähnliche Verfahren kommen daneben in vielen weiteren Bereichen zum Einsatz. Im Bereich der Familien- und Gleichstellungspolitik sind unlängst unter der Schirmherrschaft des Bundesfamilien- und des Bundeswirtschaftsministeriums zwei Zertifikate entwickelt worden. Das Audit Beruf und Familie der gemeinnützigen Hertie-Stiftung dient als Qualitätsstandard familienbewusster Personalpolitik in Unternehmen. Seit der erstmaligen Vergabe des Zertifikats im Jahr 1999 haben 90 Unternehmen das Audit durchlaufen. Das Prädikat TOTAL-EQUALITY wird an Unternehmen vergeben, die im Bereich der Förderung der Chancengleichheit von Frauen und Männern besondere Leistungen und Erfolge vorzuweisen haben. Auch bei diesem Zertifikat hat die Erhöhung des Bekanntheitsgrads der teilnehmenden Unternehmen mittelbar positive Auswirkungen auf deren Wettbewerbsstellung.

Im Bereich der Internationalen Seeschifffahrts-Organisation (IMO) wurden standardisierte Verfahren zu Selbsteinschätzung über die Erfüllung flaggenstaatlicher Pflichten eingeführt. Ein solches Programm ist „Qualship 21“ der U.S.-Coast Guard, mit dem die Einhaltung von Sicherheits- und Qualitätsstandards durch den Flaggenstaat, die Reedereien und die Schiffsführung geprüft wird.

Die Erfahrungen mit den verschiedenen Verfahren lassen sich auf das Datenschutzaudit nicht ohne weiteres übertragen. Die Situation beim Umweltaudit ist dadurch gekennzeichnet, dass Zertifizierungsschemata aufgrund technischer oder rechtlicher Vorgaben bereits bestehen, während solche Schemata für Produkte und Dienstleistungen im Bereich des Datenschutzes noch entwickelt werden müssen. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat zu dem schleswig-holsteinischen IT-Gütesiegel berichtet, dass bei jedem neuen Prüfverfahren ein individuell auf das zu prüfende Produkt zugeschnittener Anforderungskatalog mit jeweils unterschiedlicher Prüftiefe ausgearbeitet werden müsse. Der Katalog, den das ULD den Gutachtern vorgebe, beruhe zwar auf den gesetzlichen Grundanforderungen. Diese gäben jedoch nur eine grobe Struktur vor. Diese Einschätzung entspricht nach Kenntnis der Bundesregierung den (wenigen) Erfahrungen mit Datenschutz-Gütesiegeln im so genannten ungeregelten Bereich.

In welchem Umfang ein Datenschutzaudit positive Auswirkungen auf die Wettbewerbssituation eines Unternehmens haben könnte, wird vor allem von dem jeweiligen Produkt oder der Dienstleistung abhängen, die Gegenstand einer Auditierung werden. Bezüglich der bestehenden Datenschutz-Gütesiegel liegen bislang, auch wegen der geringen Zahl der bisher erteilten Zertifikate, noch keine aussagekräftigen Erkenntnisse vor. Das ULD und die beim ULD akkreditierten externen Gutachter haben seit Beginn der Zertifizierung im Jahr 2002 18 Siegel verliehen. Das ULD hat festgestellt, dass die Produktwerbung mit dem Gütesiegel für die jeweiligen Unternehmen sehr attraktiv ist. Das Gütesiegel werde vermehrt gezielt eingesetzt, um Attraktivität und Marktchancen zu erhöhen.

7. Steht die Bundesregierung weiterhin zu ihren Plänen, ein Informationsfreiheitsgesetz vorzulegen, wie es in den Koalitionsvereinbarungen vom 20. Oktober 1998 und vom 16. Oktober 2002 festgelegt wurde, wenn ja, wann wird die Bundesregierung ein solches Gesetz in den Deutschen Bundestag einbringen, bzw. wenn nein, was hat sie veranlasst, ihr Vorhaben aufzugeben?

Eine Arbeitsgruppe der Koalitionsfraktionen hat einen Gesetzentwurf vorbereitet, der am 17. Dezember 2004 in erster Lesung im Deutschen Bundestag behandelt wurde (Bundestagsdrucksache 15/4493).

II. Bankgeheimnis

8. Beabsichtigt die Bundesregierung auf das Urteil des Bundesverfassungsgerichts vom 9. März 2004 (Az: 2 BvL 17/02) mit einer Änderung des § 30a Abgabenordnung (AO) zu reagieren?

Das Bundesverfassungsgericht hat für die Jahre 1997 und 1998 ein strukturelles Erhebungsdefizit bei der Besteuerung von privaten Wertpapier-Veräußerungsgewinnen festgestellt, zugleich aber in den Entscheidungsgründen deutlich gemacht, dass sich die Situation durch die gesetzgeberischen Maßnahmen seit 1999 deutlich verbessert hat. Allerdings hat sich das Gericht sehr kritisch mit der Regelung des § 30a AO – dem so genannten Bankgeheimnis – auseinander gesetzt. Es hat diese Vorschrift zwar nicht für verfassungswidrig erklärt, aber klar darauf hingewiesen, dass sie ein Hindernis für eine sachgerechte Verifikation darstellt.

Die Bundesregierung prüft deshalb, ob aufgrund der Entscheidung des Bundesverfassungsgerichts über die seit 1999 initiierten Maßnahmen, insbesondere über die Einführung der Kontenabfragemöglichkeit nach § 93 Abs. 7 in Verbindung mit § 93b AO ab dem 1. April 2005 hinaus weitere Maßnahmen zur Verbesserung der verfassungsrechtlich gebotenen Verifikation der Einkünfte aus privaten Wertpapier-Veräußerungsgeschäften erforderlich sind. Diese Prüfung ist noch nicht abgeschlossen.

9. Wie bewertet die Bundesregierung vor diesem Hintergrund die Bedeutung des Bankgeheimnisses sowie das datenschutzrechtliche Prinzip, dass Daten grundsätzlich beim Betroffenen zu erheben sind?

Im Besteuerungsverfahren gilt der Amtsermittlungsgrundsatz (§ 88 AO), wobei die Beteiligten in weitem Umfang zur Mitwirkung bei der Ermittlung aller steuererheblichen Tatsachen verpflichtet sind (§ 90 AO). Ermittlungen bei Dritten erfolgen grundsätzlich nur dann, wenn der Beteiligte seine Mitwirkungs-

pflicht verletzt, Auskunftsersuchen an den Beteiligten keinen Erfolg versprechen oder unmittelbare Ermittlungen bei Dritten gesetzlich vorgesehen sind.

Ausgangspunkt der Ermittlungen der Finanzbehörden sind daher grundsätzlich die Erklärungen und Anträge der Beteiligten. Für den Regelfall können die Finanzbehörden dabei auch weiterhin davon ausgehen, dass die Angaben des Beteiligten in seiner Steuererklärung vollständig und richtig sind. Die Finanzbehörde kann diesen Angaben Glauben schenken, wenn nicht greifbare Umstände vorliegen, die darauf hindeuten, dass seine Angaben falsch oder unvollständig sind (Anwendungserlass zur Abgabenordnung – AEAO – zu § 88, Nr. 2).

Wenn die Finanzbehörde jedoch eingehende Ermittlungen für erforderlich hält und ein Auskunftsersuchen an den Beteiligten selbst erfolglos war oder keinen Erfolg verspricht, kann sie künftig – ab dem 1. April 2005 – über die bereits bestehenden Möglichkeiten hinaus nach § 93 Abs. 7 in Verbindung mit § 93b AO einzelfallbezogen feststellen, bei welchem Kreditinstitut ein Beteiligter ein Konto oder ein Depot hat. Da die Finanzbehörde auf diesem Weg keine Informationen über Kontostände und Kontobewegungen erlangt, muss sie bei Bedarf aber weitere Ermittlungen anstellen. Auch hierbei ist erster Ansprechpartner der Beteiligte selbst. Weitere Ermittlungen bei Dritten, zum Beispiel bei Kreditinstituten, sollen auch in diesen Fällen nach § 93 Abs. 1 in Verbindung mit § 30a Abs. 5 Satz 2 AO erst erfolgen, wenn ein Auskunftsersuchen an den Beteiligten nicht zum Ziel geführt hat oder keinen Erfolg verspricht.

Insgesamt wird durch diese Grundsätze sowohl dem Datenschutz als auch dem verfassungsrechtlichen Verifikationsprinzip, das das Deklarationsprinzip ergänzt, sinnvoll Rechnung getragen.

Für das Steuerstrafverfahren gilt Folgendes: § 30a AO entfaltet eine beschränkende Wirkung lediglich im Hinblick auf die anlassunabhängige allgemeine Überwachung von Guthabenkonten oder Depots. Soweit die Finanzbehörden anlassbezogen wegen des Verdachts einer Steuerstraftat ermitteln, kann ihnen gegenüber die Auskunft nicht unter Berufung auf das Bankgeheimnis verweigert werden. Von öffentlich-rechtlichen Bankinstituten kann die ermittelnde Finanzbehörde nach § 161 Satz 1 der Strafprozessordnung (StPO) Auskunft verlangen. Kommt im Übrigen eine Bank dem Auskunftsverlangen nicht nach, so ist dieses durch Zeugenvernehmung von Mitarbeitern gleichwohl faktisch durchsetzbar.

10. Welche konkreten Kontoinformationen der Bürger sollen mit dem Gesetz zur Förderung der Steuerehrlichkeit beim Bundesamt für Finanzen zentral gespeichert werden, und auf welche dieser Kontoinformationen sollen die Finanzbehörden Zugriff erhalten?

Das Bundesamt für Finanzen darf nach § 93b in Verbindung mit § 93 Abs. 7 AO ab dem 1. April 2005 auf Ersuchen der für die Besteuerung zuständigen Finanzbehörden bei den Kreditinstituten die nachfolgend aufgeführten Daten aus den von den Kreditinstituten nach § 24c des Kreditwesengesetzes (KWG) zu führenden Dateien im automatisierten Verfahren abrufen und sie an die ersuchende Finanzbehörde übermitteln. Die damit verbundene Datenerhebung und -speicherung durch das Bundesamt für Finanzen erfolgt allein zum Zweck der Weiterübermittlung an die ersuchende Finanzbehörde. Eine darüber hinausgehende Verwendung der Daten durch das Bundesamt ist nicht gestattet; allerdings muss dieses Daten über einen Kontenabruf zum Zweck der Datenschutzkontrolle speichern (§ 93b Abs. 4 AO in Verbindung mit § 24c Abs. 4 KWG).

Folgende in § 24c Abs. 1 KWG aufgeführten Daten dürfen abgerufen werden:

– Nummer eines Kontos oder Depots, das nach § 154 AO der Verpflichtung zur Legitimationsprüfung unterliegt,

– Tag der Errichtung und der Auflösung des Kontos oder Depots,

– Name, bei natürlichen Personen auch Geburtstag, des Inhabers und ggf. eines Verfügungsberechtigten,

– ggf. Name und Anschrift eines abweichend wirtschaftlich Berechtigten.

Die Verantwortung für die Zulässigkeit des Datenabrufs und der Datenübermittlung, insbesondere im Hinblick auf die Vorgaben des § 93 Abs. 7 AO, trägt die ersuchende Finanzbehörde.

11. Welchen weiteren Behörden soll der Zugriff auf diese Daten ermöglicht werden, und welche Möglichkeiten der Datenzusammenführung und/oder -verknüpfung ergeben sich daraus?

Wenn eine öffentliche Stelle, die für die Anwendung eines Gesetzes, das an Begriffe des Einkommensteuergesetzes anknüpft, zuständig ist, versichert, dass eigene Ermittlungen nicht zum Ziel führen oder keinen Erfolg versprechen, so darf sie die Finanzbehörde darum ersuchen, bei den Kreditinstituten die in § 24c Abs. 1 KWG aufgeführten Daten über das Bundesamt für Finanzen abzurufen (§ 93b in Verbindung mit § 93 Abs. 8 AO) und an sie zu übermitteln. Die Verantwortung für die Zulässigkeit des Datenabrufs und der Datenübermittlung trägt in diesem Fall die ersuchende Behörde oder das ersuchende Gericht (§ 93b Abs. 3 AO).

Derartige Ersuchen sind danach nur zulässig, wenn gesetzlich ausdrücklich angeordnet ist, dass eine staatliche Leistung an einen Begriff des Einkommensteuergesetzes anknüpft, beispielsweise an die „festgesetzte Einkommensteuer“ oder die ihr zugrunde liegenden Besteuerungsgrundlagen wie etwa „zu versteuernde Einkünfte“ oder „Einkommen“. Dies betrifft auch Sozialleistungen. Darüber hinaus gilt, wie bei allen Datenverarbeitungsvorschriften, der Verhältnismäßigkeitsgrundsatz. Daraus folgt hier insbesondere, dass die Datenübermittlung für den Vollzug der nichtsteuerlichen Vorschriften erforderlich sein muss.

12. Wie bewertet die Bundesregierung die Sicherheit der Daten vor Missbrauch, wenn mit den durch das Gesetz zur Förderung der Steuerehrlichkeit in Kraft tretenden Regelungen der Datenaustausch zwischen einzelnen Behörden zunimmt?

Die in Frage stehenden Daten unterliegen dem Steuergeheimnis, denn dieses gilt nicht nur für die Finanzbehörde, sondern nach § 30 Abs. 2 Nr. 1 Buchstabe c AO auch für solche Amtsträger, denen bei der Besteuerung getroffene Feststellungen durch eine Finanzbehörde mitgeteilt worden sind. Die unbefugte Verletzung des Steuergeheimnisses ist strafbar (§ 355 StGB). Vor diesem Hintergrund erwartet die Bundesregierung keine erhöhte Missbrauchsgefahr.

13. Hält die Bundesregierung an ihren Plänen fest, im Zuge der Einführung einer Ist-Versteuerung ein so genanntes Cross-Check-Verfahren für die Umsatzsteuer vorzugeben, mit dem die Verpflichtung einhergehen soll, jeden einzelnen steuerrelevanten Umsatz den Finanzbehörden anzuzeigen und zu speichern?

Angesichts der massiven Umsatzsteuerausfälle aufgrund von Umsatzsteuerbetrug werden derzeit auch grundlegende Überlegungen zur Änderung des Umsatzsteuerrechts angestellt, um den Umsatzsteuerbetrug einzudämmen. Zwei Modelle werden derzeit geprüft. Eines davon ist das so genannte Modell der Ist-Versteuerung mit Cross-Check-Verfahren. Um eine zuverlässige Steuererhebung zu erreichen, wird nach diesem Modell die Ist-Versteuerung abgesichert durch die Meldung der steuerpflichtigen Transaktionen oberhalb einer Bagatellgrenze durch das leistende Unternehmen und den Leistungsempfänger, soweit er Unternehmer ist, an die Steuerverwaltung. Eine generelle Ist-Versteuerung ohne Cross-Check-Verfahren wäre für Zwecke der Umsatzsteuerbetrugsbekämpfung nicht zielführend.

III. Datenschutzrechte von Kindern

14. Sieht die Bundesregierung einen Unterschied zwischen dem Recht auf informationelle Selbstbestimmung von Kindern in Abgrenzung zu dem von Erwachsenen, und wenn ja, wie bewertet die Bundesregierung diesen Unterschied in qualitativer Hinsicht?

Jeder Mensch verfügt über das Recht auf informationelle Selbstbestimmung. Dieses ist nicht altersabhängig und steht auch Minderjährigen zu. Auch diese haben daher insbesondere ein Recht auf Wahrung des Steuergeheimnisses, des Arztgeheimnisses und des Sozialgeheimnisses. Regelungen, die die Verarbeitung personenbezogener Daten von Minderjährigen erlauben, haben dem Gesichtspunkt Rechnung zu tragen, dass Minderjährige im Gegensatz zu Erwachsenen ihre Persönlichkeit erst entwickeln müssen und daher eines besonderen Schutzes bedürfen (vgl. BVerfGE 101, 361, 385; BVerfG NJW 2000, 2191 f.).

Gegenüber den sorgeberechtigten Eltern gilt dies allerdings nur eingeschränkt, da diese sonst als gesetzliche Vertreter ihrer Kinder ihrem Erziehungsauftrag wie auch ihrer Verpflichtung zur Wahrung der Interessen des Kindes Dritten gegenüber nicht hinreichend nachkommen könnten. Abhängig vom Alter und der Einsichtsfähigkeit kann aber ausnahmsweise ein Recht auf informationelle Selbstbestimmung für Minderjährige gegenüber ihren Eltern in Betracht kommen.

Im Strafverfahrensrecht gilt für Kinder nach § 489 Abs. 4 Nr. 4 StPO ein besonderer Schutz des Rechts auf informationelle Selbstbestimmung. Da Kinder nicht Beschuldigte eines Strafverfahrens sein können (§ 19 StGB), sind im Regelfall Speicherungen personenbezogener Informationen von zur Tatzeit Strafunmündigen nicht erforderlich und deswegen unzulässig (vgl. Bundestagsdrucksache 14/1484, Seite 35). In Ausnahmefällen, in denen eine Speicherung dennoch erforderlich ist, sieht das Gesetz deutlich kürzere Speicherfristen als bei Jugendlichen und Erwachsenen vor.

15. Was unternimmt die Bundesregierung, um die Durchsetzung der Datenschutzrechte gerade von Kindern zu fördern?

Da den Kindern gegenüber Dritten die gleichen Datenschutzrechte wie Volljährigen zustehen (siehe Antwort zu Frage 14), bedarf es insoweit keiner besonderen Maßnahmen der Bundesregierung.

16. Wie beurteilt die Bundesregierung das Spannungsverhältnis zwischen dem Recht der Kinder, grundsätzlich selbst über die Preisgabe und Verwendung ihrer Daten zu entscheiden, und dem Erziehungsrecht der Eltern?

Da Datenschutzrechte der Kinder gegenüber den Eltern als ihren gesetzlichen Vertretern nur ausnahmsweise bestehen (siehe Antwort zu Frage 14), kann es nur in besonderen Fällen zu einem Spannungsverhältnis kommen. Dabei ist zwischen dem Recht des Kindes, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu entscheiden, und den Erfordernissen der Betreuung und Erziehung durch die Sorgeberechtigten abzuwägen. Danach ist zu entscheiden, ob und wieweit die Schutzrechte des Kindes gegenüber den Sorgeberechtigten einzuschränken sind. Dies kann auch nach dem Alter und der Einsichtsfähigkeit des Kindes jeweils unterschiedlich zu beurteilen sein. Entscheidend ist in jedem Fall allein das Wohl des Kindes.

17. Wie bewertet die Bundesregierung die Sicherheit der Daten von Kindern, die bei der Benutzung des Internets zur Angabe von Daten durch Lockangebote verleitet werden?

Die Rechte und Pflichten zum Schutz der personenbezogenen Daten der Nutzer von Internetangeboten sind im Teledienste-Datenschutz-Gesetz (TDDSG) des Bundes und weitestgehend gleich lautend im Mediendienstestaatsvertrag (MDStV) der Länder geregelt. Deren spezifische Bestimmungen zum Datenschutz ergänzen die allgemeinen Vorschriften des BDSG. Die genannten Regelwerke enthalten keine besonderen Bestimmungen zum Schutz der personenbezogenen Daten von Kindern. Vielmehr werden alle Nutzer bei der Verarbeitung personenbezogener Daten durch Diensteanbieter gleichermaßen geschützt. Dabei zielen die Vorschriften und der Ansatz einer spezifischen Regelung gerade darauf ab, der ausufernden Datenverarbeitung, die mit der Nutzung der neuen Dienste einhergeht, entgegenzuwirken und ihr enge rechtliche Grenzen zu setzen. So ist die Datenverarbeitung gesetzlich nur erlaubt, wenn dies für die Ermöglichung des Dienstes oder zur Abrechnung des Dienstes erforderlich ist. Insbesondere hat der Diensteanbieter die Inanspruchnahme von Telediensten oder Mediendiensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die Nutzer sind über diese Möglichkeit zu informieren (vgl. § 4 Abs. 6 TDDSG, § 18 Abs. 6 MDStV). Jede darüber hinausgehende Erhebung von personenbezogenen Daten bedarf der Einwilligung der betroffenen Person.

Vor diesem Hintergrund ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Diensteanbieter im Internet, die über die gesetzlichen Erlaubnistatbestände des TDDSG/MDStV hinausgeht, rechtlich nur zulässig, wenn die Nutzer darüber entsprechend den Anforderungen des Gesetzes unterrichtet werden und ausdrücklich eingewilligt haben. Bei Kindern und insbesondere den hier genannten Lockangeboten dürften diese Anforderungen nicht erfüllt sein, denn Kinder können grundsätzlich nicht ohne das Einverständnis ihrer Eltern in die Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten einwilligen.

Die Aufsicht über die Einhaltung der Datenschutzvorschriften für Tele- und Mediendienste ist Sache der Länder. Die zuständigen Aufsichtsbehörden können entsprechende Maßnahmen gegen die rechtswidrige Verarbeitung von personenbezogenen Daten durch Diensteanbieter ergreifen. Verstöße gegen die Datenschutzvorschriften des TDDSG/MDStV sind als Ordnungswidrigkeit bußgeldbewehrt.

Die hohen Anforderungen des Datenschutzes im TDDSG und im MDStV haben dazu beigetragen, dass heute eine sehr hohe Sensibilität auf Nutzerseite im Hinblick auf den Schutz ihrer personenbezogenen Daten im Internet besteht. Es ist daher davon auszugehen, dass Eltern und Schule diese Sensibilität im Rahmen ihrer Erziehung und ihres Bildungsauftrages an Kinder und Jugendliche weitergeben.

18. Wie beurteilt die Bundesregierung aus datenschutzrechtlicher Sicht Angebote GPS-basierter Handydienste wie „Track your kid“, die es ermöglichen, den Aufenthaltsort eines Handynutzers, insbesondere von Kindern, festzustellen, und wessen Recht ist im Sinne des in Frage 16 skizzierten Spannungsverhältnisses stärker zu gewichten, das der Kinder oder das der Eltern?

Standortdaten dürfen nach § 98 Abs. 1 Satz 1 des Telekommunikationsgesetzes (TKG) nur mit Einwilligung des Teilnehmers in dem zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß verarbeitet werden. Das Tatbestandsmerkmal „Teilnehmer“ verlangt nach § 3 Nr. 20 TKG ein Vertragsverhältnis über die Erbringung von Telekommunikationsdiensten. Minderjährige können daher grundsätzlich nicht Teilnehmer sein, wohl aber „Nutzer“ im Sinne von § 3 Nr. 14 TKG. Der Teilnehmer hat Mitbenutzer nach § 98 Abs. 1 Satz 2 TKG über die erteilte Einwilligung zur Verarbeitung von Standortdaten zu unterrichten.

Bei der Pflege und Erziehung berücksichtigen die Eltern nach § 1626 Abs. 2 BGB die wachsende Fähigkeit und das wachsende Bedürfnis des Kindes zu selbständigem verantwortungsbewusstem Handeln. Sie besprechen mit ihm, soweit es nach dessen Entwicklungsstand angezeigt ist, Fragen der elterlichen Sorge und streben Einvernehmen an. Dabei ist das Recht des Kindes auf informationelle Selbstbestimmung zu berücksichtigen.

19. Sieht die Bundesregierung die informationelle Selbstbestimmung von Kindern und Jugendlichen durch derart lokalisierbare Handys gefährdet, wenn ja, welche Möglichkeiten des Schutzes der informationellen Selbstbestimmung Minderjähriger sieht sie, bzw. wenn nein, warum nicht?

Auf die Antwort zu Frage 18 wird verwiesen.

20. Wie begründet die Bundesregierung die Vergabe einer Identifikationsnummer für Neugeborene nach § 139a AO unabhängig von einer etwaigen Steuerpflicht, und welche datenschutzrechtlichen Probleme wirft dieses Vorgehen auf?

Nach § 1 Abs. 1 Satz 1 EStG ist jede natürliche Person unbeschränkt steuerpflichtig, die ihren Wohnsitz oder ihren gewöhnlichen Aufenthaltsort im Inland hat. Von der Frage der Steuerpflicht zu trennen ist die daran anschließende Frage, inwieweit diese Person auch konkret Einkommensteuer schuldet. Diese Frage richtet sich nach den Umständen des Einzelfalls.

Neugeborene können im Einzelfall, zum Beispiel in Erb- oder Schenkungsfällen, bereits Einkommensteuer schulden. Andererseits schulden nicht alle volljährigen Personen zwangsläufig Einkommensteuer. § 139a AO sieht daher die Vergabe der steuerlichen Identifikationsnummer bereits bei Eintritt der abstrakten Steuerpflicht nach dem Einkommensteuergesetz vor. Damit wird zugleich sichergestellt, dass steuerlich relevante Daten, die eine bestimmte Person betreffen, in jedem Fall zweifelsfrei zugeordnet werden können.

Datenschutzrechtliche Probleme werden hierdurch nicht aufgeworfen, da es sich bei der Identifikationsnummer um ein bereichsspezifisches Ordnungsmerkmal handelt, welches strengen Zweckbindungsvorschriften unterliegt. Darüber hinaus hat das Gesetz zur Umsetzung von EU-Richtlinien in nationales Steuerrecht und zur Änderung weiterer Vorschriften vom 9. Dezember 2004 auf Anregung des Bundesbeauftragten für den Datenschutz einen Bußgeldtatbestand für den Fall zweckwidriger Verwendung des steuerlichen Identifikationsmerkmals geschaffen.

21. Plant die Bundesregierung vor Erlass der zur Umsetzung dieses Vorhabens noch erforderlichen Verordnung die Datenschutzbeauftragen des Bundes und der Länder zu den datenschutzrelevanten Aspekten anzuhören?

Der Bundesbeauftragte für den Datenschutz wird bei Erlass der Rechtsverordnung zu § 139d AO beteiligt werden. Die Beteiligung der Datenschutzbeauftragten der Länder ist Angelegenheit der Länder, die der Rechtsverordnung im Bundesrat zustimmen müssen.

22. Welche Erkenntnisse hat die Bundesregierung hinsichtlich der tatsächlichen Praxis bei der Einholung des elterlichen Einverständnisses für ein Neugeborenen-Screening in den jeweiligen Krankenhäusern und Kliniken, und hält die Bundesregierung dieses Vorgehen für ausreichend gemäß § 4a BDSG?

Eltern müssen vor der Probennahme über die Ziele, Inhalte und mögliche Folgen des Neugeborenen-Screenings, über die Risiken der Gewinnung der Probe, über deren Verwertung sowie über die Verwendung der erhobenen Daten angemessen informiert werden. Wie andere freiwillige medizinische Maßnahmen erfordert das Screening die in der Krankenakte dokumentierte Einwilligung des gesetzlichen Vertreters des Neugeborenen. Die Einwilligung muss den Anforderungen des § 4a BDSG entsprechen. In der Regel wird die Einwilligung in ein Neugeborenen-Screening im Rahmen des Behandlungsvertrages erteilt, den die Eltern mit dem Krankenhaus, der Hebamme oder dem Kinderarzt abschließen.

Erkenntnisse hinsichtlich der tatsächlichen Praxis bei der Einholung des elterlichen Einverständnisses für ein Neugeborenen-Screening in den jeweiligen Krankenhäusern und Kliniken liegen der Bundesregierung nicht vor. Auskünfte hierüber können nur die Länder erteilen, die im Übrigen auch für die stationäre Krankenhausversorgung und Überwachung der Einhaltung des ärztlichen Berufsrechts sowie für die Kontrolle der Beachtung datenschutzrechtlicher Vorschriften durch öffentliche Stellen der Länder und durch nichtöffentliche Stellen zuständig sind.

Im Übrigen wird auf die Antwort der Bundesregierung vom 23. September 2003 zu Frage 4 der Kleinen Anfrage der Fraktion der FDP „Rechtsstaatlicher Umgang mit Restblutproben beim Neugeborenen-Screening“ (Bundestagsdrucksache 15/1610) verwiesen.

23. Wie weit sind die Arbeiten an einem Gesetzentwurf der Bundesregierung über genetische Untersuchungen bei Menschen vorangeschritten, und welche konkreten Regelungen in Bezug auf ein Neugeborenen-Screening und eine Gen-Datei soll dieses Gesetz enthalten?

Die Bundesregierung hat unter Federführung des Bundesministeriums für Gesundheit und Soziale Sicherung entsprechend der im Koalitionsvertrag der Regierungsparteien geschlossenen Vereinbarung einen Diskussionsentwurf für ein Gendiagnostikgesetz erstellt, der zurzeit von einer Arbeitsgruppe der Koalitionsfraktionen im Deutschen Bundestag beraten wird. In dem Gesetz sollen unter anderem die Gewinnung und Verwertung genetischer Proben sowie die Gewinnung und Verwendung genetischer Daten geregelt werden, wobei auch genetische Reihenuntersuchungen bei Neugeborenen erfasst werden sollen. Der Entwurf sieht sachgerechte Bestimmungen zum Datenschutz vor.

Im Übrigen wird auf die Antwort der Bundesregierung vom 12. November 2004 auf die Kleine Anfrage der Fraktion der FDP „Massen-Gentests bei Krankenkassen“ (Bundestagsdrucksache 15/4221) verwiesen.

IV. Biometrische Daten

24. Welche Verfahren zur Verwendung biometrischer Daten zur Identifizierung von Personen sind nach Kenntnis der Bundesregierung nach derzeitigem Stand der Technik für den Einsatz in der Praxis verfügbar?

Für einen Praxiseinsatz sind derzeit Gesichtserkennung, Fingerabdruckerkennung und Iriserkennung verfügbar.

25. Welche Verfahren favorisiert die Bundesregierung für Reisepässe und andere Ausweisdokumente, und aus welchen Gründen?

Biometrische Verfahren für Reisepässe und andere Ausweisdokumente entfalten nur dann ihren Nutzen, wenn sie in Abstimmung mit den Partnerländern in und außerhalb der EU eingesetzt werden können. Hierfür ist ein gemeinsamer Standard unerlässlich, der die Interoperabilität der eingesetzten Biometrie-Lösungen sicherstellt.

Die internationalen Standards für Reisedokumente werden von der International Civil Aviation Organization (ICAO), einer Unterorganisation der Vereinten Nationen, festgelegt. Sie hat sich bei der Frage der Implementierung biometrischer Merkmale in Reisedokumente für das Gesicht als primäres biometrisches Merkmal ausgesprochen. Alternativ oder zusätzlich können Fingerabdrücke und das Bild der Iris aufgenommen werden.

Mitte 2003 haben sich die EU-Staatschefs in Thessaloniki auf ein Gesamtkonzept zur Einführung von Biometrie in Pässen, Visa und Aufenthaltstitel und Aufnahme biometrischer Merkmale in das Visainformationssystem (VIS) geeinigt. Technische Spezifikationen für Einführung von Biometrie-Dokumenten werden unter deutscher Beteiligung auf Grundlage der ICAO-Spezifikationen in drei Arbeitsgruppen erstellt.

Hinsichtlich der Herausgabe von Reisepässen hat der Rat für Justiz und Inneres am 25./26. Oktober 2004 politisches Einvernehmen erzielt, stufenweise die beiden biometrischen Merkmale Gesichtsbild und Fingerabdruck verbindlich festzulegen. Das Gesichtsbild soll binnen 18 Monaten nach Festlegung der technischen Spezifikationen, der Fingerabdruck binnen 36 Monaten als biometrisches Merkmal in den EU-Reisepass aufgenommen werden. Die Regelung wurde im Allgemeinen Rat am 16./17. Dezember 2004 verabschiedet. Mit der Festlegung der technischen Spezifikationen ist im Januar 2005 zu rechnen.

Die Bundesregierung beabsichtigt, im Herbst 2005 mit der Ausgabe interoperabler, biometriegestützter Pässe zu beginnen.

Die Einführung eines neuen Personalausweises mit biometrischen Daten und einer Bürgerkartenfunktion einschließlich elektronischer Unterschrift zur Verwendung im elektronischen Geschäftsverkehr wird für das Jahr 2007 angestrebt.

26. Auf welche Verfahren haben sich die EU-Justiz- und -Innenminister geeinigt, und aufgrund welcher Überlegungen?

Auf die Antwort zu Frage 25 wird verwiesen.

27. Plant die Bundesregierung die Aufnahme zusätzlicher biometrischer Merkmale außer solchen, auf die sich die EU verständigen wird, und falls ja, welche zusätzlichen Merkmale will die Bundesregierung warum aufnehmen, und wird sie diese mit anderen Staaten, z. B. den USA, abstimmen bzw. sich von deren Vorstellungen leiten lassen?

Über die Aufnahme biometrischer Merkmale ist im europäischen Kontext, abgestimmt mit den USA, entschieden worden. Eine darüber hinausgehende Aufnahme weiterer biometrischer Merkmale ist nicht geplant.

28. Welche Erkenntnisse hat die Bundesregierung aus den laufenden Pilotprojekten zur Verwendung biometrischer Daten zur Identifizierung von Personen, z. B. Automatisierte Biometriegestützte Grenzkontrolle (ABG) oder BIOPII am Frankfurter Flughafen, bereits heute gewonnen, und wann ist mit einem Abschlussbericht zu rechnen?

Das im Februar 2004 zunächst für 6 Monate begonnene Pilotprojekt der Automatisierten und Biometriegestützten Grenzkontrolle (ABG) ist im August 2004 um weitere 12 Monate verlängert worden. Ein Abschlussbericht ist erst danach zu erwarten.

Der Abschlussbericht zum Projekt BIOPII wird zum Jahresende 2004 erwartet. Zuvor können keine verlässlichen Aussagen über die getesteten biometrischen Verfahren getroffen werden, weil die Auswertungen nicht abgeschlossen sind.

29. In welchem Umfang und zu welchen Zwecken werden biometrische Daten zur Identifizierung von Personen bereits neben dem Projekt am Frankfurter Flughafen von Behörden genutzt?

Das Auswärtige Amt führt in Zusammenarbeit mit dem Bundesministerium des Innern seit dem 19. Mai 2003 ein Pilotprojekt an der Außenstelle der Botschaft Abuja in Lagos, Nigeria, durch. Nach § 49 Abs. 3 Nr. 5 des Aufenthaltsgesetzes (AufenthG) ist die Möglichkeit von Maßnahmen zur Feststellung und Sicherung der Identität von Visaantragstellern bei Anträgen für eine Aufenthaltsdauer von mehr als drei Monaten vorgesehen, wenn der Antragsteller aus einem so genannten Risikostaat (§ 73 Abs. 4 AufenthG) oder einem Staat kommt, bei dem Rückführungsschwierigkeiten bestehen. Da dies bei Nigeria der Fall ist, werden von allen Antragstellern, die einen Daueraufenthalt in Deutschland beantragen, Fingerabdrücke genommen und auf elektronischem Wege an das Bundeskriminalamt übermittelt. Das Pilotprojekt wurde darüber hinaus im April 2004 um eine Komponente „Gesichtsbiometrie“ erweitert.

Ferner werden in begründeten Einzelfällen biometrische Daten (in der Regel Fingerabdrücke) auf Ersuchen von Ausländerbehörden in deutschen Auslandsvertretungen erfasst, sofern sich im Visumantragsverfahren Hinweise ergeben, die identitätssichernde Maßnahmen erfordern.

Darüber hinaus setzt der Bundesnachrichtendienst ein biometrisches Personenidentifizierungssystem zur Eingangskontrolle ein.

30. Welche Verfahren sind aus Sicht der Bundesregierung am besten mit den Grundsätzen des deutschen und europäischen Datenschutzrechts zu vereinbaren, und warum?

Aus Sicht der Bundesregierung muss eine Technologie zum Einsatz kommen, die die Ziele der höheren Dokumentensicherheit und der besseren Identifizierbarkeit der Dokumenteninhaber mit dem geringstmöglichen Eingriff in die Rechte der Betroffenen erreicht. Da sich alle in Betracht kommenden Verfahren hinsichtlich der Eingriffstiefe kaum unterscheiden dürften, kommt es vor allem darauf an, welche technisch-organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes getroffen werden können (zum Beispiel Art und Ort der Speicherung der biometrischen Merkmale, Verschlüsselung etc.). Die Bundesregierung lässt derzeit die verschiedenen Verfahren auch unter diesen Gesichtspunkten untersuchen. Geprüft werden Iris-, Gesichts- und Fingerabdruckerkennung.

V. Gesundheitssystem

31. Trifft es zu, dass der Bundesbeauftragte für den Datenschutz den ihm zur datenschutzrechtlichen Prüfung des Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung (GMG) zur Verfügung stehenden sehr knapp bemessenen Zeitrahmen kritisiert hat, und wenn ja, was war Inhalt seiner Kritik?

Der Zeitrahmen zur Erarbeitung, Prüfung und Beschlussfassung eines Gesetzes zur Modernisierung der Gesetzlichen Krankenversicherung (GMG) war von dem Ablauf der Konsensverhandlungen zwischen den Fraktionen SPD, CDU/CSU und BÜNDNIS 90/DIE GRÜNEN geprägt. Der Zeitraum zwischen dem Vorliegen der Eckpunkte der Konsensverhandlungen zur Gesundheitsreform am 22. Juli 2003 bis zur Beschlussfassung des Deutschen Bundestages am 26. September 2003 war für alle Beteiligten knapp bemessen.

Der Bundesbeauftragte für den Datenschutz wurde vom Bundesministerium für Gesundheit und Soziale Sicherung unverzüglich mit Schreiben vom 11. August 2003 um eine erste datenschutzrechtliche Einschätzung von Änderungen im Zusammenhang mit der Umsetzung der Eckpunkte der Konsensverhandlungen der Gesundheitsreform gebeten. Die fünfseitige Stellungnahme des Bundesbeauftragten für den Datenschutz ging am Freitag, den 15. August 2003 beim Bundesministerium für Gesundheit und Soziale Sicherung per Fax ein. In diesem Schreiben machte der Bundesbeauftragte für den Datenschutz gegen die Änderung des Abrechnungsverfahrens zwischen Kassenärztlicher Vereinigung und Krankenkasse wegen der versichertenbezogenen Übermittlung der ärztlichen Abrechnungsdaten datenschutzrechtliche Bedenken geltend. Diese Änderung war zur Reform des bisherigen Vergütungssystems der niedergelassenen Vertragsärzte (Ablösung der Gesamtvergütung durch Regelleistungsvolumina) erforderlich.

Nach einem Gespräch am 15. September 2003 mit dem Bundesministerium für Gesundheit und Soziale Sicherung hat der Bundesbeauftragte für den Datenschutz in Abstimmung mit dem Bundesministerium für Gesundheit und Soziale

Sicherung Formulierungsvorschläge für den Ausschussbericht und für einen Entschließungsentwurf des Deutschen Bundestages erarbeitet. Diese Vorschläge hatte der Bundesbeauftragte für den Datenschutz mit Schreiben vom 19. September 2003 dem Vorsitzenden des Ausschusses für Gesundheit und Soziale Sicherung des Deutschen Bundestages sowie den Gesundheitspolitischen Sprechern der Fraktionen der SPD, CDU/CSU, BÜNDNIS 90/DIE GRÜNEN sowie der FDP übersandt. Der Ausschuss hat sie in seinem Bericht (Bundestagsdrucksache 15/1584, Seite 11) unverändert übernommen und der Deutsche Bundestag hat sie als Entschließung wie vorgeschlagen beschlossen (siehe 64. Sitzung am 26. September 2003, Plenarprotokoll 15/64, Seite 5475 (C)).

32. Trifft es ferner zu, dass der Bundesbeauftragte für den Datenschutz die Regelungen des Gesetzes dahin gehend beurteilt hat, dass ein Paradigmenwechsel stattfinde, der sehr tief in das Selbstbestimmungsrecht der Versicherten eingreife, und wenn ja, wie hat er seine diesbezügliche Auffassung begründet, und was ist die Auffassung der Bundesregierung hierzu?

Die Auffassung des Bundesbeauftragten für den Datenschutz ergibt sich aus den in Frage 31 angeführten Schreiben des Bundesbeauftragten für den Datenschutz vom 19. September 2003, unter anderem an den Vorsitzenden des Ausschusses für Gesundheit und Soziale Sicherung des Deutschen Bundestages sowie an die gesundheitspolitischen Sprecher der Bundestagsfraktionen, darunter auch an den Abgeordneten Dr. Dieter Thomae, FDP.

Wie bereits zu Frage 31 ausgeführt, hat der Deutsche Bundestag fraktionsübergreifend den aus der Konsensrunde resultierenden gesetzlichen Vorschlägen zugestimmt. Die Bundesregierung sieht keine Veranlassung, die Rechtmäßigkeit der vom Bundestag und Bundesrat beschlossenen gesetzlichen Regelungen in Frage zu stellen.

33. Welche detaillierte datenschutzrechtliche Prüfung der Konsequenzen aus der Einführung des GMG hat die Bundesregierung mit welchem Ergebnis durchgeführt?

Über die vom Deutschen Bundestag und vom Bundesrat beschlossenen gesetzlichen Regelungen hinaus erwartet der Deutsche Bundestag Erkenntnisse aus dem bis Ende 2008 vorzulegenden Bericht des Bundesministeriums für Gesundheit und Soziale Sicherung über die datenschutzrechtliche Evaluierung der Spitzenverbände der Krankenkassen, insbesondere auch zur Frage der Anwendung von Pseudonymisierungsverfahren.

34. Welche Möglichkeiten werden für den Patienten bei der geplanten elektronischen Patientenkarte bestehen, Art und Umfang der gespeicherten Daten zu beeinflussen und Informationen hierüber zu erhalten?

Die Gewährleistung der Entscheidungsfreiheit der Versicherten über die Speicherung und die Verwendung der auf der elektronischen Gesundheitskarte gespeicherten medizinischen Daten ist einer der wichtigsten Grundsätze bei der Konzeption der Gesundheitskarte. Der medizinische Teil der Gesundheitskarte soll nur auf freiwilliger Basis genutzt werden können. Das bedeutet, dass alle Versicherten zwar eine Gesundheitskarte erhalten, mit der administrative Funktionen wie die Abwicklung des elektronischen Rezepts erledigt werden, es ihnen darüber hinaus aber freigestellt wird, die zusätzlichen Funktionen, also den medizinischen Teil, zu nutzen oder nicht. Die Versicherten können selbst ent-

scheiden, ob und welche ihrer Gesundheitsdaten gespeichert werden. Dementsprechend sehen die Regelungen in § 291a Abs. 3 Satz 3 Sozialgesetzbuch V (SGB V) vor, dass mit dem Erheben, Verarbeiten und Nutzen von Daten der Versicherten erst begonnen werden darf, wenn die Versicherten jeweils gegenüber dem Arzt, Zahnarzt oder Apotheker dazu ihre Einwilligung erklärt haben. Die Einwilligung ist nach § 291a Abs. 3 Satz 4 SGB V bei der ersten Verwendung der Karte vom Leistungserbringer auf der Karte zu dokumentieren; sie ist jederzeit widerruflich und kann auf einzelne der in § 291a Abs. 3 Satz 1 SGB V genannten Anwendungen beschränkt werden.

Den Versicherten steht darüber hinaus das Recht zu, alle über sie gespeicherten Daten einzusehen und Ausdrucke hiervon zu erhalten.

Auf Verlangen der Versicherten müssen Daten, soweit es sich nicht um Vertragsdaten nach § 291 Abs. 2 Satz 1 bzw. Rezeptdaten handelt, die noch zu Abrechnungszwecken benötigt werden, gelöscht werden.

35. In welcher Art und Weise soll der Patient sein Recht wahrnehmen, einem gemäß § 291a Abs. 5 Satz 3 Fünftes Buch Sozialgesetzbuch (SGB V) grundsätzlich zugriffsberechtigten Arzt, Zahnarzt oder Apotheker den Einblick in Teile der medizinischen Dokumentationsdaten zu verwehren, die insgesamt gespeichert sind?

Durch technische Vorkehrungen wird gewährleistet, dass nur mit Einverständnis der Versicherten durch hierzu berechtigte Ärzte, Zahnärzte und Apotheker unter Einsatz ihres elektronischen Heilberufsausweises auf die Gesundheitskarte zugegriffen werden kann.

Die Patienten können ihr Recht, grundsätzlich zugriffsberechtigten Ärzten, Zahnärzten oder Apothekern den Einblick in Teile der medizinischen Daten zu verwehren, dadurch ausüben, dass sie die zur Einsicht erforderliche technische Autorisierung (zum Beispiel mittels einer PIN) nicht durchführen. Sie halten damit stets den Schlüssel zu ihren Daten in der Hand. Weitere Details sind im Rahmen der jetzt zu erarbeitenden Lösungsarchitektur festzulegen.

36. Wie kann sichergestellt werden, dass es nicht zu einer zentral gespeicherten Datensammlung über Patienten kommt, insbesondere im Rahmen der Vereinbarung der Partner der Selbstverwaltung gemäß § 291a Abs. 7 SGB V über die erforderliche Informations-, Kommunikations- und Sicherheitsinfrastruktur?

Durch die Gesundheitskarte wird die Gefahr einer Zentrierung personenbezogener Daten nicht vergrößert. Medizinische Daten der Versicherten werden nur dann mittels der Gesundheitskarte gespeichert, wenn der Versicherte hierzu seine Einwilligung erteilt. Das Sicherheitskonzept sieht vor, dass Daten auf Servern grundsätzlich nur verschlüsselt gespeichert werden und nur mittels der Gesundheitskarte wieder entschlüsselt werden können. Mit den Spitzen der Selbstverwaltung wurde am 28. Oktober 2004 vereinbart, dass das Bundesministerium für Gesundheit und Soziale Sicherung ein Gesetzgebungsverfahren zur Verankerung einer Betriebsorganisation einleiten wird, die die Aufgaben der Vertragsgemeinschaft nach § 291a Abs. 7 SGB V übernimmt. Damit die Rechte der Versicherten im Hinblick auf die Verwendung ihrer Daten auch im Rahmen der von der Betriebsorganisation zu erarbeitenden Informations-, Kommunikations- und Sicherheitsinfrastruktur sichergestellt werden, ist vorgesehen, dass die entsprechenden Beschlüsse der Betriebsorganisation durch das Bundesministerium für Gesundheit und Soziale Sicherung unter Beteiligung des Bundesbeauftragten für den Datenschutz geprüft und gegebenenfalls beanstandet werden können.

37. Wie bewertet die Bundesregierung allgemein die Gefahr, dass gesetzlich Krankenversicherte trotz der Bestimmungen des § 291a Abs. 6 und 8 SGB V sozialem, medizinischem oder sonstigem Druck ausgesetzt werden, Daten ihrer elektronischen Gesundheitskarten zu offenbaren?

Die Gefahr, dass Unbefugte Einsicht in Patientendaten nehmen oder sich diese erzwingen, ist nach Auffassung der Bundesregierung durch die neuen gesetzlichen Regelungen sogar reduziert worden. Denn nach § 291a Abs. 5 Satz 3 SGB V ist durch technische Vorkehrungen zu gewährleisten, dass der Zugriff auf medizinische Daten der Gesundheitskarte grundsätzlich nur mit einem elektronischen Heilberufsausweis möglich ist. Darüber hinaus ist nach § 291a Abs. 6 Satz 2 SGB V eine Protokollierung der Zugriffe zu gewährleisten. Damit bestehen ausreichende Schutzmaßnahmen gegen einen unberechtigten Zugriff, zum Beispiel durch Arbeitgeber. Der Schutz vor Missbrauch der Gesundheitsdaten wird zusätzlich durch spezielle Straf- und Bußgeldvorschriften gestärkt.

38. Durch welche technischen und organisatorischen Maßnahmen soll über die gesetzlichen Bestimmungen des § 291a Abs. 6 und 8 SGB V hinaus nach den Vorstellungen der Bundesregierung sichergestellt werden, dass Versicherte in ihrer Eigenschaft als Arbeit- oder Versicherungsnehmer nicht dem Druck ausgesetzt werden, medizinische Daten ihrer Gesundheitskarte Dritten gegenüber zugänglich zu machen?

Auf die Antwort zu Frage 37 wird verwiesen.

39. Hält die Bundesregierung den technischen Schutz der Gesundheitskarte für ausreichend, um einen missbräuchlichen Zugriff Dritter auf die Daten ausschließen zu können, und wie begründet sie ihre diesbezügliche Auffassung?

Die Bundesregierung hält die gesetzlichen Regelungen für Schutzmaßnahmen gegen einen missbräuchlichen Zugriff Dritter auf die Daten der Gesundheitskarte für ausreichend. Um sicherzustellen, dass die Gesundheitskarte den in der Antwort zu Frage 37 erwähnten gesetzlichen Vorgaben ausreichend Rechnung trägt, werden insbesondere der Bundesbeauftragte für den Datenschutz und das Bundesamt für Sicherheit in der Informationstechnik eng in die Arbeiten einbezogen.

40. Soll für Ärzte die Möglichkeit bestehen, die auf den geplanten Patientenkarten gespeicherten Daten z. B. anderer Ärzte in die eigene Patientenerfassung einzufügen, zu speichern und zu verwenden, und wenn ja, welche Speicherfristen sollen in diesem Fall gelten?

Für Ärzte soll die Möglichkeit bestehen, die auf der Gesundheitskarte gespeicherten Daten in die eigene Patientenerfassung einzufügen, zu speichern und zu verwenden, wie dies derzeit auch bei Daten geschieht, die andere Leistungserbringer zur Verfügung stellen. Die Übernahme und Integration von Daten verschiedener Systeme soll dazu beitragen, Arbeitsprozesse effektiver zu gestalten und dadurch auch Zeit zu sparen, die für die Behandlung der Patientinnen und Patienten eingesetzt werden kann. Selbstverständlich sind diese Vorgänge nur mit Einwilligung der Versicherten zulässig. Die Speicherfrist richtet sich nach den allgemeinen berufsrechtlichen Regelungen.

41. Entspricht die Zuordnung aller in der gesetzlichen Krankenversicherung Versicherten zu Risikoklassen gemäß § 85a, b SGB V einer zu erwartenden Behandlungsnotwendigkeit und -intensität der Patienten, und ermöglicht sie somit zukünftig Aussagen über die zu erwartenden Behandlungskosten jedes Versicherten?

Diagnosebezogene Risikoklassen-Verfahren sind eine international angewandte Methodik zur Schätzung der Morbidität und des daraus resultierenden Behandlungsbedarfs von Versichertenpopulationen. Vergütungssysteme, die sich an direkten Morbiditätsindikatoren orientieren, können Versorgungsanforderungen deutlich realitätsnäher abbilden als Verfahren, die sich nur an indirekten Parametern wie zum Beispiel Alter und Geschlecht ausrichten. Der theoretisch vorhersagbare Anteil der Kostenvariationen wird in prospektiven Verfahren in der Literatur auf drei- bis zu viermal höher geschätzt. Je kleiner die Populationen sind, auf die die Risikoklassen-Methodik angewandt wird, desto problematischer ist die Güte bzw. Vorhersagekraft dieser Schätzung.

Die gesetzlichen Regelungen zur vertragsärztlichen Vergütung sehen eine Anwendung des Risikoklassen-Verfahrens nur zwischen den Krankenkassen (als Versichertengemeinschaft) und den Kassenärztlichen Vereinigungen (als Leistungserbringergemeinschaft) vor. Nach den gesetzlichen Vorgaben ist eine Anwendung dieses Verfahrens mit dem Zweck, Aussagen über die zu erwartenden Behandlungskosten für einzelne Versicherte zu treffen, nicht vorgesehen und insoweit unzulässig.

42. Hält die Bundesregierung den Grundsatz der Verhältnismäßigkeit für gewahrt, wenn solche sehr sensiblen privaten Daten von allen gesetzlich Krankenversicherten mit der Zielsetzung gesammelt und verarbeitet werden dürfen, ein neues Abrechnungsverfahren für ärztliche Leistungen im ambulanten Bereich einzuführen?

Wie bereits in der Antwort zu Frage 31 ausgeführt, hat der Deutsche Bundestag fraktionsübergreifend den aus der Konsensrunde resultierenden gesetzlichen Vorschlägen zugestimmt. Die Bundesregierung sieht keine Veranlassung, die Rechtmäßigkeit der vom Deutschen Bundestag und vom Bundesrat beschlossenen gesetzlichen Regelungen in Frage zu stellen.

Auf der Grundlage der vom Deutschen Bundestag in seiner Entschließung geforderten datenschutzrechtlichen Evaluationserfahrungen der Spitzenverbände der Krankenkassen, auch zur Verhältnismäßigkeit der Maßnahmen, wird das Bundesministerium für Gesundheit und Soziale Sicherung gebeten, dem Deutschen Bundestag bis Ende 2008 zu berichten.

43. Welche Voraussetzungen müssen nach Auffassung der Bundesregierung an eine Schweigepflichtentbindung zur Übermittlung von Patientendaten an Krankenversicherer gestellt werden?

Die Entbindung von der ärztlichen Schweigepflicht erfolgt durch Einwilligung der Patienten in die entsprechende Datenübermittlung. Da es sich um besonders sensible Gesundheitsdaten handelt (vgl. §§ 3 Abs. 9 BDSG, 67 Abs. 12 SGB X), muss die Einwilligung besonderen Erfordernissen genügen. Diese sind allgemein in § 4a Abs. 1 und 3 BDSG sowie, für die Sozialdatenverarbeitung, in §§ 67a Abs. 1 Satz 4, 67b Abs. 1 Satz 2 und Abs. 2 SGB X geregelt.

Die Träger der gesetzlichen Krankenversicherung dürfen Sozialdaten auf gesetzlicher Grundlage erheben, verarbeiten und nutzen. Das SGB V enthält im zehnten Kapitel (§§ 284 bis 305b SGB V) bereichsspezifische Datenverarbeitungsregelungen. Diese und weitere Vorschriften des SGB V, zum Beispiel die

Vorschriften über den Medizinischen Dienst der Krankenversicherung, bestimmen, welche Daten die Krankenkassen in welchem Umfang und zu welchem Zweck verwenden dürfen und inwieweit Ärzte und sonstige, einer Schweigepflicht unterliegende Leistungserbringer befugt und sogar verpflichtet sind, Daten an die Krankenkassen zu übermitteln.

Träger der privaten Krankenversicherung dürfen Patientendaten auch auf der Grundlage von § 28 Abs. 6 bis 8 BDSG erheben und verwenden.

44. Wie bewertet die Bundesregierung die derzeit gängige Praxis der pauschalen vorab erteilten Schweigepflichtentbindung?

Der Bundesregierung ist eine derzeit gängige Praxis einer pauschalen, vorab erteilten Schweigepflichtentbindung nicht bekannt.

Eine Schweigepflichtentbindung, d. h. eine Einwilligung in eine Übermittlung von Gesundheitsdaten, ist nur wirksam, wenn sie nach entsprechender Aufklärung des Patienten oder der Patientin sowie hinreichend bestimmt erfolgt (vgl. § 4a Abs. 1 und 3 BDSG). Pauschale Erklärungen, die „vorab", also in der Regel in Unkenntnis von Zweck, Umfang und Empfänger der Übermittlung abgegeben werden, dürften diesen Vorgaben nicht entsprechen und demnach unwirksam sein. Dies aber immer nur im Hinblick auf den Einzelfall zu beurteilen.

Da zwischen den datenschutzrechtlichen Aufsichtsbehörden der Länder und dem Gesamtverband der Deutschen Versicherungswirtschaft e. V. im Einzelnen unterschiedliche Rechtsauffassungen im Hinblick auf eine Schweigepflicht-Entbindungserklärung vor Behandlungsbeginn bestehen, holen beispielsweise vielfach die behandelnden Ärzte beim Patienten eine besondere, zusätzliche Entbindungserklärung ein, wenn die privaten Krankenversicherungen bei ihnen Behandlungsunterlagen anfordern. Andere Versicherer fordern die Unterlagen über die Versicherten an. Die Bundesregierung begrüßt und begleitet die Beratungen im „Düsseldorfer Kreis", in dem sich die Aufsichtsbehörden auch zu diesem Thema abstimmen. In der dortigen Arbeitsgemeinschaft Versicherungswirtschaft wird derzeit nach einer datenschutzrechtlich zweifelsfreien Lösung der angesprochenen Frage gesucht. Dabei tauscht sich die Arbeitsgemeinschaft auch mit Vertretern der Versicherungswirtschaft aus.

VI. Wirtschaft

45. Hat die Bundesregierung Informationen darüber, in welchem Umfang personenbezogene Daten bei Kundenbindungsprogrammen wie dem Rabattverfahren der Kundenkarte, die Auskunft über das Konsumverhalten und die Interessen der Verbraucher geben, erfasst werden?

Der Bundesregierung sind nur Schätzungen über die Zahl der derzeit in Deutschland ausgegebenen Rabatt- oder Kundenkarten bekannt. Diese schwanken zwischen 24,5 und 70 Millionen.

46. Wie beurteilt die Bundesregierung unter datenschutzrechtlichen Gesichtspunkten die Praxis zahlreicher Unternehmen, die durch den Einsatz von Kundendaten gewonnenen Konsumdaten zum Zweck der Kundenprofilbildung über viele Jahre hinweg zu sammeln und auszuwerten?

Die Verwendung der angesprochenen Daten ist zum einen auf der Grundlage einer Einwilligung der Kunden zulässig, die allerdings eine entsprechende Aufklärung über Zweck und Umfang der Verwendung voraussetzt. Zum anderen

dürfen Unternehmen Kundendaten, die das Unternehmen zu vertraglichen Zwecken erhoben hat, auf der Grundlage von § 28 Abs. 3 Satz 1 Nr. 3 BDSG zu Zwecken der Werbung, Markt- und Meinungsforschung nutzen und übermitteln. Hier gelten jedoch enge Voraussetzungen, die insbesondere eine Profilbildung in Bezug auf einzelne Personen nicht erlauben. Die Betroffenen haben darüber hinaus nach § 28 Abs. 4 BDSG ein Widerspruchsrecht.

47. Wie beurteilt die Bundesregierung ferner unter datenschutzrechtlichen Gesichtspunkten unternehmensübergreifende Rabattsysteme wie z. B. Payback, bezüglich derer Unternehmen aus allen Bereichen des Alltagslebens Daten erfassen, bündeln und eventuell auch untereinander austauschen, um so ein noch umfassenderes Profil ihrer Kunden zu erhalten?

Insoweit gelten dieselben rechtlichen Anforderungen wie zu Frage 46 dargelegt. Die Payback-Betreibergesellschaft Loyalty Partner GmbH (Payback) betont, dass sie personenbezogene Daten von Kunden weder an Partnerunternehmen noch an Dritte weitergebe. Auch erstelle man keine Kundenprofile. Soweit die erforderliche Einwilligung vorliege, würde zur gezielten Werbeansprache lediglich eine Selektion der erhobenen Daten nach bestimmten Kriterien vorgenommen, beispielsweise nach Wohnort oder Alter.

48. Wie beurteilt die Bundesregierung aus datenschutzrechtlichen Gesichtspunkten die Praxis der Unternehmen, von ihren Kunden durch die Verwendung von allgemeinen Geschäftsbedingungen die Einwilligung zur Nutzung und Erfassung von Kundendaten zu erhalten?

Nach § 307 Abs. 1 BGB darf die Einwilligung die betroffenen Kunden nicht entgegen den Geboten von Treu und Glauben unangemessen benachteiligen, wenn sie durch die Verwendung von allgemeinen Geschäftsbedingungen erteilt werden soll. Eine unangemessene Benachteiligung kann sich auch daraus ergeben, dass die Bestimmung nicht klar und verständlich ist. Darüber hinaus ist die Einwilligung zur Nutzung und Erfassung personenbezogener Kundendaten nach § 4a Abs. 1 Satz 4 BDSG besonders hervorzuheben, wenn sie zusammen mit anderen Erklärungen, etwa zu weiteren allgemeinen Geschäftsbedingungen, erteilt werden soll. Diese besondere Hervorhebung muss sich insbesondere aus dem Schriftbild ergeben.

49. Wie beurteilt die Bundesregierung die Tatsache, dass eine Einwilligung des Kunden zur weiteren Bearbeitung seiner persönlichen Daten zu Marketingzwecken auch den Verkauf dieser Daten und eine Verwendung im Ausland einschließen kann?

Die wirksame Einwilligung des Kunden setzt voraus, dass dieser über den Zweck der Datenerhebung, -verarbeitung und -nutzung unterrichtet ist. Er muss daher vor Erteilung der Einwilligung insbesondere über eine etwa beabsichtigte Datenübermittlung gegen Entgelt informiert werden. Eine Datenübermittlung ins Ausland setzt voraus, dass entweder dort ein angemessenes Datenschutzniveau gewährleistet ist, oder der Kunde vor Erteilung seiner Einwilligung auf das Fehlen eines solchen Schutzniveaus besonders hingewiesen wurde. Diese Rechtslage ist nach Ansicht der Bundesregierung sachgerecht.

50. Inwiefern sieht die Bundesregierung in diesem Bereich Handlungsbedarf, eventuell auch auf europäischer Ebene?

Die Bundesregierung sieht in diesem Bereich zurzeit keinen rechtlichen Handlungsbedarf.

51. Sieht die Bundesregierung in der umfangreichen Sammlung von Kundendaten durch die Privatwirtschaft ein Risikopotenzial aus datenschutzrechtlicher Sicht, wenn ja, welches bzw. wenn nein, warum nicht?

Einem eventuell vorhandenen Risikopotential trägt die gegenwärtige Rechtslage, die dem Schutzbedürfnis der Betroffenen gerecht wird, Rechnung. Die zuständigen Aufsichtsbehörden überwachen deren Einhaltung.

52. Ist die Bundesregierung bereit, die Wirtschaft zu unterstützen bzw. zu fördern, wenn sich diese freiwillig einem Datenschutzaudit unterzieht bzw. ein Datenschutzsiegel als Qualitätsmerkmal einführt?

Das Konzept des Datenschutzaudits bzw. eines Datenschutzsiegels als Qualitätsmerkmal beruht nicht auf (zusätzlicher) staatlicher Förderung, sondern auf der Erzielung von Wettbewerbsvorteilen und damit auf dem Eigeninteresse der Wirtschaft. Auf die Antwort zu Frage 3 und 6 wird verwiesen.

53. Wie hat sich die BA organisatorisch, insbesondere im Hinblick auf die Datenverarbeitung, auf die Übernahme bzw. den Abgleich persönlicher Daten von Sozialhilfeempfängern vorbereitet, und wie soll die Sicherheit dieser Daten gewährleistet werden?

Die für die Grundsicherung für Arbeitsuchende erforderlichen Daten von Sozialhilfebeziehern werden im Rahmen von § 65a Sozialgesetzbuch II (SGB II) in aller Regel von den kommunalen Trägern erhoben. In diesen Fällen erhält die Bundesagentur für Arbeit die Daten nach § 65d SGB II vom kommunalen Träger, der ihr den ersten Leistungsbescheid und die vollständigen Antragsunterlagen für die Leistungen der Grundsicherung für Arbeitsuchende übermittelt. Eine darüber hinausgehende Übernahme und ein Abgleich persönlicher Daten von Sozialhilfebeziehern ist nicht vorgesehen.

Für die Datenerhebung und -erfassung und die damit zusammenhängenden weiteren Arbeiten, die einen zeitlich begrenzten zusätzlichen Aufwand erfordern, wurden ca. 3 000 Mitarbeiterinnen und Mitarbeiter an die Bundesagentur für Arbeit zur Unterstützung abgeordnet. Der Prozess der Einführung der Grundsicherung für Arbeitsuchende wurde vom Bundesbeauftragten für den Datenschutz kritisch begleitet. In mehreren Gesprächen zwischen dem Bundesministerium für Wirtschaft und Arbeit, der Bundesagentur für Arbeit und dem Bundesbeauftragten für den Datenschutz wurden datenschutzrechtliche Probleme der Einführung der Grundsicherung für Arbeitsuchende erörtert und Lösungen gefunden, die zu einem großen Teil schon umgesetzt worden sind. Insoweit wird auf die Antwort der Bundesregierung zur Kleinen Anfrage der Fraktion der FDP „Arbeitslosengeld II und Datenschutz“ (Bundestagsdrucksache 15/4588) verwiesen. Zukünftig wird die Sicherheit der von den Mitarbeitern in der Software zur Leistungsgewährung des Arbeitslosengelds II (A2LL) erfassten Daten über organisatorische und technische Maßnahmen eines IT-Sicherheitskonzepts gewährleistet.

54. Wann beabsichtigt die Bundesregierung die Einbringung eines Arbeitnehmerdatenschutzgesetzes, welches für die Mitte der 15. Wahlperiode angekündigt worden war?

Die Bundesregierung strebt an, einen zeitgemäßen rechtlichen Rahmen für den Datenschutz im Arbeitsverhältnis zu schaffen. Bei einer solchen nationalen Kodifikation ist es nach Auffassung der Bundesregierung jedoch sinnvoll, die Überlegungen der Europäischen Kommission für einen Gemeinschaftsrahmen zum Arbeitnehmerdatenschutz zunächst abzuwarten.

VII. Mobilfunk

55. Sind der Bundesregierung Maßnahmen bekannt, die von einer staatlichen Behörde ergriffen werden, um den Nutzer eines Mobiltelefons zu lokalisieren, und wenn ja, welche Behörden oder Ämter nutzen diese Möglichkeiten, und wie werden die Erkenntnisse aus einer solchen Maßnahme verwertet?

Im Rahmen der Strafverfolgung bestehen folgende Möglichkeiten: Eine Erhebung der Standortdaten eines Mobilfunkgerätes kommt im Rahmen einer Überwachung der Telekommunikation, etwa nach den §§ 100a, 100b StPO, in Betracht. Die Verwendung der Erkenntnisse aus einer solchen Maßnahme richtet sich nach den jeweils einschlägigen Vorschriften, im Falle der §§ 100a, 100b StPO nach § 100b Abs. 5 StPO.

Daneben kommt noch eine Auskunft über die Standortdaten eines Mobilfunkgerätes im Falle einer Verbindung aufgrund eines Auskunftsanspruchs der berechtigten Stellen über Telekommunikationsverbindungsdaten, etwa nach §§ 100g, 100h StPO, in Betracht.

Nicht möglich ist es dagegen, durch ein auf § 100g StPO gestütztes Auskunftsverlangen über die Standortkennung eines Mobilfunkgerätes im Stand-by-Betrieb den Aufenthaltsort eines Beschuldigten zu ermitteln, da § 100g Abs. 3 StPO eine Auskunft über Telekommunikationsverbindungsdaten ausdrücklich nur im Falle einer Verbindung zulässt. Die Erstellung nachträglicher Bewegungsprofile ist damit ausgeschlossen. Die Verwendung der Erkenntnisse aus einer solchen Maßnahme richtet sich nach den jeweils einschlägigen Vorschriften, im Falle der §§ 100g, 100h StPO nach § 100h Abs. 3 StPO.

Eine weitere Möglichkeit der Standortbestimmung stellt die Nutzung der so genannten stillen SMS dar. Beim Einsatz einer solchen stillen SMS, die etwa auf die Ermittlungsklauseln in §§ 161 Abs. 1, 163 Abs. 1 StPO gestützt werden kann, wird eine Telekommunikationsverbindung zu einem eingeschalteten Mobilfunkgerät der Zielperson hergestellt, ohne dass diese darüber Kenntnis erlangt. Ebenso wie bei einem gewöhnlichen Anruf wird dabei insbesondere eine Kennung der jeweiligen Funkzelle erhoben, in die das Mobilfunkgerät des Betroffenen zum Zeitpunkt der Übermittlung der SMS eingebucht war. Die auf diese Weise anfallenden Telekommunikationsverbindungsdaten gelangen dann zur Kenntnis der jeweils berechtigten Stellen, wenn bereits zum Zeitpunkt der Versendung der stillen SMS der betroffene Mobilfunkanschluss Gegenstand einer Telekommunikationsüberwachung, etwa nach den §§ 100a, 100b StPO, war. Daneben kommt eine Auskunft über die jeweilige Standortkennung nach Versand einer stillen SMS auch im Rahmen eines Auskunftsanspruchs über Telekommunikationsverbindungsdaten in Betracht.

Zur Lokalisierung eines Mobilfunkgerätes kann zudem ein so genannter IMSI-Catcher eingesetzt werden. Ein IMSI-Catcher simuliert die Basisstation eines Mobilfunknetzbetreibers und veranlasst damit die Mobilfunkgeräte, die sich in seinem Wirkungsbereich befinden, sich bei ihm anzumelden. Nach § 100i

Abs. 1 Nr. 2 StPO darf mit Hilfe des IMSI-Catchers der Standort eines aktiv geschalteten Mobilfunkgerätes auch zum Zweck der vorläufigen Festnahme und der Ergreifung des Täters auf Grund eines Haft- oder Unterbringungsbefehls ermittelt werden. Nach § 100i Abs. 3 StPO dürfen personenbezogene Daten Dritter anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung der Zwecke nach §100i Abs. 1 StPO unvermeidbar ist. Sie sind nach Beendigung der Maßnahme unverzüglich zu löschen.

Die genannten Maßnahmen können durch die Strafverfolgungsbehörden getroffen werden; die Verwertung der gewonnenen Erkenntnisse richtet sich nach den §§ 100b Abs. 5, 100d Abs. 5 Satz 1, 100h Abs. 3 und 100i Abs. 3 Satz 2 StPO.

Darüber hinaus darf das Bundesamt für Verfassungsschutz (BfV) den IMSI-Catcher zur Erfüllung seiner Aufgaben nach § 3 Abs. 1 Nr. 2 bis 4 BVerfSchG unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkgerätes und zur Ermittlung der Geräte- und Kartennummern einsetzen (§ 9 Abs. 4 Satz 1 BVerfSchG). Der Bundesnachrichtendienst (BND) und das Amt für den Militärischen Abschirmdienst (MAD) sind ebenfalls befugt, den IMSI-Catcher einzusetzen (§ 3 Satz 2 BND-G, § 5 MAD-G). Der Einsatz des IMSI-Catchers durch die Nachrichtendienste des Bundes bedarf grundsätzlich der (vorherigen) Zustimmung durch die G 10-Kommission (§ 9 Abs. 4 Satz 6 in Verbindung mit § 8 Abs. 9 Satz 4 ff. BVerfSchG).

Auch die Einholung von Auskünften unter anderem zur Standortkennung des anrufenden und des angerufenen Anschlusses durch das BfV (§ 8 Abs. 8 Satz 3 Nr. 1 BVerfSchG) unterliegt der Kontrolle durch die G 10-Kommission (vgl. § 8 Abs. 9 Satz 4 ff. BVerfSchG). Gleiches gilt für die entsprechenden Befugnisse von BND und MAD.

56. Welche technischen Möglichkeiten bestehen hinsichtlich der Lokalisierung des Nutzers eines Mobiltelefons sowohl bei eingeschaltetem als auch bei ausgeschaltetem Mobiltelefon?

Die Erbringung des Mobiltelefondienstes setzt voraus, dass dem Mobilfunknetz der ungefähre Standort des Nutzers oder der Nutzerin bekannt ist. Mobilfunknetze sind funktechnisch in eine Vielzahl so genannter Funkzellen aufgeteilt. Um einen bestmöglichen Telekommunikationsdienst zu erbringen, erfolgt in regelmäßigen Abständen ein Dialog zwischen Mobilfunkgerät und dem Mobiltelefonnetz, für den das Mobilfunkgerät die beste der aktuell empfangbaren Funkzellen auswertet. Das Mobilfunknetz verfügt mithin über die aktuellen Informationen, welches Mobilfunkgerät eingeschaltet und in welcher Funkzelle es eingebucht ist.

Die Größe einer Funkzelle ist in erster Linie von der Technik, die dem Mobilfunknetz zu Grunde liegt, und vom Umfang des in der jeweiligen Zelle abzuwickelnden Telekommunikationsaufkommens abhängig. Ihr Durchmesser liegt zwischen etwa 100 m und 30 km. Bei der Umsetzung der Information über die Funkzelle, die einem bestimmten Mobilfunkanschluss aktuell zugeordnet ist, in geografische Ortsangaben ist die Genauigkeit mithin auf die Größe der jeweiligen Funkzelle begrenzt.

Bei einem Ortswechsel des Mobilfunkgerätes werden die früheren Angaben überschrieben. Dieser Vorgang heißt „location update“.

Ausgeschaltete Mobilfunkgeräte führen den Dialog mit dem Mobiltelefonnetz nicht weiter fort. Die Informationen über deren ungefähren Standort, die dem Netz vorliegen, sind mithin nicht mehr aktualisierbar. Das Mobiltelefonnetz be-

hält jedoch den letzten Eintrag bei und überschreibt diesen beim Einbuchen ins Netz nach Wiedereinschalten des Mobilfunkgerätes mit der Kennzeichnung der dann aktuellen Funkzelle.

Die in der Antwort zu Frage 55 beschriebenen Möglichkeiten der Lokalisierung eines Mobilfunkgerätes setzen daher voraus, dass über das Telefon Verbindungen aufgebaut worden sind bzw. dass das Gerät zumindest eingeschaltet ist. Die Lokalisierung eines ausgeschalteten Mobilfunkgerätes ist nach Kenntnis der Bundesregierung derzeit technisch nicht möglich.

57. Ist die Bundesregierung der Ansicht, dass die derzeitigen Rechtsgrundlagen zur Ortung von Nutzern von Mobiltelefonen ausreichend sind, wenn ja, warum, bzw. wenn nein, wann wird die Bundesregierung die erforderlichen gesetzlichen Änderungen vornehmen?

Die Bundesregierung prüft derzeit den möglichen Änderungsbedarf im Hinblick auf die strafprozessualen Regelungen über die Telekommunikationsüberwachung. Dabei wird sich die Bundesregierung auch mit der Frage befassen, ob im Hinblick auf die Rechtsgrundlagen zur Ortung von Mobilfunkgeräten Änderungsbedarf besteht. Diese Frage wird zugleich Gegenstand der beabsichtigten Evaluation des Terrorismusbekämpfungsgesetzes sein.

Vorbehaltlich neuer Erkenntnisse hieraus sind nach Ansicht der Bundesregierung die derzeitigen Rechtsgrundlagen zur Ortung von Nutzern von Mobilfunkgeräten ausreichend. Es ist indes nicht ausgeschlossen, dass durch eine weitere technische Entwicklung gesetzliche Änderungen veranlasst werden.

58. Wie beurteilt die Bundesregierung Systeme wie beispielsweise „Phonetracker“, einen Mobilfunkerweiterungsdienst, durch den sich so genannte räumliche „Schutzzonen“ definieren lassen, bei deren Verlassen Alarm ausgelöst wird, so dass beispielsweise Eltern über die Bewegungen ihres Kindes informiert werden?

§ 98 TKG regelt die Nutzung von Standortdaten ausführlich. Nach Absatz 1 dürfen Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder Telekommunikationsdiensten für die Öffentlichkeit verwendet werden, nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat. Der Teilnehmer muss Mitbenutzer über eine erteilte Einwilligung unterrichten. Eine Einwilligung kann jederzeit widerrufen werden. Nach Absatz 2 ist, wenn die Teilnehmer ihre Einwilligung zur Bearbeitung von Standortdaten gegeben haben, ihnen auch weiterhin die Möglichkeit einzuräumen, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen. Bei Verbindungen zu Anschlüssen mit der Rufnummer 112, den in der Rechtsverordnung nach § 108 Abs. 2 TKG festgelegten Rufnummern oder der Rufnummer 124124 hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Übermittlung von Standortdaten ausgeschlossen wird (Absatz 3). Die Bundesregierung sieht hierdurch auch die so genannten Phonetracker ausreichend geregelt. Im Übrigen wird auf die Beantwortung der Schriftlichen Frage 38 der Abgeordneten Gisela Piltz vom 19. Dezember 2003 (Bundestagsdrucksache 15/2319, Seite 20 f.) Bezug genommen.

59. Wie beurteilt die Bundesregierung die Abhörfunktion von „Phonetracker“, bei der das Handy ein Gespräch annimmt, aber das Klingeln unterdrückt wird und so dem Anrufer das unbemerkte Mithören von Gesprächen in der Umgebung des Angerufenen ermöglicht wird?

Die Bundesregierung ist der Auffassung, dass das Mobilfunkgerät durch diese Funktion aus telekommunikationsrechtlicher Sicht zu einer Sendeanlage umgewandelt wird, die einen Gegenstand des täglichen Gebrauchs (nämlich ein Mobilfunkgerät) vortäuscht und die daher in besonderer Weise geeignet ist, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören. Die Anwendung verstößt daher gegen § 90 TKG. Daneben sind aber auch strafrechtliche Vorschriften zu beachten.

Die Verwertbarkeit von Informationen in einem Strafverfahren, die durch das heimliche Mithören von Gesprächen mittels der Abhörfunktion von „Phonetracker“ erlangt wurden, kann problematisch sein. Der Bundesgerichtshof hat in einer Entscheidung vom 14. März 2003 – 2 StR 341/02 – die Verwertung von Informationen aus einem so genannten Raumhintergrundgespräch aufgrund eines hypothetischen Ersatzeingriffs nach den §§ 100a, 100b StPO als zulässig erachtet. Da beim Einsatz der Abhörfunktion von „Phonetracker“ das Mobilfunkgerät von dem betroffenen Nutzer nicht unmittelbar zu Kommunikationszwecken eingesetzt wird, ist allerdings fraglich, ob der Einsatz dieser Funktion zu Strafverfolgungszwecken auf die §§ 100a, 100b StPO gestützt werden kann. Alternativ kommt als Rechtsgrundlage § 100c Abs. 1 Nr. 2 StPO bzw., wenn das gegenständliche Gespräch in einer Wohnung geführt wird, § 100c Abs. 1 Nr. 3 StPO in Betracht.

60. Sieht die Bundesregierung in dieser Möglichkeit zum unbemerkten Mithören von Gesprächen via Handy, bei denen nicht nur der Angerufene, sondern gegebenenfalls auch dessen Gesprächspartner abgehört werden, einen Verstoß gegen die Vertraulichkeit des Wortes?

Die Ermöglichung des Mithörens von Gesprächen durch Aktivieren der Funktion „Phonetracker“ durch eine Privatperson stellt zunächst keinen Eingriff in das Recht am gesprochenen Wort aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG dar, weil die Grundrechte nur Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht binden (Artikel 1 Abs. 3 GG).

Ein Eingriff in das genannte Grundrecht kann in der Verwertung der aus einem solchen unbemerkten Mithören gewonnenen Beweismittel in einem Rechtsstreit, etwa im Wege des Zeugenbeweises, liegen. Das Grundrecht aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG ist indes nicht schrankenlos gewährleistet. Allerdings bedarf die Verwertbarkeit eines durch heimliches Mithören gewonnenen Beweismittels in einem Rechtsstreit einer besonderen Rechtfertigung. Allein das allgemeine Interesse an einer funktionstüchtigen Straf- und Zivilrechtspflege reicht nicht aus, um im Rahmen der Abwägung stets von einem gleichen oder gar höheren Gewicht dieses Interesses ausgehen zu können, als es dem allgemeinen Persönlichkeitsrecht zukommt. Vielmehr müssen weitere Aspekte hinzutreten, die ergeben, dass das Interesse an der Beweiserhebung trotz der Persönlichkeitsbeeinträchtigung schutzbedürftig ist. Im Strafverfahren kann dies etwa die Aufklärung besonders schwerer Straftaten sein. Auch im Zivilprozess kann es Situationen geben, in denen dem Interesse an der Beweiserhebung – über das stets gegebene „schlichte“ Beweiserhebungsinteresse hinaus – besondere Bedeutung für die Rechtsverwirklichung einer Partei zukommt. Dies kann etwa der Fall sein, wenn sich die Partei, die die Beweislast trifft, in einer Notwehrsituation oder einer notwehrähnlichen Lage befindet, beispielsweise bei der Anfertigung heimlicher Tonbandaufnah-

men zur Identifikation eines anonymen Anrufers, der sich als eine andere Person ausgegeben hatte, um unter diesem Deckmantel Verleumdungen gefahrlos aussprechen zu können, bei Maßnahmen zur Feststellung erpresserischer Drohungen oder wenn es der eingreifenden Person bei der Schaffung des Beweismittels darauf ankam, einem auf andere Weise nur schwer, möglicherweise überhaupt nicht abwehrbaren kriminellen Angriff auf die berufliche Existenz zu begegnen (vgl. BVerfG, Beschluss vom 9. Oktober 2002 – 1 BvR 1611/96, 805/98 –, BVerfGE 106, 28 [49 f.]).

61. Hält die Bundesregierung datenschutzrechtliche Bestimmungen bei den „Location Based Services“ für in ausreichendem Maße berücksichtigt, wenn ja, warum, bzw. nein, warum nicht?

Die Bundesregierung hält die datenschutzrechtlichen Bestimmungen bei den „location based services“ für ausreichend. Hierfür gilt die in der Antwort zu Frage 58 dargestellte Vorschrift des § 98 TKG.

62. Welchen Nutzen sieht die Bundesregierung in der in der Telekommunikationsgesetz-Novelle formulierten Verpflichtung zur Erhebung persönlicher Daten von Prepaid-Karten-Kunden?

Angesichts der hohen Zahl von Prepaid-Karten (nach Angaben der Regulierungsbehörde für Post und Telekommunikation sind dies über 50 % aller in Deutschland genutzten Mobilfunkanschlüsse) ist die Kenntnis bestimmter Kundendaten im Falle von Prepaid-Produkten für eine erfolgreiche Arbeit der Strafverfolgungs- und Sicherheitsbehörden unerlässlich. Die Ermittlung einer Anschlussinhaberin oder eines Anschlussinhabers stellt in vielen Fällen häufig den ersten und einzigen Ermittlungsansatz dar. Die Verwendung anonym erworbener Prepaid-Karten kann die Ermittlungstätigkeit der Strafverfolgungs- und Sicherheitsbehörden daher erheblich erschweren. Die Ermittlungen zu den Sprengstoffanschlägen im März dieses Jahres in Madrid, bei denen Mobilfunkgeräte mit Prepaid-Karten als Zünder benutzt wurden, haben verdeutlicht, wie wichtig die Kenntnis dieser Daten für erfolgreiche Ermittlungen sein kann.

Aus diesem Grund sieht das novellierte Telekommunikationsgesetz in §§ 111 ff. vor, dass im Falle von in Deutschland erworbenen Prepaid-Karten bestimmte Kundendaten für Auskunftsersuchen der Strafverfolgungs- und Sicherheitsbehörden zu erheben und zu speichern sind (Name und Anschrift des Rufnummerninhabers, bei natürlichen Personen deren Geburtsdatum, das Datum des Vertragsbeginns und, soweit bekannt, das des Vertragsendes sowie bei Festnetzanschlüssen die Anschrift des Anschlusses).

63. Wie begegnet die Bundesregierung dem Argument, durch die Pflicht zur Erhebung persönlicher Daten im Prepaid-Verfahren könne lediglich der Ersterwerber einer solchen Karte identifiziert werden und der schwunghafte Handel mit solchen Karten würde den Sicherheitsaspekt dieser Maßnahme zunichte machen?

Eine Weitergabe von Prepaid-Karten vom Ersterwerber an Dritte kann selbstverständlich nicht ausgeschlossen werden. Aufgrund der nunmehr seit dem 26. Juni 2004 geltenden Rechtslage ist aber sichergestellt, dass zumindest der Ersterwerber ermittelt werden kann und damit den Strafverfolgungs- und Sicherheitsbehörden ein erster und in vielen Fällen weiterführender Ermittlungsansatz gegeben ist. Überdies lässt sich auch bei Postpaid-Verträgen auf fremde Kennungen ausweichen – etwa durch die Verwendung gestohlener

SIM-Karten –, wodurch gleichfalls nicht der grundsätzliche Nutzen der Erhebung entsprechender Bestandsdaten in Frage gestellt wird.

64. Plant die Bundesregierung als Konsequenz hieraus, den Verkauf und die anderweitige Weitergabe von Prepaid-Karten zu verbieten?

Da den Strafverfolgungs- und Sicherheitsbehörden bei Ermittlung des Ersterwerbers, wie dargelegt, in vielen Fällen wertvolle Ermittlungsansätze zur Verfügung stehen, plant die Bundesregierung nicht, den Verkauf und die anderweitige Weitergabe von Prepaid-Karten zu verbieten.

VIII. Internet

65. Plant die Bundesregierung gesetzliche Änderungen im Bereich des Datenschutzes im Internet, wenn ja, welche, und wie werden diese begründet?

Der Schutz der personenbezogenen Daten der Nutzer von Internet-Diensten ist derzeit im Teledienste-Datenschutz-Gesetz (TDDSG) des Bundes und im Mediendienste-Staatsvertrag (MDStV) der Länder geregelt. Darüber hinaus gelten die Datenschutzbestimmungen des Telekommunikationsgesetzes, soweit solche Dienste – wie bei der Gewährleistung eines Internet-Zugangs (Access-Provider) oder der Übermittlung von elektronischer Post (E-Mail) – auch Verkehrsdaten verarbeiten.

Das derzeitige Regelungsgefüge im TDDSG und im MDStV geht auf eine Bund-Länder-Verständigung zurück, die darauf abzielt, gleich lautende Bestimmungen für Tele- und Mediendienste durch Bundesgesetz und einen Länder-Staatsvertrag zu schaffen. An dieser Verfahrensweise wurde bei der Novellierung des Teledienstegesetzes (TDG) und des TDDSG durch das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG), das Anfang 2002 in Kraft getreten ist, festgehalten.

In Zukunft soll eine stärkere Vereinheitlichung und Harmonisierung erreicht werden. Ein erster Schritt ist die Vereinheitlichung des Jugendschutzes im Bereich der elektronischen Medien. Dies wurde bereits 2003 mit den Neuregelungen des Jugendschutzes im Jugendschutzgesetz (JuSchG) des Bundes und im Jugendmedienschutz-Staatsvertrag der Länder (JMStV) umgesetzt. Dabei war es ein besonderes Anliegen der Länder, zu einer möglichst geschlossenen Regelung des Jugendschutzes bei allen elektronischen Medien (Rundfunk, Tele- und Mediendienste) im Länder-Staatsvertrag zu gelangen.

Ebenso soll nun der Datenschutz bei Tele- und Mediendiensten zu einem einheitlichen bundesgesetzlichen Regelwerk zusammengeführt werden. Dies ist Teil einer Reihe von Eckpunkten, die Bund und Länder zur Fortentwicklung der Medienordnung vereinbart haben.

Im Zuge der anstehenden Neuregelung werden in einem zukünftigen Telemediengesetz unter anderem die Datenschutzvorschriften für Tele- und Mediendienste zusammengeführt. Dabei sollen zum einen auch das Verhältnis zum Datenschutz bei der Telekommunikation weiter klargestellt sowie zum anderen gesetzliche Grundlagen für Initiativen im Bereich der freiwilligen Selbstkontrolle geschaffen werden. Ein entsprechendes Gesetzesvorhaben wird derzeit auf Fachebene vorbereitet.

66. Wie bewertet die Bundesregierung die Sicherheit der von Bürgern in Behördencomputern mit Internetzugang gespeicherten Daten, insbesondere unter dem Aspekt der zuletzt vielfältig in Erscheinung getretenen Würmer und anderweitiger Angriffe auf Behördennetzwerke?

Das Internet ist auch für die öffentliche Verwaltung ein wichtiges Kommunikationsmedium. Durch Einrichtung von Sicherheitsvorkehrungen, ihre regelmäßige Überprüfung sowie eine fortlaufende Aktualisierung von Schutzmechanismen wird den Gefahren aus dem Internet begegnet. Das Regierungsnetzwerk „Informationsverbund Berlin-Bonn“ (IVBB) erfüllt diese Anforderungen.

67. Welche besonderen Anforderungen an den Datenschutz ergeben sich im Zusammenhang mit den E-Government-Projekten?

Im Zusammenhang mit E-Government-Projekten ergeben sich keine grundsätzlich neuen Anforderungen, die sich von denen anderer Projekte der Verwaltungen im Bereich der Informations- und Kommunikationstechnologie unterscheiden. Zwar sind im Rahmen von E-Government-Projekten durch die IT-Unterstützung von Verwaltungsprozessen oder die Einrichtung bzw. Vernetzung elektronischer Archive durchaus spezifische Bedrohungspotenziale denkbar. Aber auch diesen kann mit den gängigen Methoden zur Sicherung der Vertraulichkeit, der Integrität, der Verfügbarkeit und nicht zuletzt der Authentizität wirksam begegnet werden. Rechtlich ist dies in § 9 BDSG bereits verankert.

Die Behörden der Bundesverwaltung sind verpflichtet, diese Aspekte in ihren IT-Sicherheitskonzepten zu berücksichtigen. Dies gilt für den internen Einsatz der IT gleichermaßen wie für E-Government-Projekte.

68. Welche datenschutzrechtlichen Probleme ergeben sich aus der in § 21 Abs. 1a S. 1 Melderechtsrahmengesetz vorgesehenen Möglichkeit, einfache Melderegisterauskünfte via Internet zu erhalten?

Aus dem vorgesehenen Verfahren ergeben sich keine datenschutzrechtlichen Probleme. Denn dabei handelt es sich nicht um einen automatisierten Abruf im Sinne eines freien, an keinerlei Voraussetzungen gebundenen Zugangs zum Melderegister. Vielmehr wird eine Auskunft nur aus einem duplizierten Teildatenbestand und erst dann erteilt, wenn die Angaben des Auskunftssuchenden eine eindeutige Identifizierung des Betroffenen ermöglichen und eine Gebühr gezahlt worden ist. Darüber hinaus soll diese Form der Auskunftserteilung nur möglich sein, wenn der Betroffene dem nicht widersprochen hat.

IX. Navigationssysteme

69. Ist der Bundesregierung bekannt, ob von staatlichen Stellen ein Zugriff auf Informationen, die von Navigationssystemen gesendet werden, erfolgt?

Die von einem Navigationssystem gesendeten Informationen werden als Navigationssignale bezeichnet. Diese Navigationssignale können von allen entsprechend ausgerüsteten Nutzern innerhalb des Überdeckungsgebiets der Navigationsanlage empfangen werden. Davon zu unterscheiden sind Ortungssysteme (zum Beispiel Radaranlagen), die der Bestimmung des Ortes von Zielobjekten dienen.

Staatliche Stellen verwerten Informationen, die von Navigationssystemen an diese Stellen aktiv gesendet werden, in der Schifffahrt. Im Bereich der Seeschifffahrt wurde von der International Maritime Organisation (IMO) ein welt-

weit für alle Schiffe mit einer Bruttoraumzahl von mehr als 300[1] verbindliches automatisches Schiffsidentifizierungssystem (AIS – Automatic Identification System) zur Erhöhung der Sicherheit und Leichtigkeit des Seeverkehrs durch einen automatischen Austausch von Identifizierungs- und Navigationsdaten eingeführt. Bei diesen Daten handelt es sich um statische und dynamische schiffs- und reisebezogene Daten. AIS ermöglicht es, dass diese Daten von jedem Verkehrsteilnehmer im jeweiligen Verkehrsgebiet und auch von landseitigen Verkehrsüberwachungs- und Verkehrslenkungsstellen empfangen und gespeichert werden.

Sofern sich Luftfahrzeuge unter der Kontrolle der Flugsicherung bewegen, müssen sie Daten zur Bestimmung ihrer Position an die Flugsicherungskontrollstellen senden. Die Positionsbestimmung erfolgt hierbei nicht über Navigationssysteme, sondern auf der Grundlage eines Ortungssystems (Radar) am Boden in einem kooperativen Prozess. Dabei wird die Höhe der Luftfahrzeuge von diesen selbst ermittelt und aktiv an die Flugsicherung am Boden übertragen. Auch der Bundeswehr stehen diese Positionsdaten zur Verfügung. Neue Ortungssysteme, die zum Teil bereits in Betrieb, aber durch die Ausrüstungsvorschriften noch nicht verlangt sind, strahlen die durch ein Satellitennavigationssystem ermittelte Position eines Flugzeugs ständig ab.

Dagegen ist der Bundesregierung kein Zugriff staatlicher Stellen auf gesendete Informationen von Navigationsgeräten im Straßenverkehr bekannt.

Im Einzelnen:

Unter dem Aspekt der Möglichkeit eines Zugriffs auf Lokalisierungsinformationen sind folgende Arten von Navigationssystemen in Kraftfahrzeugen zu unterscheiden:

1. On Board Navigationssysteme:

   Diese funktionieren autonom, d. h. die Kartenhaltung und Routenberechnung erfolgen ausschließlich geräte- oder fahrzeugintern. Darunter gibt es folgende Ausprägungen:

   a) Völlig autonome Navigationssysteme ohne Kommunikationsanbindung: Bei diesen Systemen verlassen Daten das Gerät nicht. Sie können im Hinblick auf die hiesigen Fragen mithin unberücksichtigt bleiben.

   b) Autonome Navigationssysteme mit Broadcastkommunikationsanbindung zum Empfang von Verkehrsdaten (kostenfrei oder gebührenpflichtig): Bei diesen Systemen erfolgt lediglich ein Datenempfang, aber keine Datenaussendung. Auch sie können mithin unberücksichtigt bleiben.

   c) Autonome Navigationssysteme mit bidirektionaler Kommunikation zur orts- oder routenindividuellen Versorgung mit Verkehrsdaten, zum Beispiel über SMS (AUDI DynNav oder DC DynAPS bzw. BMW Telematik). Hier liegen dem Telematik Service Provider (TSP) fahrzeugbezogene Informationen zum Aufenthaltsort vor, die während der Fahrt regelmäßig aktualisiert werden. Damit ist prinzipiell die Rekonstruktion der Fahrstrecke online und rückwirkend möglich. Exakte Angaben zu den Start- und Zieladressen oder dem genauen Routenverlauf werden jedoch nicht an den TSP oder sonstige Dritte übermittelt.

2. Off-Board-Systeme:

   Bei diesen Systemen werden die Kartendaten in der Servicezentrale vorgehalten, in der auch die Routenberechnung erfolgt; lediglich die Routen-

1 Die „Bruttoraumzahl“ nach dem Londoner Vermessungs-Übereinkommen hat die früher übliche Einheit „Bruttoregistertonne“ abgelöst und entspricht ihr annähernd auch in der Größe.

beschreibung wird an das Endgerät zur Routenführung übermittelt. Systembedingt liegen dem TSP in diesem Fall genaue Angaben über die Start- und Zieladressen sowie die empfohlenen Routen vor. Je nach Ausprägung werden unterschiedlich umfangreiche Netzausschnitte zur Routenführung an das Endgerät übertragen. Während der Fahrt kann der Nutzer außerdem um Aktualisierung bitten, um beispielsweise Informationen zur Verkehrslage berücksichtigen zu können oder um eine Aktualisierung der Route beim Abweichen von der ursprünglichen Vorgabe zu erhalten. Dabei wird jeweils die aktuelle Position übermittelt, was prinzipiell Rückschlüsse auf die tatsächlich gewählte Route ermöglicht. In der Regel ist jedoch nicht erkennbar, ob und wann das angefragte Ziel tatsächlich erreicht wird. Im Fahrzeug wird teilweise Bluetooth, ein Funkstandard für die Nahbereichsübertragung (typisch 10 m Reichweite), für die Übermittlung der Fahrzeugposition aus dem Satellitennavigationsempfänger zum Navigationsendgerät eingesetzt. Sobald die Verbindung zustande gekommen ist, ist diese Kommunikation für Dritte nicht mehr sichtbar.

Die Netzbetreiber (mobil und fest) unterliegen den Bestimmungen des Telekommunikationsgesetzes. Danach sind sie verpflichtet, Verbindungsdaten nur zum Zweck der vom Kunden genutzten Dienstleistung zu erheben und sie danach zu löschen oder bei einer Weiterverarbeitung diese anonymisiert vorzunehmen.

Zugriffe von staatlichen Stellen auf Informationen aus den genannten On-Board- oder Off-Board-Systemen sind der Bundesregierung nicht bekannt.

Zwar nutzt das Lkw-Mautsystem die Satellitennavigation zur Ortung der mautpflichtigen Lkw. Dabei bucht sich der Lkw automatisch und selbständig in das Mautsystem ein. Ein im Lkw eingebautes Fahrzeuggerät, die so genannte On-Board-Unit (OBU), erkennt automatisch anhand von Satellitensignalen des Global Positioning Systems (GPS) und zusätzlich unterstützender Ortungssensoren (Koppelortung), welchen mautpflichtigen Streckenabschnitt der Lkw befährt. Das Fahrzeuggerät erkennt die Position des Lkw und kann sie jederzeit einem der rund 5 200 Streckenabschnitte auf etwa 12 000 Autobahnkilometern zuordnen. Mit Hilfe der aufgenommenen Streckendaten, der vorprogrammierten Fahrzeugdaten, der hinterlegten Tarifdaten sowie der Fahrzeugdaten, die der Fahrer eingegeben hat, ermittelt das Fahrzeuggerät den Betrag der zu zahlenden Maut und speichert diese Information. Die Information über den zu entrichtenden Mautbetrag sendet dieses dann über GSM-Mobilfunk (Global System for Mobile Communication) an die zentrale Mauterhebungsstelle. Diese Information wird zum einen nach Erreichen eines bestimmten Mautbetrages und zum anderen nach Ablauf einer definierten Zeit versandt. Sollte das Gerät zu diesem Zeitpunkt ausgeschaltet sein, so werden die Daten nach dem nächsten Einschalten gesendet. Positions- und Streckendaten werden somit nicht laufend mit der zentralen Mauterhebungsstelle ausgetauscht, sondern erst zeitversetzt übermittelt. Die Daten, die als SMS übermittelt werden, werden kryptographisch verschlüsselt. Erst in der zentralen Mauterhebungsstelle werden die zu zahlenden Mautbeträge anhand des Fahrzeugkennzeichens dem registrierten Nutzer (Transportunternehmen) zugeordnet. Die mit der dargestellten Funktionalität ausgestattete OBU ist insofern nicht mit der Funktionalität eines herkömmlichen Navigationssystems vergleichbar und lässt sich allenfalls als ein einem Navigationssystem in Teilbereichen (zum Beispiel Nutzung GPS) ähnliches System bezeichnen.

70. Sind der Bundesregierung technische Methoden bekannt, mit denen auf Informationen oder Daten von Navigationssystemen zugegriffen werden kann?

Auf die Zustandsdaten von Navigationssystemen, d. h. auf Daten über das technische Navigationssystem als solches, nicht aber über seine Nutzer, kann unmittelbar an der Navigationsanlage sowie über ein Fernwirksystem zugegriffen werden. Es sind indes keine technischen Möglichkeiten bekannt, allein mittels eines Navigationssystems auf Informationen oder Daten seiner Nutzer zuzugreifen, da dem System seine Nutzer und deren Aufenthaltsorte nicht bekannt sind.

Ein Zugriff auf die Navigationsdaten ist – mit Ausnahme bei der Luftfahrt – nur möglich, wenn das Gerät zusätzlich über kommunikationstechnische Komponenten verfügt. Dies ist bisher allgemein nur in sehr geringem Umfang der Fall. Die Verknüpfung von Navigation und Kommunikation ist jedoch Teil neuer innovativer Dienstleistungen. So werden etwa mobile Internetverbindungen in Kombination mit dem GPS

- im Vermessungswesen zur Übertragung von Korrekturdaten,
- im Rettungswesen zum Orten von Notfallsituationen und
- im Flottenmanagement zur Überwachung und Steuerung von Fahrzeugeinsätzen

verwendet. In diesen Fällen nimmt eine Zentrale Daten von Navigationssystemen auf.

Bei der Übermittlung von Navigationsdaten ist ein Zugriff auf diese technisch möglich, soweit der Übermittlungsweg dies zulässt. Dabei handelt es sich allerdings um ein allgemeines Problem bei der Übermittlung von Daten, das sich nicht spezifisch für Navigationssysteme stellt.

Der Bundesregierung sind die angesprochenen Methoden im Rahmen der Auswertung von gespeicherten Navigationsdaten von Fluggeräten bekannt. So verfügt die Bundesstelle für Flugunfalluntersuchung (BFU) über technische Einrichtungen, um nach einem Flugunfall die Informationen, die in Protokolldatenträgern von GPS-Empfängern gespeichert sind, auszulesen und auszuwerten. Gesetzliche Grundlage dafür ist § 11 Abs. 3 Flugunfall-Untersuchungsgesetz (FlUUG). Das Datenauslesen und die Datenauswertung kann auch im Auftrag anderer Behörden erfolgen, zum Beispiel im Auftrag von Staatsanwaltschaften auf der Grundlage der Strafprozessordnung sowie nach Annex 13 der ICAO Convention on International Civil Aviation „Aircraft Accident and Incident Investigation“ im Auftrag von Flugunfalluntersuchungsbehörden anderer Länder (§ 5 Abs. 3 FlUUG).

Im Seeschifffahrtsbereich wird AIS (Automatic Identification System, siehe Antwort zu Frage 69) entsprechend den international vereinbarten betrieblichen und technischen Standards für den Austausch von Navigationsdaten verwendet.

Bei der differentiellen Satellitennavigation im Vermessungswesen schließlich müssen für einige Verfahren Daten des Navigationssystems an den Betreiber eines Referenzstationsnetzes versandt werden. Wie im Rettungswesen und im Flottenmanagement folgt die Datenaufnahme auf Betreiberseite an dieser Stelle zwingend aus dem technischen Zusammenhang.

71. Ist der Bundesregierung bekannt, ob staatliche oder private Stellen nachvollziehen können, wo sich der Nutzer eines Navigationssystems befindet, wenn ja, ist der Bundesregierung ferner bekannt, welche Stellen von dieser Möglichkeit Gebrauch machen, wie mit den erfassten Daten weiter verfahren wird und auf welcher Ermächtigung diese Eingriffe basieren?

Die Möglichkeit, den Aufenthaltsort des Nutzers nachzuvollziehen, ist bei Navigationssystemen in Kraftfahrzeugen gegeben, sofern das Navigationssystem dafür telekommunikationstechnisch ausgestattet ist. Wenn Anbieter die Systeme und die anfallenden Daten für das Angebot innovativer Dienstleistungen nutzen, zum Beispiel zur Beantwortung von Kundenanfragen über den Routenverlauf oder zur Information über aktuelle Verkehrsstörungen, kann es sich abhängig vom Einzelfall um Teledienste, Telekommunikationsdienste oder beides handeln, so dass die spezifischen Datenschutzbestimmungen des Teledienste-Datenschutzgesetzes (TDDSG) und/oder des Telekommunikationsgesetzes zur Anwendung kommen, soweit dabei personenbezogene Daten wie beispielsweise Standortdaten übermittelt werden.

Im Rahmen der Erhebung der Lkw-Maut ist eine aktuelle Positionsortung von Fahrzeugen anhand der von den Fahrzeuggeräten übermittelten SMS nicht möglich, da diese zeitversetzt versandt werden. Die Verwendung der durch das Lkw-Mautsystem erfassten Daten ist auf die im Autobahnmautgesetz für schwere Nutzfahrzeuge (ABMG) genannten Zwecke beschränkt. Der Gesetzgeber hat insoweit datenschutzrechtliche Regelungen in den §§ 4, 7 und 9 ABMG getroffen. Nach § 4 Abs. 2 Satz 4 und 5 sowie § 7 Abs. 2 Satz 2 und 3 ABMG in der Fassung der Bekanntmachung vom 2. Dezember 2004 dürfen die Mauterhebungs- und Mautkontrolldaten ausschließlich für Zwecke des ABMG verarbeitet und genutzt werden, wobei eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften unzulässig ist.

Bei der automatischen Schiffsidentifizierung (AIS) kann jede am Informationsaustausch beteiligte Stelle, wie beispielsweise Schiffe und Verkehrszentralen an Land, alle zur Verfügung gestellten und vom jeweiligen Schiff freigegebenen Daten empfangen und auswerten. Ob und in welchem Umfang private Stellen von diesen Daten Gebrauch machen, etwa für den Geschäftsbereich von Mehrwertdiensten, ist nicht bekannt. Mit dem Absenden der international verbindlich abzugebenden Informationen bestimmter Navigationsdaten mit Hilfe von AIS erfüllen die am Verkehr teilnehmenden Schiffe ihre Meldeverpflichtungen, die für Kollisionsverhütung, Verschmutzungsverhütung und Notfallbekämpfung erforderlich sind.

Das Nachvollziehen der Position eines Luftfahrzeuges ist durch die Flugsicherung mittels eines Navigationssystems nicht möglich. Neue Ortungssysteme, auf die die Antwort zu Frage 69 bereits hinweist, strahlen allerdings die Position eines Flugzeugs ständig ab. Es ist technisch möglich, dass jede Person, die einen geeigneten Empfänger und ein Monitorsystem betreibt, die Position eines so ausgerüsteten Flugzeugs bestimmen kann; dies ist allerdings aufwändig.

Sofern ein Navigationsgerät mit einer Sendeeinrichtung versehen wird, ist im Rahmen des strafprozessualen Ermittlungsverfahrens die Durchführung einer Observation auch unter Einsatz von technischen Hilfsmitteln im Sinne des § 100c Abs. 1 Nr. 1 Buchstabe b StPO erlaubt.

72. Falls Daten von Navigationssystemen erfasst werden, ist der Bundesregierung bekannt, ob und von wem diese gespeichert werden, und ob diese Daten nach einer zu bestimmenden Zeit gelöscht werden?

Der Bundesregierung ist bekannt, dass bei der Nutzung eines Navigationssystems im Straßenverkehr angefallene Daten zum Zweck der Rechnungsstellung und -prüfung gegenüber den Endkunden und eventuellen Zulieferern

sowie für statistische Auswertungen gespeichert werden. Für die Kunden-Abrechnung sind jedoch Angaben zu den Routen und damit zu den Aufenthaltsorten des Nutzers während der Nutzung des Systems nicht erforderlich. Für die Zulieferer-Abrechnung von verbrauchsabhängigen Leistungen sind keine personenbezogenen Nutzungsdaten erforderlich; sie werden daher anonymisiert. Soweit der Bundesregierung bekannt ist, speichern die Dienstleister lediglich die für den jeweiligen Rechnungszweck notwendigen Angaben. Auch die Daten für statistische Auswertungen werden anonymisiert.

Mauterhebungsdaten nach § 4 Abs. 2 Satz 2 ABMG dürfen vom Bundesamt für Güterverkehr (BAG) sowie der Firma Toll Collect GmbH zum Zweck des Betriebs des Mautsystems erhoben, verarbeitet und genutzt werden. Diese sind nach § 9 Abs. 1 ABMG unverzüglich bei der Toll Collect GmbH zu löschen, wenn ein Mauterstattungsverlangen nicht fristgerecht gestellt worden ist. Bei fristgerechtem Erstattungsverlangen sind die Daten unverzüglich nach Abschluss des Verfahrens zu löschen. Das BAG darf die Mauterhebungsdaten dagegen nach § 9 Abs. 2 ABMG länger aufbewahren und muss die Kennzeichendaten 3 Jahre nach Ablauf des Kalenderjahres, in dem die mautpflichtige Autobahnbenutzung beendet wurde, die übrigen Mauterhebungsdaten 6 Jahre nach Übermittlung löschen. Kontrolldaten sind nach § 9 Abs. 3 ABMG spätestens nach Abschluss eines Mauterstattungsverfahrens, Daten nicht mautpflichtiger Lkw nach § 9 Abs. 5 ABMG sofort nach dem Kontrollvorgang zu löschen. Im Falle der Nacherhebung sind Kontrolldaten nach § 9 Abs. 4 ABMG bei der Toll Collect GmbH nach Abschluss des Nacherhebungsverfahrens und beim BAG zwei Jahre nach erstmaliger Speicherung zu löschen. Darüber hinaus dürfen nach dem ABMG gespeicherte Daten gemäß § 9 Abs. 6 in anonymisierter Form zur Erstellung von Geschäftsstatistiken verwendet werden.

Die im Seeschifffahrtsbereich ausgetauschten Daten werden von der nationalen zuständigen Stelle entsprechend den gesetzlichen Vorschriften bis zur nächsten Aktualisierung gespeichert.

Im Rahmen der Kontrolle der Flugsicherung entstandene Radardaten werden mindestens 14 Tage aufbewahrt (§ 24 Abs. 2 Satz 1 3. Variante der Verordnung über die Betriebsdienste der Flugsicherung) und anschließend gelöscht, sofern sie nicht Gegenstand einer behördlichen oder gerichtlichen Untersuchung sind. Zustandsdaten von Navigationssystemen (vgl. die Antwort zu Frage 70) werden zur Qualitätssicherung gespeichert und in der Regel nach zwölf Monaten gelöscht.

Die Erhebung, Verarbeitung und Nutzung von Daten durch die Bundesstelle für Flugunfalluntersuchung erfolgt nach § 25 FlUUG. Die Aufbewahrungs- und Löschfristen sind in § 27 FlUUG definiert.

Ob Daten von Navigationssystemen im Bereich des Vermessungswesens zum Beispiel bei den Ländern oder bei Privatfirmen über die Verwendung für Gebührenabrechnungen entsprechend den Vorschriften zur Belegführung im Rechnungswesen hinaus gespeichert werden, ist der Bundesregierung nicht bekannt.

X. Strafverfolgung

73. Sieht die Bundesregierung vor dem Hintergrund des Urteils des Bundesverfassungsgerichts zum so genannten Großen Lauschangriff unter datenschutzrechtlichen Gesichtspunkten Änderungsbedarf, und falls ja, welchen?

Das Bundesverfassungsgericht knüpft in seinem Urteil vom 3. März 2004 – 1 BvR 2378/98, 1 BvR 1084/99 – an eine mittlerweile gefestigte Rechtsprechung zur Problematik der strafprozessualen heimlichen Ermittlungsmaßnahmen an. Diese Rechtsprechung zielt darauf ab, den Rechtsschutz der von

solchen Maßnahmen Betroffenen – unter anderem durch Benachrichtigungs-, Kennzeichnungs-, Datenlöschungs- und Dokumentationspflichten – zu verbessern. Insoweit prüft die Bundesregierung, ob auch im Hinblick auf andere strafprozessuale heimliche Ermittlungsmaßnahmen Änderungsbedarf besteht.

74. Wie ist der Stand der Evaluation der Vorschriften der Strafprozessordnung zur Telekommunikationsüberwachung, und wann wird diese Evaluation abgeschlossen sein?

Die Regelungen der §§ 100a, 100b StPO sind Gegenstand des ersten Teils der im Auftrag der Bundesregierung vom Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg erstellten und im Mai 2003 vorgelegten Untersuchung zur „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen“. Der zweite Teil dieser rechtstatsächlichen Untersuchung wurde im November 2004 vorgelegt und befasst sich mit der „Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung („großer Lauschangriff“) nach § 100c Abs. 1 Nr. 3 StPO“. Da die Bundesregierung ein harmonisches Gesamtkonzept der strafprozessualen heimlichen Ermittlungsmaßnahmen anstrebt, ist der Stand der Evaluation der Vorschriften der Strafprozessordnung zur Telekommunikationsüberwachung jedoch auch von der Ausgestaltung der Vorschriften, die die akustische Wohnraumüberwachung regeln, sowie von den zur Verfügung stehenden rechtstatsächlichen Erkenntnissen zur Auskunft über Telekommunikationsverbindungsdaten abhängig. Im Hinblick auf die Frist, die das Bundesverfassungsgericht in seinem Urteil vom 3. März 2004 – 1 BvR 2378/98, 1 BvR 1084/99 – gesetzt hat, genießt die Novellierung der Vorschriften zur akustischen Wohnraumüberwachung derzeit Vorrang. Die Bundesregierung prüft ferner, auf welche Weise der einstimmig vom Bundestag gefassten Entschließung Rechnung getragen werden kann, die die Bundesregierung auffordert, dem Deutschen Bundestag bis zum 30. Juni 2007 einen Erfahrungsbericht über die praktische Umsetzung der §§ 100g und 100h StPO seit deren Einführung vorzulegen (Bundesratsdrucksache 845/04).

75. Wie beurteilt die Bundesregierung die Gefahr, dass bei so genannten Joker-Abfragen, z. B. durch Namensgleichheit oder unvollständige oder falsche Suchabfragen, Unverdächtige ins Visier der Ermittlungsbehörden geraten?

Nach § 112 Abs. 1 Satz 4 TKG hat der Verpflichtete zu gewährleisten, dass im Rahmen des automatisierten Auskunftsverfahrens der Abruf von Daten unter der Verwendung unvollständiger Abfragedaten oder die Suche mittels einer Ähnlichenfunktion erfolgen kann. Die nähere Ausgestaltung dieser für eine erfolgreiche Arbeit der Strafverfolgungs- und Sicherheitsbehörden unerlässlichen Möglichkeit, ist nach § 112 Abs. 3 Satz 1 Nr. 3 TKG einer Rechtsverordnung vorbehalten, in der die Mindestanforderungen an den Umfang der einzugebenden Daten zur möglichst genauen Bestimmung der gesuchten Person, der zulässige Umfang der an die ersuchende Stelle zu übermittelnden Treffer und die Anforderungen an die Löschung der nicht benötigten Daten geregelt werden. Hierdurch wird den Datenschutzinteressen hinreichend Rechnung getragen. Im Übrigen liegt eine möglichst große Begrenzung der Trefferanzahl auch im Interesse der Strafverfolgungs- und Sicherheitsbehörden.

Darüber hinaus wird die Problematik in dem durch das Gesetz zur effektiveren Nutzung von Dateien im Bereich der Staatsanwaltschaften vom 10. September 2004 (BGBl. I Seite 2318) neu eingeführten § 492 Abs. 4a StPO ausdrücklich geregelt und begrenzt.

76. Auf welche Daten, insbesondere auf welche staatlichen Datensammlungen und Register, sollen andere europäische Staaten bei der vom Bundesminister des Innern, Otto Schily, geforderten europaweiten Rasterfahndung (vgl. BILD vom 27. März 2004) Zugriff erhalten?

Die Durchführung von EU-weiten Maßnahmen, die mit der Bezeichnung „Profilfahndungen“ zutreffender beschrieben sind, könnte in der Weise erfolgen, dass jeder EU-Mitgliedstaat anhand abgestimmter Profilkriterien nach eigenem Recht eine Profilfahndung in eigenen Datenbeständen durchführt. Ein Zugriff anderer Staaten auf deutsche Dateien wäre im Rahmen EU-weiter Profilfahndungen nicht vorgesehen.

77. Wie soll gewährleistet werden, dass deutsche Bürgerinnen und Bürger über die über sie gespeicherten und weitergegebenen Daten informiert werden?

Nach § 19 Abs. 1 Satz 1 BDSG hat der Betroffene das Recht, von der verantwortlichen Stelle Auskunft über die zu seiner Person gespeicherten Daten zu erhalten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, über die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und über den Zweck der Speicherung. Dies gilt nach § 491 Abs. 1 StPO auch im Strafverfahren sowie nach § 12 Abs. 5 BKAG auch im Hinblick auf die durch das Bundeskriminalamt an das Ausland zur Strafverfolgung übermittelten Daten. Auch das Europol-Übereinkommen enthält einen solchen Auskunftsanspruch (Artikel 19 Europol-ÜE).

Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist dieser nach § 19a Abs. 1 Satz 1 und 2 BDSG von der Speicherung, der Identität der verantwortlichen Stelle, über die Zweckbestimmungen der Erhebung und Verwendung sowie über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten. Bei aus heimlichen Ermittlungsmaßnahmen im Strafverfahren gewonnenen Daten wird nach § 101 StPO gewährleistet, dass die Betroffenen nachträglich von der Maßnahme benachrichtigt werden.

Allerdings muss berücksichtigt werden, dass beispielsweise bei Daten, die zum Zwecke der Fahndung übermittelt werden, eine Auskunftserteilung den Zweck der Maßnahme gefährden kann. Aus diesem Grunde unterbleibt eine Auskunftserteilung bzw. Unterrichtung nach § 19 Abs. 4 BDSG unter anderem dann, wenn die ordnungsgemäße Aufgabenerfüllung der verantwortlichen Stelle oder die öffentliche Sicherheit gefährdet würde und deshalb das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

In diesen Fällen hat der Betroffene jedoch das Recht, sich nach § 19 Abs. 6 BDSG an den Bundesbeauftragten für den Datenschutz zu wenden, der anstelle des Betroffenen die Auskunft erhält. Er darf dem Betroffenen jedoch ohne Zustimmung der verantwortlichen Stelle keine Mitteilungen machen, die Rückschlüsse auf deren Erkenntnisstand zulassen.

78. Nach welchen Kriterien sollen Daten im Rahmen der Rasterfahndung abgefragt werden, um potenzielle islamistische Terroristen zu finden, insbesondere vor dem Hintergrund, dass so genannte Schläfer sich gerade unauffällig verhalten und sich nach außen in die deutsche Gesellschaft eingliedern?

Profilkriterien werden jeweils kurzfristig vor Beginn einer Maßnahme auf der Basis aktueller, personenbezogener Erkenntnisse erstellt, die sich verallgemeinern lassen. Darüber hinaus ist anzumerken, dass Kriterien der Profilfahndung aus kriminaltaktischen Gründen der Geheimhaltung unterliegen, um den möglichen Erfolg einer solchen Maßnahme nicht von vornherein zu unterlaufen.

XI. Videoüberwachung

79. In welchem Umfang – auch im Vergleich zu den Vorjahren – werden öffentliche Plätze, Straßen und Wege durch Polizei- und Ordnungsbehörden Video überwacht?

Die Videoüberwachung öffentlicher Plätze, Straßen und Wege durch Polizei- und Ordnungsbehörden erfolgt nach Maßgabe des polizeilichen Gefahrabwehrrechts der Länder, die in den vergangenen Jahren vermehrt an Kriminalitätsbrennpunkten offene Videoüberwachungsmaßnahmen durchführen. Die ständige Konferenz der Innenminister und -senatoren der Länder hatte sich im Mai 2000 für einen offenen Einsatz von Videoüberwachungsmaßnahmen im öffentlichen Raum ausgesprochen. Entsprechende Änderungen im Polizeirecht haben die meisten Länder bereits vollzogen. Konkrete Erkenntnisse über den Erfolg solcher Maßnahmen liegen der Bundesregierung nicht vor.

Im Zuständigkeitsbereich des Bundes ist die Videoüberwachung auf Bahnhöfen (seit 1993), Flughäfen und im Bereich des Schutzes von Bundesorganen ein wichtiges Unterstützungsinstrument polizeilicher Arbeit des Bundesgrenzschutzes.

Darüber hinaus hat der Bundesgrenzschutz im Rahmen seiner bahnpolizeilichen Aufgabenwahrnehmung nach dem Fund der Bombe auf dem Hauptbahnhof Dresden im Juni 2003 verschiedene Maßnahmen in enger Abstimmung mit den Polizeien der Länder sowie der Deutschen Bahn AG ergriffen. Dazu gehört neben verbesserten Verfahrensabsprachen vor allem seit November 2003 der verstärkte Einsatz moderner Video-Technik mit der Möglichkeit der Aufzeichnung an Bahnhöfen und Haltepunkten. Der Einsatz dieser Technik erfolgt nur für die Bewertung von Gefahrensituationen und zur Strafverfolgung und führte bereits zu beträchtlichen polizeilichen Erfolgen. Im Zeitraum von Oktober 2003 bis Oktober 2004 konnten mit Hilfe der Videoaufzeichnung 703 Straftaten festgestellt werden. Dabei reicht die Bandbreite der Tatbestände von Hausfriedensbruch und Sachbeschädigung über Taschendiebstahl und Körperverletzung bis zu Raub und Vergewaltigung. Von 703 Straftaten konnten 411 mit Hilfe der Videoaufzeichnung als Beweismittel aufgeklärt werden. Hierbei wurden 546 Straftäter ermittelt und identifiziert. Darüber hinaus wurde in 772 Fällen zur Unterstützung Gefahren abwehrender Einsätze auf Videotechnik zurückgegriffen. Zu diesen Einsätzen zählten insbesondere Gewahrsamnahmen, Platzverweise, Hilfeleistungen, Personenfahndungen und Überwachungsmaßnahmen im Zusammenhang mit Fußballfans auf Bahngelände. Schließlich wurden Videoaufzeichnungen in 122 Fällen bei unklaren Gefahrenlagen, wie beispielsweise beim Auffinden verdächtiger Gegenstände und bei Anschlagsandrohungen, herangezogen.

80. Liegen der Bundesregierung Erkenntnisse darüber vor, ob die Sicherheit Video überwachter Plätze tatsächlich gestiegen ist, und wie lässt sich dies belegen?

Auf die Antwort zu Frage 79 wird verwiesen.

81. Hat die Videoüberwachung öffentlicher Plätze, Straßen und Wege zu einer besseren Aufklärung von Straftaten geführt, und woran lässt sich dies ablesen?

Auf die Antwort zu Frage 79 wird verwiesen.

82. Welchen Handlungsbedarf sieht die Bundesregierung hinsichtlich der Videoüberwachung öffentlicher Plätze, Straßen und Wege?

Auf die Antwort zu Frage 79 wird verwiesen.

83. Hat die Bundesregierung Kenntnisse über technische Möglichkeiten und deren Anwendung durch Polizei- und Ordnungsbehörden, aus Standbildern der Videoüberwachung mittels biometrischer Verfahren (Gesichtsscan) konkrete Personen zu ermitteln, sieht sie insoweit gesetzgeberischen Handlungsbedarf, und wenn ja, welchen?

Die hier in Rede stehende Technologie befindet sich noch im Entwicklungsstadium und ist für polizeiliche Zwecke noch nicht einsatzreif. Insofern kann keine Aussage getroffen werden, für welche Einsatzszenarien solche Systeme aus technischer und taktischer Sicht geeignet sind und könnte erst nach Feststellung der grundsätzlichen Eignung eines solchen Verfahrens ein eventuell notwendiger gesetzgeberischer Handlungsbedarf eingeschätzt werden.

84. Ist die Bundesregierung der Ansicht, dass der Missbrauch von Aufzeichnungsmöglichkeiten als eigener Straftatbestand in das Strafgesetzbuch aufgenommen werden sollte, und wenn ja, wie begründet sie ihre diesbezügliche Auffassung?

Nein. Zur Begründung ist auf den am 6. August 2004 in Kraft getretenen § 201a StGB (Verletzung des höchstpersönlichen Lebensbereiches durch Bildaufnahmen) hinzuweisen, der auf einem interfraktionellen Gesetzentwurf beruht. Die Vorschrift bedroht unter anderem diejenigen mit Strafe, die von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick geschützten Raum befindet, unbefugt Bildaufnahmen herstellen oder übertragen und dadurch deren höchstpersönlichen Lebensbereich verletzen. Öffentlich zugängliche Orte sind bewusst aus dem Schutzbereich der Strafvorschrift ausgeklammert worden. Die Gesetzesbegründung führt dazu aus (vgl. Bundestagsdrucksache 15/2466, Seite 5 f.):

„Mit Bildaufnahmen, die in der Öffentlichkeit hergestellt werden, würde ein breites Spektrum an Alltagshandlungen unter Strafe gestellt werden. Ein Kriterium, mit dem solche Phänomene annähernd trennscharf ausgegrenzt werden könnten, ist nicht vorhanden. Insbesondere hilft die Einfügung einer Bagatellklausel wie der des § 201 Abs. 2 Satz 2 StGB nicht weiter. Ein Straftatbestand, der die unbefugte Abbildung in allen Lebensbereichen unter Strafe stellt, liefe Gefahr, das Übermaßverbot staatlichen Strafens sowie das strafrechtliche Bestimmtheitsgebot zu verletzen. Zudem erscheint die engere Tatbestandsfassung vertretbar, da der Einzelne im öffentlichen Lebensraum damit rechnen muss, auf Bildaufnahmen abgebildet zu werden."

Die Bundesregierung schließt sich diesen Ausführungen an.

XII. Kfz-Kennzeichen-Scanning

85. Welche Einsatzmöglichkeiten des Kfz-Kennzeichen-Scannings sieht die Bundesregierung, und welche Erfahrungen wurden hiermit in der Bundesrepublik Deutschland bisher gemacht?

Ein möglicher Anwendungsbereich für die automatisierte Erfassung und Auswertung von Kfz-Kennzeichen im öffentlichen Straßenraum besteht in der Verfolgung von Straßenverkehrsordnungswidrigkeiten. Insbesondere bei Geschwindigkeitskontrollen, Rotlichtüberwachungsanlagen und Abstandskontrol-

len wenden die Polizeien der Länder seit langem Verfahren an, bei denen im Falle der Feststellung eines Verstoßes die Kennzeichen der Fahrzeuge, mit denen die Betroffenen die Zuwiderhandlung begangen haben, erfasst und für die spätere Auswertung durch die Bußgeldbehörde gespeichert werden.

Anhand der gespeicherten Kennzeichendaten werden sodann die Kfz-Halter ermittelt und anschließend das Bußgeldverfahren gegen die (mutmaßlichen) Fahrer durchgeführt (vgl. auch Antwort zu Frage 86). Diese Form der Verkehrskontrolle ist auch Gegenstand der Empfehlung der Europäischen Kommission zu Durchsetzungsmaßnahmen im Bereich der Straßenverkehrssicherheit vom 21. Oktober 2003.

Für die Kennzeichenerfassung kommen verschiedene technische Systeme, darunter prinzipiell auch das Kfz-Kennzeichen-Scanning, in Betracht. Für die Erhebung und die Verwendung der Daten gelten die Regelungen der Strafprozessordnung und des Ordnungswidrigkeitengesetzes (vgl. § 46 Abs. 1, insbesondere in Verbindung mit § 100c Abs. 1 Nr. 1 Buchstabe a StPO, § 49c OWiG in Verbindung mit § 483 ff. StPO, für die Halterdatenabfragen §§ 35, 36 StVG).

Unbeschadet dessen hat die Bundesregierung die Einsatzmöglichkeiten des Kfz-Kennzeichen-Scannings und deren Rechtsgrundlagen noch nicht abschließend geprüft. Ein Einsatz im Zuständigkeitsbereich des Bundes ist im öffentlichen Straßenraum noch nicht erfolgt und derzeit auch nicht geplant.

Vor einer abschließenden Entscheidung über einen Einsatz beim Bundesgrenzschutz sind insbesondere die Ergebnisse der Untersuchung der rechtlichen und technischen Möglichkeiten zur Einführung eines automatischen Kfz-Kennzeichen-Lesesystems abzuwarten, die derzeit auch im Rahmen der ständigen Konferenz der Innenminister und -senatoren der Länder durchgeführt werden. Daher besteht kein Anlass, (Vor-)Festlegungen für den Bundesgrenzschutz zu treffen. Erprobungen nimmt der Bundesgrenzschutz derzeit nicht vor.

86. Soll das Kfz-Kennzeichen-Scanning nach Ansicht der Bundesregierung auf das Scannen von Kfz-Kennzeichen beschränkt werden bzw. beschränkt bleiben, oder soll auch der Fahrzeugführer erfasst werden, sollen die Daten gespeichert werden, und wenn ja, wie lange?

Soweit die Verfahren zur Kennzeichenerkennung zum Zweck der Verfolgung von Straßenverkehrsordnungswidrigkeiten eingesetzt werden, ist es grundsätzlich erforderlich, auf dem Beweisfoto auch den Fahrer erkennen zu können, weil ihm – und nicht dem Halter – die Sanktionen für den Verkehrsverstoß aufzuerlegen sind. Die Dauer der Speicherung richtet sich grundsätzlich nach der Dauer des Bußgeldverfahrens (vgl. § 49c Abs. 2 OWiG in Verbindung mit § 483 Abs. 1, § 489 StPO). Im Übrigen wird auf die Antwort zu Frage 85 verwiesen.

87. Ist die Bundesregierung der Ansicht, dass die Strafprozessordnung eine geeignete Rechtsgrundlage bietet für das Scannen von Kraftfahrzeugen, um gestohlene Autos und gesuchte Personen ausfindig zu machen?

Nach derzeitiger Rechtslage ist nach Ansicht der Bundesregierung der Einsatz von automatischen Kennzeichenlesesystemen – abgesehen von der in der Antwort zu Frage 85 dargestellten Fallgestaltung – nur im Rahmen von Straßenkontrollen nach § 111 StPO zulässig.

88. Ist die Bundesregierung der Ansicht, dass für die rechtliche Beurteilung im Hinblick auf eine geeignete Rechtsgrundlage ein Unterschied besteht, ob sich das Scanning nur auf das reine Beobachten beschränkt, oder ob die Kennzeichen anschließend gespeichert werden?

Das Bundesverfassungsgericht hat in seiner Grundsatzentscheidung zum Volkszählungsgesetz festgestellt, dass jede natürliche Person gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe ihrer persönlichen Daten geschützt werden müsse. Jeder Eingriff in das Grundrecht auf informationelle Selbstbestimmung bedürfe einer gesetzlichen Grundlage, aus der sich Voraussetzungen und Umfang der Beschränkung klar und für den Bürger erkennbar ergeben (BVerfGE 65, 1, 43 f.).

Jeder der genannten Datenverarbeitungsvorgänge ist demnach nur dann zulässig, wenn und soweit eine Rechtsgrundlage gerade diesen Eingriff erlaubt. Es ist also eine Rechtsgrundlage erforderlich, die klar und für den Bürger erkennbar regelt, welche seiner Daten von wem wann für welchen Zweck erhoben, gespeichert, übermittelt oder genutzt werden. Das Beobachten als Erheben von Daten ist also zu unterscheiden vom Speichern der Daten und von weiteren Datenverarbeitungsvorgängen. Jede einzelne dieser Maßnahmen bedarf einer gesonderten Rechtsgrundlage.

89. Wie will die Bundesregierung der Gefahr begegnen, dass bei einer Ausweitung der Kfz-Kennzeichen-Scannings im Rahmen von Kriminalitätsbekämpfung, Verkehrsüberwachung und Mautsystemen oder anderer Anwendungsbereiche Bewegungsprofile erstellt und gespeichert werden?

Von entscheidender Bedeutung ist in diesem Zusammenhang zunächst, dass eine flächendeckende Überwachung mittels der angegebenen Systeme nicht vorgesehen ist. Darüber hinaus regeln die erforderlichen konkreten Rechtsgrundlagen die nur beschränkten Möglichkeiten des Einsatzes, insbesondere der Speicherung und Verwertung gewonnener Daten.

So werden bei der Verkehrsüberwachung die Daten nur im Bußgeldverfahren bei der jeweiligen Behörde und in einem späteren Verfahrensstadium ggf. bei der Staatsanwaltschaft oder dem Gericht verwertet. Hierbei handelt es sich somit um eine rein lokale Verwertung, aus der ein Bewegungsprofil nicht erstellt werden kann.

Da die StPO für den Einsatz von Kfz-Kennzeichenlesesystemen außerhalb des Anwendungsbereichs des § 100c Abs. 1 Nr. 1 Buchstabe a StPO (vgl. Antwort zu Frage 85) und des § 111 StPO (vgl. Antwort zu Frage 87) keine Rechtsgrundlage vorsieht, stellt sich auch in diesem Zusammenhang die Frage nach der Zulässigkeit der Erstellung von Bewegungsprofilen nicht.

90. Unterstützt die Bundesregierung Forderungen nach Einführung einer City-Maut nach Londoner Vorbild, wie z. B. vom Abgeordneten Albert Schmidt erhoben (vgl. BILD am Sonntag vom 29. Februar 2004), und wenn ja, welche datenschutzrechtlichen Belange werden nach Auffassung der Bundesregierung davon betroffen sein?

Die Einführung einer City-Maut, d. h. einer Straßenbenutzungsgebühr für innerstädtische Gebiete oder einzelne Ballungsräume ist von Seiten der Bundesregierung nicht vorgesehen, zumal Planung und Umsetzung von Verkehrskonzepten in Ballungsräumen primär Angelegenheit der Länder und Gemeinden ist.

XIII. Innerbehördlicher Datenabgleich

91. Plant die Bundesregierung Behörden stärker zu vernetzen und so in stärkerem Maße als heute verschiedenen Stellen Zugriff auf die bei einer Stelle gespeicherten Daten von Bürgern zu ermöglichen, und wenn ja, welche Behörden und Daten sind davon betroffen?

Die Bundesregierung strebt an, Behörden stärker zu vernetzen, indem sie die Verwendung der vorhandenen Netzinfrastrukturen fördert und für besondere Anforderungen eigene Netzinfrastrukturen aufbaut. Beispiele für eigene Netzinfrastrukturen sind der Informationsverbund Berlin-Bonn (IVBB) und dessen geplanter Ausbau zu einem Informationsverbund der Bundesverwaltung (IVBV), der die Netze der Ressorts umfassen soll. Darüber hinaus wird ein eigenes Netz für den Datenaustausch mit Bundesländern und Kommunen angestrebt, welches in Teilen im so genannten TESTA-Deutschland realisiert ist und zum „Deutschen Verwaltungsnetz“ ausgebaut werden soll.

Ferner arbeitet die Bundesregierung derzeit an einer Umstrukturierung beim Bundesverwaltungsamt, um dort die Daten von Antragstellern in Visaverfahren unter jeweils einem Aktenzeichen zusammen zu führen. Dies wird einen verstärkten Datenaustausch bewirken, weil ein Datenaustausch im Visaverfahren zwischen den Auslandsvertretungen ermöglicht wird. Dieser ist derzeit nur zwischen den Auslandsvertretungen und dem Bundesverwaltungsamt möglich. Das Auswärtige Amt hat bezüglich der für 2005 vorgesehenen Umsetzung bereits den Bundesbeauftragten für den Datenschutz befasst und wird sich mit diesem auch weiterhin eng abstimmen.

Für die Übermittlung der elektronischen Personalakten der Antragsteller auf Kriegsdienstverweigerung sowie gegebenenfalls die Übermittlung von deren Daten von den Kreiswehrersatzämtern an das Bundesamt für den Zivildienst (BAZ) soll zukünftig das Bundesverwaltungsnetz genutzt werden. Dann kann die Übermittlung in Papierform entfallen; eventuell werden so später auch die bisher genutzten Magnetbänder entbehrlich. Ein Zugriff des BAZ auf die Daten und Personalakten bei den Kreiswehrersatzämtern oder umgekehrt ist nicht beabsichtigt.

Durch das Gesetz zur effektiveren Nutzung der Dateien im Bereich der Staatsanwaltschaften (vgl. Antwort zu Frage 75), das am 1. März 2005 in Kraft treten wird, erhalten die Staatsanwaltschaften die Befugnis, aus dem polizeilichen Informationssystem (INPOL) Daten über Fahndungsausschreibungen zur Festnahme und Aufenthaltsermittlung, über Freiheitsentziehungen und aus der DNA-Analysedatei abzurufen. Ferner wird den Staatsanwaltschaften durch Rechtsverordnung des Bundesministeriums des Innern der Zugriff auf weitere Daten aus dem INPOL-System eingeräumt werden können. Außerdem erhält die Polizei durch das Gesetz ein Zugriffsrecht im automatisierten Verfahren auf das Zentrale Staatsanwaltschaftliche Verfahrensregister. Das Gesetz zur effektiveren Nutzung der Dateien im Bereich der Staatsanwaltschaften (siehe Antwort zu Frage 75) trägt den Belangen des Datenschutzes angemessen Rechnung.

Das Bundesministerium der Justiz arbeitet zurzeit mit den Justizministerien von Frankreich, Spanien und Belgien an einem Pilotprojekt der Gründung und des Aufbaus eines Strafregisterverbundes. Die Teilnahme an dem Projekt der elektronischen Vernetzung der nationalen Strafregister steht anderen Mitgliedstaaten der Europäischen Union offen. Damit sollen die Möglichkeiten der Strafverfolgungsbehörden verbessert werden, von im jeweils anderen Staat verhängten Vorstrafen Kenntnis zu erhalten und diese in laufenden Ermittlungs- oder Strafverfahren zu berücksichtigen. Dabei wird eine Zusammenarbeit derart angestrebt, dass die im jeweiligen nationalen Register vorhandenen Daten auf Anfrage eines anderen Registers elektronisch über definierte Formate und Stan-

dards ausgetauscht werden. Die Auskunftsanträge an das Register des anderen Staates sollen dabei über das jeweilige nationale Register kanalisiert werden. Die jeweils fremden Register erhalten somit keinen unmittelbaren Zugriff auf die beim Bundeszentralregister gespeicherten Daten. Stattdessen wird ihnen jeweils auf eine konkrete elektronische Anfrage ein konkreter Datensatz oder eine Fehlanzeige übermittelt. Auch hierbei sieht die Bundesregierung im Ergebnis keine Gefahr für den Datenschutz: Das neue Verfahren soll lediglich die derzeit bereits zulässige, aber aufwändigere Auskunftserteilung auf dem Post- oder Telefaxweg ersetzen. Dabei ist ein direkter lesender Zugriff der abfrageberechtigten Stellen auf die Datenbestände des Bundeszentralregisters nicht vorgesehen. Damit sind Online-Auswertungen der Datenbestände ausgeschlossen, womit eine der typischerweise mit einem automatisierten Abruf personenbezogener Daten verbundenen datenschutzrechtlichen Gefahren nicht zu befürchten ist. Risiken des geplanten Verfahrens für den Datenschutz und die Datensicherheit, die darin bestehen, dass Verfahren zur Datenfernübertragung grundsätzlich geeignet sind, die Gefahr einer unbefugten Kenntnisnahme von gespeicherten Daten zu erhöhen, sind nicht neuartig. Ihnen kann und wird durch geeignete technische und organisatorische Maßnahmen wirksam begegnet werden.

Die Bundesregierung beabsichtigt schließlich, im Rahmen einer völkerrechtlichen Vereinbarung mit den Nachbarstaaten Belgien, Luxemburg, den Niederlanden und Österreich zur Bekämpfung der grenzüberschreitenden Kriminalität, des Terrorismus sowie der illegalen Migration den Abgleich und Austausch von Daten insbesondere im Bereich der DNA-Identifizierungsmuster, der Fingerabdrücke und der Kfz-Daten zu intensivieren. Die Vereinbarung soll gegebenenfalls Modell für entsprechende EU-weite Regelungen sein. Präzise datenschutzrechtliche Bestimmungen in dem geplanten Übereinkommen selbst verhindern in diesem Zusammenhang einen unzulässigen Umgang mit den genannten Daten, deren Übermittlung im Übrigen an die Vorgaben des jeweiligen nationalen Rechts anknüpft.

92. Sieht die Bundesregierung darin eine Gefahr für den Datenschutz, und wenn ja, wie will sie dieser begegnen?

Auf die Antwort zu Frage 91 wird verwiesen.

93. Wie will die Bundesregierung die Zusammenlegung von Arbeitslosen- und Sozialhilfe und den damit einhergehenden Datenabgleich zwischen Kommunen und Bundesagentur für Arbeit datenschutzrechtlich absichern?

Wie in der Antwort auf Frage 53 dargelegt, findet bei der Zusammenführung von Arbeitslosenhilfe und Sozialhilfe in der Grundsicherung für Arbeitsuchende ein Datenabgleich zwischen Kommunen und der Bundesagentur für Arbeit nicht statt. Die Bundesregierung beabsichtigt allerdings, im Rahmen von § 52 Abs. 4 SGB II zur Verhinderung von Leistungsmissbrauch einen automatisierten Datenabgleich vorzusehen. Sie bereitet dafür eine Rechtsverordnung vor, die das Verfahren und die Kosten des automatisierten Datenabgleichs regeln soll. Im Rahmen des Verfahrens zum Erlass dieser Rechtsverordnung wird der Bundesbeauftragte für den Datenschutz beteiligt. Die Verordnung soll Anfang 2005 erlassen werden und in Kraft treten.

Soweit für die Grundsicherung für Arbeitsuchende die Kenntnis von Vorgängen zur Sozialhilfe oder zur Arbeitslosenhilfe erforderlich ist, ermöglicht es § 65d SGB II den Agenturen für Arbeit und den kommunalen Trägern, Unterlagen zu verwenden, die auf Grund des Bezugs von Arbeitslosenhilfe oder von Leistungen nach dem Bundessozialhilfegesetz entstanden sind.

XIV. Internationale Zusammenarbeit

94. Welche datenschutzrechtlichen Probleme sieht die Bundesregierung im Zusammenhang mit der internationalen Terrorismusbekämpfung, insbesondere bei der Datenübermittlung an andere Staaten?

Die Rechtsvorschriften, die die Übermittlung personenbezogener Daten im Rahmen der internationalen Verbrechensbekämpfung regeln, unterscheiden grundsätzlich nicht nach dem Anlass der jeweiligen Zusammenarbeit. Daher ergeben sich bei der Übermittlung personenbezogener Daten zum Zweck der Bekämpfung des internationalen Terrorismus keine besonderen datenschutzrechtlichen Probleme. Die gravierende Gefahr weltweiter Terroranschläge hat allerdings die Notwendigkeit der internationalen polizeilichen Zusammenarbeit einschließlich des Austauschs personenbezogener Daten generell sowie insbesondere mit den islamisch geprägten Staaten des Nahen und Mittleren Ostens, Nordafrikas, Zentral- und Südostasiens sowie mit den USA deutlich verstärkt. Das Bundeskriminalamt kann nach § 14 Abs. 1 BKAG – erstens – zur Erfüllung einer ihm obliegenden Aufgabe, hierzu gehören die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung des internationalen Terrorismus, – zweitens – zur Strafverfolgung und -vollstreckung nach Maßgabe der Vorschriften über die internationale Rechtshilfe in strafrechtlichen Angelegenheiten oder – drittens – zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr für die öffentliche Sicherheit personenbezogene Daten übermitteln. Eine Übermittlung unterbleibt, wenn durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden, insbesondere, wenn im Empfängerland ein angemessener Datenschutzstandard nicht gewährleistet wäre (§ 14 Abs. 7 Satz 7 BKAG). Die Bundesregierung prüft derzeit, ob § 14 Abs. 7 Satz 7 BKAG mit Blick auf den Entwurf eines neu zu schaffenden § 61a Abs. 1 des Gesetzes über die internationale Rechtshilfe in Strafsachen (IRG), der sich derzeit im Gesetzgebungsverfahren befindet, einer Änderung bedarf.

Der Entwurf eines § 61a Abs. 1 IRG sieht vor, dass Gerichte und Staatsanwaltschaften personenbezogene Daten aus strafprozessualen Ermittlungen ohne Ersuchen an öffentliche Stellen anderer Staaten sowie an zwischen- und überstaatliche Stellen weitergeben dürfen (so genannte Spontanauskünfte). Auch hier werden die schutzwürdigen Interessen der Betroffenen berücksichtigt, indem eine Übermittlung nach § 61a Abs. 3 IRG zu unterbleiben hat, wenn für das Gericht oder die Staatsanwaltschaft offensichtlich ist, dass im Einzelfall schutzwürdige Interessen des Betroffenen am Ausschluss der Übermittlung überwiegen.

95. An welche Staaten werden Daten deutscher Bürgerinnen und Bürger im Rahmen der internationalen Terrorismusbekämpfung weitergegeben?

Auf die Antwort zu Frage 94 wird verwiesen. Das Bundeskriminalamt übermittelt personenbezogene Daten deutscher Staatsangehöriger ebenso wie die Daten von Betroffenen mit anderer Staatsangehörigkeit an Drittstaaten nur, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist und die übrigen Übermittlungsvoraussetzungen vorliegen.

Im Rahmen der Europol-Kooperation werden personenbezogene Daten auch deutscher Bürgerinnen und Bürger, soweit dies erforderlich ist, zum einen an Europol selbst übermittelt. Europol darf die Daten im Rahmen des Europol-Informationssystems sowie innerhalb von Arbeitsdateien zu Analysezwecken nach den Bestimmungen des Europol-Übereinkommens verarbeiten. Zum anderen werden mit den nationalen Verbindungsbeamten bei Europol Daten bilateral ausgetauscht. Mit Verbindungsbeamten bei Europol, die Vertreter von Drittstaaten sind, erfolgt ein solcher Austausch nur, sofern das entsprechende

Zusammenarbeitsabkommen – unter bestimmten Bedingungen – den Austausch personenbezogener Daten ausdrücklich vorsieht. Entsprechende Abkommen wurden mit Bulgarien, Island, Norwegen, Rumänien und den USA geschlossen.

96. In welchem Umfang werden Daten sowohl hinsichtlich der Anzahl der betroffenen Personen als auch hinsichtlich der Art, Form und Menge der Daten übermittelt?

Das Bundeskriminalamt führt keine statistischen Erhebungen zum Umfang der an inländische und ausländische Dienststellen übermittelten personenbezogenen Daten durch. Im Rahmen seines gesetzlichen Auftrages (vgl. Antwort zu Frage 94) übermittelt das Bundeskriminalamt personenbezogene Daten vor allem zur Unterstützung deutscher sowie ausländischer Ermittlungsverfahren mit Bezügen zu Deutschland, zur Bearbeitung strategischer Grundsatzfragen sowie zur Unterstützung von Auswerteprojekten bei Europol.

97. Wie kontrolliert die Bundesregierung die Weiterverwendung und Speicherung der an andere Staaten übermittelten personenbezogenen Daten?

Es ist nicht Aufgabe der Bundesregierung, die Weiterverwendung und Speicherung übermittelter personenbezogener Daten im jeweiligen Empfangsstaat zu kontrollieren. Allerdings entspricht es bereits allgemeinen datenschutzrechtlichen Grundsätzen, dass übermittelnde Stellen Hinweisen auf eine zweckwidrige oder aus anderem Grund unzulässige Verwendung von Daten durch die empfangende Stelle nachgehen müssen. Dies gilt auch für die internationale Zusammenarbeit bei der Terrorismusbekämpfung.

Für den Datenaustausch im Rahmen des Europol-Übereinkommens wurde eine gemeinsame Kontrollinstanz geschaffen, die in Kooperation mit den nationalen Datenschutzbeauftragten die ordnungsgemäße Verwendung der Daten sowohl bei Europol als auch im jeweiligen EU-Mitgliedstaat kontrolliert (vgl. Artikel 23, 24 des Europol-Übereinkommens). Hinweisen auf etwaige Unregelmäßigkeiten, die sich aus dieser Kontrolltätigkeit ergeben, geht die Bundesregierung nach.

98. Liegen in jedem Fall Zusagen der ausländischen Staaten vor, deutsche und europäische Datenschutzgrundsätze bei der Verwendung und Speicherung von Daten deutscher Staatsangehöriger zu beachten, und welche Möglichkeiten haben deutsche Staatsangehörige im Falle der Nichtbeachtung dieser Grundsätze?

Nein, nicht in jedem Fall. Es ist wie folgt zu unterscheiden:

Im Rahmen der strukturierten Zusammenarbeit auf EU-Ebene, auf die ein Großteil des internationalen Datenverkehrs entfällt, ergeben sich entsprechende Verpflichtungen aus den geschlossenen europäischen Übereinkommen. Beispielhaft sei hier auf Artikel 14 des Europol-Übereinkommens verwiesen. Dieser verpflichtet die EU-Mitgliedstaaten zur Gewährleistung eines Datenschutzstandards, der zumindest dem entspricht, der sich aus der Verwirklichung der Grundsätze des Übereinkommens des Europarats vom 28. Januar 1981 ergibt. Dieser Mindeststandard wird durch weitere Verpflichtungen aus den genannten Übereinkommen ergänzt.

Soweit die Übermittlung personenbezogener Daten aufgrund einer völkervertraglich vereinbarten bilateralen Zusammenarbeit erfolgt, ergeben sich wechselseitige Zusagen der Vertragsstaaten zur Einhaltung datenschutzrechtlicher Mindeststandards aus einer entsprechenden Datenschutzklausel, die regelmäßig sei-

tens der Bundesregierung in die Verhandlungen eingebracht und als Vertragsbestandteil verankert wird.

Das Bundeskriminalamt weist bei einer Übermittlung personenbezogener Daten außerhalb des Anwendungsbereichs bilateraler und multilateraler Verträge nach § 14 Abs. 7 Satz 3 und 4 BKAG die empfangende Stelle darauf hin, dass die Daten nur zu dem Zweck genutzt werden dürfen, zu dem sie übermittelt werden. Ferner wird der empfangenden Stelle für das betreffende Datum der beim Bundeskriminalamt vorgesehene Löschungszeitpunkt mitgeteilt. Die entsprechenden Hinweise sind Gegenstand einer Datenschutzklausel, die im internationalen Schriftverkehr der übermittelten Information beigefügt wird.

Die genannten Grundsätze gelten nicht nur für die Daten deutscher Staatsangehöriger, sondern für die Daten sämtlicher Betroffener.

Ob Betroffene die Einhaltung von Zusagen im Empfangsstaat – notfalls gerichtlich – geltend machen können, bestimmt sich nach der dortigen nationalen Rechtsordnung. Aus bilateralen und multilateralen Verträgen, die zwischen Staaten geschlossen werden, ergeben sich solche Direktansprüche in der Regel nicht. Eine Nichtbeachtung gegebener Zusagen, Entsprechendes gilt auch für die Nichtbeachtung der Datenschutzklausel im „vertragslosen“ Datenverkehr, kann jedoch einen Umstand darstellen, der die Fortsetzung des Austauschs personenbezogener Daten in Frage stellen oder verbieten kann, da in einem solchem Fall – je nach Schweregrad des Verstoßes – schutzwürdige Interessen des Betroffenen im Sinne des § 14 Abs. 7 Satz 7 BKAG beeinträchtigt sein können. Dies können Betroffene gegenüber dem Bundeskriminalamt – gegebenenfalls auch gerichtlich – geltend machen. Im Falle einer unzulässigen Datenübermittlung kommen zudem Ansprüche auf Schadensersatz nach §§ 7, 8 BDSG in Betracht.

99. Welche Maßnahmen hat die Bundesregierung ergriffen bzw. wird sie ergreifen, um die Daten deutscher Bürgerinnen und Bürger nach den Grundsätzen der informationellen Selbstbestimmung in der internationalen Zusammenarbeit zu schützen?

Auf die Antwort zu Frage 97 und 98 wird verwiesen.

100. Wie will die Bundesregierung sicherstellen, dass deutsche Bürgerinnen und Bürger den Überblick über ihre an andere Staaten weitergegebenen und dort gespeicherten Daten behalten?

Das Bundeskriminalamt hat die Übermittlung personenbezogener Daten im internationalen Datenverkehr aufzuzeichnen und dabei den Anlass der Übermittlung zu vermerken (§ 14 Abs. 7 Satz 3 BKAG). Jede natürliche Person hat grundsätzlich die Möglichkeit, mit Hilfe ihres Auskunftsrechts in Erfahrung zu bringen, an welche anderen Stellen Daten über sie weitergegeben wurden (§ 12 Abs. 5 BKAG in Verbindung mit § 19 Abs. 1 Nr. 2 BDSG). Ergänzend wird auf die Antwort zu Frage 77 verwiesen.

101. Von wem und nach welchem Zeitraum werden betroffene Bürgerinnen und Bürger über die Weitergabe ihrer Daten informiert?

Eine Unterrichtungspflicht besteht nicht. Im Übrigen wird auf die Antwort zu Frage 100 verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333