

Große Anfrage

der Abgeordneten Gisela Piltz, Ernst Burgbacher, Rainer Funke, Jörg van Essen, Daniel Bahr (Münster), Rainer Brüderle, Angelika Brunkhorst, Helga Daub, Ulrike Flach, Otto Fricke, Horst Friedrich (Bayreuth), Dr. Christel Happach-Kasan, Klaus Haupt, Birgit Homburger, Dr. Werner Hoyer, Michael Kauch, Gudrun Kopp, Jürgen Koppelin, Harald Leibrecht, Markus Löning, Dirk Niebel, Günther Friedrich Nolting, Hans-Joachim Otto (Frankfurt), Eberhard Otto (Godern), Cornelia Pieper, Dr. Hermann Otto Solms, Dr. Rainer Stinner, Carl-Ludwig Thiele, Jürgen Türk, Dr. Claudia Winterstein, Dr. Volker Wissing, Dr. Wolfgang Gerhardt und der Fraktion der FDP

Überprüfung der personengebundenen datenschutzrechtlichen Bestimmungen

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

Wir fragen die Bundesregierung:

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?
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?
3. Welche Bedeutung schreibt die Bundesregierung den Datenschutzaudits für den Wettbewerb und die Förderung des Datenschutzes im privaten Bereich zu?
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?
5. Wie begründet die Bundesregierung ihr diesbezügliches Untätigbleiben seit Einführung des § 9a BDSG vor nunmehr fast drei Jahren?
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?
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?

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?
9. Wie bewertet die Bundesregierung vor diesem Hintergrund die Bedeutung des Bankgeheimnisses sowie das datenschutzrechtliche Prinzip, dass Daten grundsätzlich beim Betroffenen zu erheben sind?
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?
11. Welchen weiteren Behörden soll der Zugriff auf diese Daten ermöglicht werden, und welche Möglichkeiten der Datenzusammenführung und/oder -verknüpfung ergeben sich daraus?

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?
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?

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?
15. Was unternimmt die Bundesregierung, um die Durchsetzung der Datenschutzrechte gerade von Kindern zu fördern?
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?
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?
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?
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?
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?
21. Plant die Bundesregierung vor Erlass der zur Umsetzung dieses Vorhabens noch erforderlichen Verordnung die Datenschutzbeauftragten des Bundes und der Länder zu den datenschutzrelevanten Aspekten anzuhören?
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?
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?

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?
25. Welche Verfahren favorisiert die Bundesregierung für Reisepässe und andere Ausweisdokumente, und aus welchen Gründen?
26. Auf welche Verfahren haben sich die EU-Justiz- und -Innenminister geeinigt, und aufgrund welcher Überlegungen?
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?
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?
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?
30. Welche Verfahren sind aus Sicht der Bundesregierung am besten mit den Grundsätzen des deutschen und europäischen Datenschutzrechts zu vereinbaren, und warum?

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?
32. Trifft es ferner zu, dass der Bundesbeauftragte für den Datenschutz die Regelungen des Gesetzes dahingehend beurteilt hat, dass ein Paradigmenwechsel stattfindet, der sehr tief in das Selbstbestimmungsrecht der Versicherten eingreift, und wenn ja, wie hat er seine diesbezügliche Auffassung begründet, und was ist die Auffassung der Bundesregierung hierzu?
33. Welche detaillierte datenschutzrechtliche Prüfung der Konsequenzen aus der Einführung des GMG hat die Bundesregierung mit welchem Ergebnis durchgeführt?
34. Welche Möglichkeiten werden für den Patienten bei der geplanten elektronischen Patientenakte bestehen, Art und Umfang der gespeicherten Daten zu beeinflussen und Informationen hierüber zu erhalten?
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?
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?

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?
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?
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?
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?
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?
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?
43. Welche Voraussetzungen müssen nach Auffassung der Bundesregierung an eine Schweigepflichtentbindung zur Übermittlung von Patientendaten an Krankenversicherer gestellt werden?
44. Wie bewertet die Bundesregierung die derzeit gängige Praxis der pauschalen vorab erteilten Schweigepflichtentbindung?

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?
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?
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?

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?
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?
50. Inwiefern sieht die Bundesregierung in diesem Bereich Handlungsbedarf, eventuell auch auf europäischer Ebene?
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?
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?
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?
54. Wann beabsichtigt die Bundesregierung die Einbringung eines Arbeitnehmerdatenschutzgesetzes, welches für die Mitte der 15. Wahlperiode angekündigt worden war?

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?
56. Welche technischen Möglichkeiten bestehen hinsichtlich der Lokalisierung des Nutzers eines Mobiltelefons sowohl bei eingeschaltetem als auch bei ausgeschaltetem Mobiltelefon?
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?
58. Wie beurteilt die Bundesregierung Systeme wie beispielsweise „Phonetracker“, einen Mobilfunckerweiterungsdienst, durch den sich so genannte räumliche „Schutzonen“ definieren lassen, bei deren Verlassen Alarm ausgelöst wird, so dass beispielsweise Eltern über die Bewegungen ihres Kindes informiert werden?
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?
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?

61. Hält die Bundesregierung datenschutzrechtliche Bestimmungen bei den „Location Based Services“ für in ausreichendem Maße berücksichtigt, wenn ja, warum, bzw. nein, warum nicht?
62. Welchen Nutzen sieht die Bundesregierung in der in der Telekommunikationsgesetz-Novelle formulierten Verpflichtung zur Erhebung persönlicher Daten von Prepaid-Karten-Kunden?
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?
64. Plant die Bundesregierung als Konsequenz hieraus, 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?
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?
67. Welche besonderen Anforderungen an den Datenschutz ergeben sich im Zusammenhang mit den E-Government-Projekten?
68. Welche datenschutzrechtlichen Probleme ergeben sich aus der in § 21 Abs. 1a S. 1 Melderechtsrahmengesetz vorgesehenen Möglichkeit, einfache Melderegisterauskünfte via Internet zu erhalten?

IX. Navigationssysteme

69. Ist der Bundesregierung bekannt, ob von staatlichen Stellen ein Zugriff auf Informationen, die von Navigationssystemen gesendet werden, erfolgt?
70. Sind der Bundesregierung technische Methoden bekannt, mit denen auf Informationen oder Daten von Navigationssystemen zugegriffen werden kann?
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?
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?

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

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

XI. Videoüberwachung

79. In welchem Umfang – auch im Vergleich zu den Vorjahren – werden öffentliche Plätze, Straßen und Wege durch Polizei- und Ordnungsbehörden Video überwacht?
80. Liegen der Bundesregierung Erkenntnisse darüber vor, ob die Sicherheit Video überwachter Plätze tatsächlich gestiegen ist, und wie lässt sich dies belegen?
81. Hat die Videoüberwachung öffentlicher Plätze, Straßen und Wege zu einer besseren Aufklärung von Straftaten geführt, und woran lässt sich dies ablesen?
82. Welchen Handlungsbedarf sieht die Bundesregierung hinsichtlich der Videoüberwachung öffentlicher Plätze, Straßen und Wege?
83. Hat die Bundesregierung Kenntnisse über technische Möglichkeiten und deren Anwendung durch Polizei- und Ordnungsbehörden, aus Standbildern der Videoüberwachung mittels biometrischer Verfahren (Gesichtscan) konkrete Personen zu ermitteln, sieht sie insoweit gesetzgeberischen Handlungsbedarf, und wenn ja, welchen?
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?

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?
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?
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?
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?

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?
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?

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?
92. Sieht die Bundesregierung darin eine Gefahr für den Datenschutz, und wenn ja, wie will sie dieser begegnen?
93. Wie will die Bundesregierung die Zusammenlegung von Arbeitslosen- und Sozialhilfe und den damit einhergehenden Datenabgleich zwischen Kommunen und Bundesagentur für Arbeit datenschutzrechtlich absichern?

XIV. Internationale Zusammenarbeit

94. Welche datenschutzrechtlichen Probleme sieht die Bundesregierung im Zusammenhang mit der internationalen Terrorismusbekämpfung, insbesondere bei der Datenübermittlung an andere Staaten?
95. An welche Staaten werden Daten deutscher Bürgerinnen und Bürger im Rahmen der internationalen Terrorismusbekämpfung weitergegeben?
96. In welchem Umfang werden Daten sowohl hinsichtlich der Anzahl der betroffenen Personen als auch hinsichtlich der Art, Form und Menge der Daten übermittelt?
97. Wie kontrolliert die Bundesregierung die Weiterverwendung und Speicherung der an andere Staaten übermittelten personenbezogenen Daten?
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?
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?
100. Wie will die Bundesregierung sicherstellen, dass deutsche Bürgerinnen und Bürger den Überblick über ihre an andere Staaten weitergegebenen und dort gespeicherten Daten behalten?
101. Von wem und nach welchem Zeitraum werden betroffene Bürgerinnen und Bürger über die Weitergabe ihrer Daten informiert?

Berlin, den 26. Mai 2004

Dr. Wolfgang Gerhardt und Fraktion

