Dokumente zum Datenschutz

1999

Impressum

Herausgeber:

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg

Stahnsdorfer Damm 77, Haus 2
14532 Kleinmachnow

Telefon: 03 32 03 / 35 60
Telefax: 03 32 03 / 3 56 49

E-Mail:
Poststelle@LDA.Brandenburg.de

Internet:
http://www.lda.brandenburg.de

Berliner Beauftragter für Datenschutz und Akteneinsicht

Pallasstraße 25/26
10781 Berlin

Telefon: 0 30 / 78 76 88 44
Telefax: 0 30 / 2 16 99 27

E-Mail:
mailbox@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

Redaktion,
Layout: Laima Nicolaus, Volker Brozio

Druck: Verwaltungsdruckerei Berlin

1. Auflage: Februar 2000

Inhaltsverzeichnis

Seite

Vorwort

Die Institutionalisierung und die Kontrolle des Datenschutzes, insbesondere aber auch die Fortentwicklung der juristischen und technischen Rahmenbedingungen, sind eine Aufgabe, die wegen der föderalen Struktur der Bundesrepublik Deutschland auf eine Vielzahl von Institutionen verteilt ist. Für den öffentlichen Bereich sind in Bund und Ländern Datenschutzbeauftragte eingerichtet worden, die sich über ihre Arbeit in ihrem örtlichen Zuständigkeitsbereich hinaus auch mit grundsätzlichen Fragen der Sicherstellung der informationellen Selbstbestimmung befassen müssen. Hierbei ist ein hohes Maß an Koordination erforderlich, die in erster Linie im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geleistet wird. Deren Arbeitsergebnisse legt die Konferenz in Beschlüssen und Entschließungen nieder, die der Öffentlichkeit auch bekannt gemacht werden. Es ist eine gute Übung, dass diese Texte in den Jahresberichten der Datenschutzbeauftragten regelmäßig dokumentiert werden.

Unabhängig von der Konferenz der Datenschutzbeauftragten äußern sich mitunter einzelne Datenschutzbeauftragte zu Themen, an deren öffentlicher Diskussion ihnen besonders gelegen ist. So haben die Datenschutzbeauftragten der Länder Berlin, Brandenburg, Bremen, Nordrhein-Westfalen und Schleswig-Holstein, die sich im vergangenen Jahr bereits für einen Politikwechsel zum wirksameren Schutz der Privatsphäre ausgesprochen hatten, eine Trendwende in der Telekommunikationspolitik gefordert. Sie verlangen, dass die Politik vom Anspruch auf lückenlose Überwachung wegkommen müsse hin zu einem effektiven Schutz des Fernmeldegeheimnisses.

Wegen der steigenden Bedeutung des internationalen Datenverkehrs, insbesondere vor dem Hintergrund der sprunghaft wachsenden Nutzung des Internet, kommt der Kooperation auf europäischer und internationaler Ebene immer mehr Bedeutung zu. Gerade die Landesbeauftragten von Berlin und Brandenburg haben auf dem Gebiet des Datenschutzes in der Telekommunikation, zum Beispiel in der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation, intensive Arbeit geleistet.

Von zentraler Bedeutung für die Fortentwicklung des Datenschutzes in der Europäischen Union ist die Arbeit der Arbeitsgruppe zum Schutz der Individuen im Hinblick auf die Verarbeitung personenbezogener Daten, die nach Artikel 29 der Europäischen Datenschutzrichtlinie eingerichtet worden ist.

Die vorliegende Veröffentlichung dokumentiert die Arbeitsergebnisse der Konferenz der Datenschutzbeauftragten sowie der anderen Institutionen. Wie im vergangenen Jahr werden sie vom Brandenburgischen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht sowie dem Berliner Beauftragten für Datenschutz und Akteneinsicht gemeinsam als Ergänzung ihrer Tätigkeitsberichte für das Jahr 1999 herausgegeben.

Erneut soll die gemeinsame Veröffentlichung ein Zeichen dafür sein, dass es in den Ländern Brandenburg und Berlin Möglichkeiten der Zusammenarbeit gibt, die die Effizienz beider Seiten steigern können.

Dr. Alexander Dix

Prof. Dr. Hansjürgen Garstka

A. Beschlüsse und Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

I. Entschließungen der 57. Konferenz am 25./26. März 1999 in Schwerin

Modernisierung des Datenschutzrechts jetzt – umfassende Novellierung des BDSG nicht aufschieben

(Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein „Zwei-Stufen-Konzept" vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, dass das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbindung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nichtöffentlichen Bereich muss institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Geplante erweiterte Speicherung von Verbindungsdaten in der Telekommunikation

(Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die Bundesregierung und der Bundesrat werden demnächst über den Erlass der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, dass die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutzverordnung, dass alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbindung stattfand, kann dies in Einzelfällen dazu führen, dass die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur solange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muss sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlass für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, dass diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

Transparente Hard- und Software

(Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number – PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, dass Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL '98)

(Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999)

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFOPOL '98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, dass der entsprechende Entwurf bisher geheim gehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

II. Entschließungen zwischen den Konferenzen 1999

Angemessener Schutz auch für Untersuchungsgefangene

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. August 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die Bundesregierung den Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft vorgelegt hat. Damit wird die seit Jahren erhobene Forderung der Datenschutzbeauftragten nach einer bereichsspezifischen gesetzlichen Regelung aufgegriffen.

Diese Regelung muss das Strafverfolgungs- und Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft berücksichtigen. Gleichzeitig sind jedoch das Persönlichkeitsrecht der Gefangenen sowie die Unschuldsvermutung und der Anspruch auf wirksame Verteidigung im Strafverfahren angemessen zur Geltung zu bringen.

Der Gesetzentwurf der Bundesregierung trägt diesem Anliegen durch differenzierende Vorschriften teilweise Rechnung, lässt allerdings noch Raum für datenschutzrechtliche Verbesserungen. Die Stellungnahme des Bundesrates betont demgegenüber einseitig das staatliche Vollzugsinteresse und entfernt sich damit deutlich vom Ziel einer sorgfältigen Güterabwägung.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder muss die gesetzliche Regelung insbesondere folgenden Anforderungen genügen:

- Entgegen dem Vorschlag des Bundesrates, von einer inhaltlichen Überwachung nur ausnahmsweise nach dem Ermessen des Gerichts abzusehen, sollte im weiteren Gesetzgebungsverfahren an der Konzeption der Bundesregierung festgehalten werden. Der Gesetzentwurf der Bundesregierung differenziert bei der Überwachung der Unterhaltung mit Besucherinnen und Besuchern sowie bei der Kontrolle des Textes von Schriftstücken sachgerecht nach Haftgründen. Nur im Falle der Untersuchungshaft wegen Verdunkelungsgefahr sollten diese Maßnahmen unmittelbar und generell durch Gesetz vorgeschrieben werden, während sie bei Vorliegen anderer Haftgründe (z. B. Fluchtgefahr) nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen.

  Darüber hinaus sollte im weiteren Gesetzgebungsverfahren die Möglichkeit unüberwachter Kontakte der Gefangenen zu nahen Angehörigen mit Zustimmung der Staatsanwaltschaft auch in Fällen der Untersuchungshaft wegen Verdunkelungsgefahr erwogen werden. Stichprobenartige Überprüfungen von Schriftstücken durch die Vollzugsanstalt anstelle einer Textkontrolle sollten nicht den gesamten Schriftverkehr einzelner Gefangener umfassen. Dies könnte sich im Ergebnis als verdachtsunabhängige Totalkontrolle ohne richterliche Entscheidung auswirken.

- Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigten muss auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot wirksamer Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen, wie vom Bundesrat befürwortet.

- Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt (z. B. Sozialleistungsträger, Ausländerbehörden) und an Forschungseinrichtungen müssen die schutzwürdigen Interessen der Betroffenen im Rahmen einer

Abwägung berücksichtigt werden. Auch die Erteilung von Auskünften an die Verletzten der Straftat sollte der Gesetzgeber unter Beachtung der Unschuldsvermutung regeln.

- Die vom Bundesrat vorgeschlagene erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen im Hinblick auf den Zweck der Untersuchungshaft würde wesentliche Datenschutzrechte in einem besonders sensiblen Bereich weitgehend entwerten und ist daher abzulehnen.

„Gesundheitsreform 2000"

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1999)

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes „Gesundheitsreform 2000":

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf lässt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Gesundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiter reichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

I. Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u. a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und -verarbeitungsbefugnisse vor.

II. Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen, und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

III. Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

IV. Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

V. Die zur Begründung besonders angeführten Punkte „Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewährleistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern“ vermögen insoweit nicht zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, so dass keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

VI. Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

VII. Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotentials von derart umfassenden Datenbeständen müsste der Entwurf im Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise die Verlängerung der Speicherdauer von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von 5 auf 10 Jahre, unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarztmodell, der integrierten Versorgung und den Bonus-Modellen sowie unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17. Juni 1999)

Bei der Einführung der Befugnis zum „Großen Lauschangriff“ hat der Gesetzgeber im Grundgesetz ein Verfahren zur parlamentarischen Kontrolle weit reichender Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung verankert (Artikel 13 Abs. 6 GG). Dieses Verfahren dient nach dem Willen des Gesetzgebers der parlamentarischen Kontrolle der Normeffizienz. Auch wenn es die Überprüfung von Lauschangriffen durch die Gerichte und Datenschutzbeauftragten nicht ersetzt, hat es gleichwohl eine grundrechtssichernde Bedeutung. Jetzt ist jedoch bekannt geworden, dass einige Landesjustizverwaltungen der Ansicht sind, Art. 13 Abs. 6 GG sehe eine Berichtspflicht über Lauschangriffe zu Strafverfolgungszwecken gegenüber den Landesparlamenten nicht vor.

Im Gegensatz dazu vertritt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Auffassung, dass die Verfassung eine effektive parlamentarische Kontrolle von Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muss. Bei Maßnahmen zur Strafverfolgung durch Landesbehörden besteht die parlamentarische Verantwortlichkeit gegenüber den Landesparlamenten. Die Landtage müssen die Möglichkeit haben, die ihnen in anonymisierter Form übermittelten Berichte der Landesregierungen öffentlich zu erörtern. Die Landesparlamente sollten deshalb durch Gesetz eine regelmäßige Berichtspflicht der Landesregierung für präventiv-polizeiliche und repressive Lauschangriffe vorsehen. Nur auf diese Weise ist eine wirksame parlamentarische Kontrolle der Ausübung dieser einschneidenden Überwachungsbefugnisse gewährleistet.

Wird durch eine solche Kontrolle deutlich, dass die akustische Wohnraumüberwachung für Zwecke der Strafverfolgung in der Praxis nicht die vom Gesetzgeber angestrebte Effizienz im Verhältnis zur Häufigkeit und Intensität der Grundrechtseingriffe zeigt, können Landesregierungen, die das Bundesrecht in eigener Verantwortung auszuführen haben, über den Bundesrat darauf hinwirken, die Befugnis für eine derartige Überwachung wieder aufzuheben oder zumindest zu modifizieren.

III. Entschließungen der 58. Konferenz am 7./8. Oktober 1999 in Rostock

Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 9./10. März 1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16. August 1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss von 17. September 1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

„Täter-Opfer-Ausgleich und Datenschutz“

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28. Mai 1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut

des „Täter-Opfer-Ausgleichs“ nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei“ könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die „fachlich geleitete Auseinandersetzung“ der „am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden“.

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am „Täter-Opfer-Ausgleich“ Beteiligten muss gesetzlich geschützt werden.

Eckpunkte der deutschen Kryptopolitik – ein Schritt in die richtige Richtung

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so dass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Dis-

kussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger“ besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,
- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,
- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offen gelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: „Im gegenwärtigen Entwicklungszustand der

Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern."

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs.1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Patientenschutz durch Pseudonymisierung

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten" verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis – also ohne richterliche Anordnung – erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigt.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen – abweichend von den gesetzlich vorgesehenen Verfahren – systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Reglung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

(Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999)

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weit reichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungs-

daten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutender Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31. Dezember 1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern stattdessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

B. Datenschutzbeauftragte fordern Trendwende in der Telekommunikationspolitik: Weg vom Anspruch auf lückenlose Überwachung hin zu einem effektiven Schutz des Fernmeldegeheimnisses

Berliner Datenschutzbeauftragter

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Der Landesbeauftragte für den Datenschutz Freie Hansestadt Bremen

Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

Der Landesbeauftragte für den Datenschutz bei dem Präsidenten des Schleswig-Holsteinischen Landtages

Für eine Sicherung der freien Telekommunikation in unserer Gesellschaft

Hintergrundpapier

Inhaltsübersicht

I. Telekommunikation boomt – Grundrechte gefährdet

Die Bedeutung der Telekommunikation hat in den letzten Jahrzehnten stark zugenommen und dieser Trend wird sich weiter beschleunigen. Seit der Erfindung des „Fernsprechers" in der zweiten Hälfte des 19. Jahrhunderts sind weltweite Telekommunikationsnetze entstanden, deren Bedeutung sich grundlegend gewandelt hat. Über diese Netze wird längst nicht mehr nur Sprache transportiert, sondern auch Telefaxe (vom Telex oder „Fernschreiber" spricht heute kaum noch jemand) und Informationen aller Art in digitalisierter Form (bis hin zu Bildern, Musikstücken etc.). Mit Hilfe der Telekommunikation können Entfernungen zwischen Kontinenten z. B. satellitengestützt in Sekundenschnelle überbrückt und lebenswichtige Informationen in kürzester Zeit an den Zielort übermittelt werden. Das Internet, das zugleich die *Konvergenz von Individual- und Massenkommunikation,* von Telekommunikation, Fernsehkonsum und Multimedia verdeutlicht, ist nur die vorläufig letzte Stufe der Entwicklung von Telekommunikationsnetzen. Nicht ohne Grund widmet die *Internationale Funkausstellung Berlin 1999* dem Internet besondere Aufmerksamkeit. Die Menschen „unterhalten" sich in mehrfacher Hinsicht mit Hilfe der Telekommunikation. Digitalfernsehen, Web-TV und Push-Technologien einerseits und die bevorstehende Nutzung von Kabelnetzen für Sprachtelefonie andererseits lassen die Grenzen zwischen Fernseh- und PC-Nutzung zunehmend verschwimmen. Fest- und Mobilfunknetze wachsen immer mehr zusammen. Die Informationsgesellschaft ist ohne Telekommunikation undenkbar.

Die medial vermittelte Kommunikation ergänzt zunehmend die unmittelbare Kommunikation zwischen Menschen, ohne sie völlig ersetzen zu können. Patientinnen und Patienten holen telefonisch ärztlichen Rat ein, Menschen in seelischer Not nutzen die Telefonseelsorge oder die Drogenberatung im Internet, Wirtschaftsunternehmen tauschen Daten miteinander aus. Umso wichtiger ist es, dass die Kommunikation unter Einschaltung der Technik, die Dritte zur Verfügung stellen, ebenso *vertraulich* stattfinden kann wie die unmittelbare persönliche Kommunikation (jedenfalls wenn – was der Regelfall ist – alle Beteiligten dies wünschen). Dem dient das grundrechtlich geschützte *Fernmelde- oder Telekommunikationsgeheimnis (Art. 10 Grundgesetz)*. Es soll eine überwachungsfreie Kommunikation sichern und ist von zentraler Bedeutung nicht nur für den Grundrechtsschutz der einzelnen Bürgerinnen und Bürger, sondern auch für die freie Kommunikation in einer freien und demokratischen Gesellschaft insgesamt. Denn „. . . die Befürchtung einer Überwachung mit der Gefahr einer Aufzeichnung, späteren Auswertung, etwaigen Übermittlung und weiteren Verwendung durch andere Behörden kann schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen, hier insbesondere zur Vermeidung bestimmter Gesprächsinhalte . . . führen". Diese Umstände, die das Bundesverfassungsgericht in seiner jüngsten Entscheidung zur *verdachtslosen Rasterfahndung* im grenzüberschreitenden Fernmeldeverkehr (BVerfG, Urt. v. 14. Juli 1999, – 1 BvR 2226/94 – u. a., S. 95) ausdrücklich hervorgehoben hat, sind bisher zu wenig beachtet worden.

II. Kontrollnetz wird immer engmaschiger

Dem Telekommunikationsgeheimnis (Art. 10 Grundgesetz) droht durch die technischen und rechtlichen Entwicklungen eine *Erosion,* der dringend Einhalt geboten werden muss, wenn die Informationsgesellschaft in Deutschland eine demokratisch und rechtsstaatlich verantwortbare Zukunft haben soll.

Staatliche Überwachungsmaßnahmen in offenen Kommunikationsnetzen berühren angesichts des sich abzeichnenden Wandels des Internets zum Massenmedium zugleich die grundrechtlich geschützte Freiheit, frei die eigene Meinung zu äußern *(Meinungsfreiheit, Artikel 5 Abs.1 Satz 1 Grundgesetz)* und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten *(Informationsfreiheit, Artikel 5 Abs.1 Satz 1 Grundgesetz)*. Müssten Internet-Nutzerinnen und -Nutzer stets damit rechnen, dass sie vom Staat beobachtet werden, würde dies ihre Informationsfreiheit beeinträchtigen. Strafbare Inhalte, die im Internet angeboten werden, müssen an der Quelle, also bei denjenigen verfolgt werden, die diese Inhalte ins Netz stellen. Keinesfalls rechtfertigt es die *Strafverfolgung im Internet,* den gesamten Netzverkehr, also insbesondere das Verhalten der Nutzerinnen und Nutzer flächendeckend zu überwachen.

1. Datenspuren überall

Aufgrund der *Digitalisierung der Telekommunikationsnetze* hinterlässt jede Nutzung (jedes Telefongespräch, Fax, E-Mail, jeder Abruf aus dem WorldWideWeb) personenbezogene Spuren, die – für die Dauer ihrer Speicherung – ausgewertet werden können. In den gegenwärtig existierenden Mobilfunknetzen werden die Teilnehmerinnen und Teilnehmer „geortet", um die Verbindung herstellen zu können. Die Technik erlaubt die Erstellung von *Bewegungsprofilen.* Es gibt zwar zahlreiche Vorschläge aus der Wissenschaft für eine datenschutzfreundlichere Verbindungstechnik, sie konnten sich aber bisher – auch in der internationalen Standardisierung – nicht durchsetzen. Insofern ist das in der Bundesrepublik inzwischen flächendeckend eingeführte digitale Telekommunikationsnetz im Gegensatz zum früheren analogen Telefonnetz eine Infrastruktur, die eine *intensivere Überwachung* der Nutzerinnen und Nutzer technisch ermöglicht.

2. Immer mehr staatliche Abhörbefugnisse

Die materiell-rechtlichen *Befugnisse zur Überwachung* des Fernmeldeverkehrs durch Nachrichtendienste und Strafverfolgungsbehörden sind seit Verabschiedung der Notstandsgesetze 1968 *ständig ausgedehnt* worden. Allein der Katalog der Straftatbestände in der Strafprozessordnung, zu deren Verfolgung die Telekommunikation überwacht werden darf, ist 17-mal direkt erweitert worden. Zudem haben die Verfassungsschutzämter des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst für geheimdienstliche Zwecke sogar schon *im Vorfeld konkreter Gefahren* und seit 1994 auch das Zollkriminalamt zur Verhütung von Straftaten nach dem Außenwirtschaftsgesetz und dem Kriegswaffenkontrollgesetz das Recht, die Telekommunikation zu überwachen. Damit aber nicht genug: Es gibt kaum ein gesellschaftliches Problem *vom Doping bis zur Korruption,* zu dessen Bekämpfung nicht nach einer weiteren Ausdehnung der Abhörbefugnisse gerufen wird.

3. Effektivitätskontrolle? Fehlanzeige!

Bei der ständigen Erweiterung der Abhörbefugnisse fällt eines auf: Wenn darin ein unverzichtbares Mittel zur Bekämpfung aller möglichen Kriminalitätsformen oder auch nur gesellschaftlich unerwünschten Verhaltens gesehen wird, könnte angenommen werden, dass die Effektivität dieses Mittels hinreichend belegt ist. Das Gegenteil ist der Fall. *Aussagekräftige Statistiken oder eine Rechtstatsachenforschung zur Wirksamkeit der Fernmeldeüberwachung fehlen bisher fast völlig oder ihre Ergebnisse werden geheim gehalten.* Dies deutet darauf hin, dass die Sicherheitsbehörden

insgesamt gesehen kein Interesse an einer empirischen Überprüfung und objektiven Qualitätskontrolle der ausgedehnten Überwachungsbefugnisse haben, sondern eine öffentliche Diskussion dieser Frage eher scheuen. Zwar hat die Bundesregierung jetzt erklärt, dass die Wirksamkeit der strafprozessualen Fernmeldeüberwachung erstmals Gegenstand eines Forschungsprojekts sein soll. Der Evaluationsansatz muss allerdings sehr viel umfassender sein.

Auch fehlen Zahlen über die Häufigkeit, mit der Gerichte entsprechenden Anträgen der Sicherheitsbehörden folgen bzw. sie ablehnen. Deshalb lässt sich keine Aussage darüber treffen, ob der sog. *Richtervorbehalt* als verfahrensmäßige Sicherung gegenüber Telefonüberwachungsmaßnahmen in Strafverfahren überhaupt eine nennenswerte (sichernde) Filterfunktion ausübt. Dem steht die Praxis in den Vereinigten Staaten gegenüber, wo – übrigens vom Volk gewählte – Richterinnen und Richter über die Zahl und Wirksamkeit der von ihnen erlassenen Abhöranordnungen regelmäßig in öffentlichen Berichten *(wiretap reports)* Rechenschaft ablegen müssen.

Die wenigen vorliegenden Informationen zeigen allerdings zweierlei: Die Zahl der Überwachungsanordnungen hat in den vergangenen Jahren deutlich zugenommen (bundesweit wurden 1997 mehr als doppelt so viel Überwachungen angeordnet als 1995). Zum anderen wird deutlich, dass sich *Überwachungsmaßnahmen* keineswegs nur gegen Verdächtige, sondern mindestens genauso oft *gegen unverdächtige Dritte* richten, mit denen oder von deren Anschluss aus die Verdächtigen nach Ansicht der Ermittlungsbehörden telefonieren könnten. Jede Überwachungsmaßnahme in Kommunikationsnetzen erstreckt sich zwangsläufig auch auf andere Personen als nur die Verdächtigen. Wer aber weiß schon, dass die Telefonverbindung mit einer Person besteht, gegen die wegen einer bestimmten Straftat ermittelt wird?

4. Betrieb von Telekommunikationsnetzen verpflichtet zur geheimen Zuträgerschaft

Neben der Ausweitung der materiell-rechtlichen Überwachungsbefugnisse hat der Gesetzgeber in den letzten Jahren zahlreiche Vorschriften erlassen, die die *lückenlose technische Überwachbarkeit der Telekommunikation* möglichst unter allen Umständen und insbesondere auch in einem liberalisierten Telekommunikationmarkt sicherstellen sollen.

So verpflichtet die *Fernmelde-Überwachungsverordnung* von 1995 jede Person, die eine für den *öffentlichen Verkehr* bestimmte Fernmeldeanlage betreibt, angeordnete Überwachungsmaßnahmen mit entsprechenden technischen Schnittstellen umzusetzen und dabei nicht nur den Inhalt der übermittelten Nachrichten unverschlüsselt bereitzustellen, sondern auch Informationen über *die näheren Umstände der Telekommunikation,* also die angerufene Zielnummer, Beginn und Ende der Verbindung oder des Verbindungsversuchs, Art des genutzten Dienstes und bei Mobilfunkanschlüssen auch die Funkzellen (die Standorte), über die die Verbindung abgewickelt wird.

Auch das *Telekommunikationsgesetz* von 1996 verpflichtet alle, die Telekommunikationsanlagen (bisher: Fernmeldeanlagen) betreiben, angeordnete Überwachungsmaßnahmen jederzeit umzusetzen. Dabei sind unter Telekommunikationsanlagen nach der weiten gesetzlichen Definition alle „technischen Einrichtungen oder Systeme" zu verstehen, „die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können".

Der 11. Teil des Telekommunikationsgesetzes regelt sowohl das Fernmeldegeheimnis als auch die Pflicht zur Beteiligung an Überwachungsmaßnahmen. Zu Recht hat der Gesetzgeber den Anwendungsbereich des Fernmeldegeheimnisses nach dem Wegfall des Postmonopols auf alle Unternehmen und Personen erstreckt, die Telekommunikationsdienste erbringen, um die Vertraulichkeit der Telekommunikation auch in einem liberalisierten Markt auf demselben Niveau zu gewährleisten wie bisher. Dass der Gesetzgeber aber in diesem Zusammenhang im gleichen Atemzug auch *alle, die geschäftsmäßig Telekommunikation anbieten,* also selbst diejenigen, die *Nebenstellenanlagen* z. B. in *Krankenhäusern und Hotels* betreiben, zur Umsetzung von Überwachungsmaßnahmen verpflichtet, führt zu einem weit über den bisherigen Zustand unter Monopolbedingungen hinausreichenden Grad an Überwachbarkeit und ist unverhältnismäßig. Erfasst werden nun alle, die Telekommunikationsanlagen betreiben; ausreichend ist z. B. schon, dass in einem Betrieb oder einer Behörde den Mitarbeiterinnen und Mitarbeitern erlaubt wird, die Nebenstellenanlage oder das interne Netz auch für private Zwecke zu nutzen. Die Nebenfolge dieser Bestimmung ist nicht nur, dass die genannten Stellen ihre Telekommunikationsanlage nur in Betrieb nehmen dürfen, wenn sie abhörfähig und entsprechend getestet ist, sondern dass sich mit dem Kreis der Mitwirkungspflichtigen auch das *Risiko für illegale Abhörmaßnahmen erweitert.*

Das *Begleitgesetz zum Telekommunikationsgesetz* von 1997 hat diese erweiterten Mitwirkungspflichten auch in die Abhörbestimmungen nach dem G-10 und §§ 100 a ff. StPO aufgenommen und die Überwachungsmöglichkeiten auf *E-Mail-Adressen, IP-Nummern und Internet-Namen* erstreckt.

Das Bundeswirtschaftsministerium legte 1998 den Entwurf für eine Nachfolgeverordnung für die Fernmeldeüberwachungsverordnung, die sog. *Telekommunikationsüberwachungsverordnung* (TKÜV) vor, der die Einrichtung von permanenten Schnittstellen für die jederzeitige zeitgleiche Überwachung jeder Kommunikationsverbindung vorsah. Zugleich sollte eine Technische Richtlinie „Internet“ die Einzelheiten der Internet-Überwachung regeln. Beide Entwürfe wurden nach einhelliger Kritik aus der Wirtschaft und vonseiten der Datenschutzbeauftragten im vergangenen Jahr zurückgezogen. *Neuere Überlegungen des Bundeswirtschaftsministeriums* für eine Telekommunikationsüberwachungsverordnung zeigen zwar, dass der Umfang der Überwachungsverpflichtungen begrenzt werden soll. Mit Hilfe von Ausnahmeregelungen auf der Verordnungsebene ist das Problem der überschießenden gesetzlichen Überwachungsbefugnisse aber nicht zu lösen. Das Telekommunikationsgesetz selbst muss geändert werden.

5. Bundesweiter Zugriff auf Kundendateien

Darüber hinaus verpflichtet das Telekommunikationsgesetz von 1996 alle, die geschäftsmäßig Telekommunikationsdienste anbieten, also nicht nur lizenzpflichtige Telefongesellschaften wie die Telekom und ihre Wettbewerber, sondern nach dem Wortlaut des Gesetzes auch jedes Unternehmen, das Inhouse-Netze und Nebenstellenanlagen z. B. in Krankenhäusern und Hotels betreibt, *„Kundendateien“* zu führen, auf die die Sicherheitsbehörden jederzeit online und unbemerkt über die Regulierungsbehörde zugreifen dürfen. Der Sinn dieser Vorschrift bestand ursprünglich darin, in einem liberalisierten Telekommunikationsmarkt den Sicherheitsbehörden die Feststellung zu ermöglichen, bei welcher Telefongesellschaft eine verdächtige Person Kundin oder Kunde ist, um den zu überwachenden Anschluss identifizieren zu können. Das Gesetz ist aber in diesem Punkt so blankettartig formuliert, dass es auch die Nutzung der bei der Regulierungsbehörde vorliegenden Kundendateien als *bundesweites Adress- und Einwohnerregister* zulässt, ohne dass die so gewonnenen

Informationen zur Überwachung des Telekommunikationsverkehrs genutzt werden müssen. Noch 1990 hatte der Einigungsvertrag aus guten Gründen – nicht nur wegen der Querverbindung zur Staatssicherheit – die Auflösung des Zentralen Einwohnerregisters der ehem. DDR vorgeschrieben. Ungeklärt ist im Übrigen, wie die Kundendateien gegen Hackerangriffe wirksam geschützt werden können.

6. Überwachungsvorschrift aus der analogen Telefonwelt wieder belebt

Hinzu kommt, dass der aus der Zeit des analogen Telefonverkehrs stammende *§ 12 Fernmeldeanlagengesetz* nach wie vor in Kraft ist. Er erlaubt den Sicherheitsbehörden unter relativ einfachen Voraussetzungen den Zugriff auf Daten über die Telekommunikation, obwohl seit der Digitalisierung der Telekommunikation ein wesentlich umfangreicherer und aussagekräftigerer Datenkranz bei den Unternehmen, die Telekommunikation anbieten, gespeichert wird. Er entspricht nicht den Voraussetzungen, die das Bundesverfassungsgericht für Einschränkungen des Fernmeldegeheimnisses verlangt. Obwohl eine Einschränkung von § 12 FAG bei der Verabschiedung des TKG in Aussicht gestellt wurde, steht zu befürchten, dass seine Weitergeltung nach Ablauf der Frist Ende 1999 beschlossen wird.

7. Europäische Überwachungsstruktur im Aufbau (ENFOPOL)

Auch auf europäischer Ebene wird an einer *Intensivierung der Kommunikationsüberwachung* gearbeitet. Die Ratsarbeitsgruppe „Polizeiliche Zusammenarbeit" hat unter der Bezeichnung *„ENFOPOL 98"* Vorschläge für eine Entscheidung des Rates zur „Überwachung des Telekommunikationsverkehrs in Bezug auf neue Technologien" erarbeitet, die lange Zeit der Öffentlichkeit vorenthalten wurden. Hauptziel dieser Vorschläge ist es vordergründig, die Überwachungsmöglichkeiten der Polizei den neuen Technologien wie z. B. der Satellitentelefonie anzupassen. Zugleich sollen aber technische Überwachungsmöglichkeiten auf europäischer Ebene verabredet werden, für deren Ausnutzung zumindest in der Bundesrepublik die materielle Rechtsgrundlage fehlt. So verlangen die Sicherheitsbehörden in der Bundesrepublik bei Mobilfunkgesellschaften den Zugriff auf Personalien solcher Kundinnen und Kunden, die mit den immer populäreren datenschutzfreundlichen Guthabenkarten telefonieren wollen. Diese Forderung der Sicherheitsbehörden ist ebenso wenig nach dem Telekommunikationsgesetz gerechtfertigt wie es die Forderung nach einer Identifizierung all der Personen wäre, die bei der Telekom Telefonkarten für das Festnetz kaufen. Auch wenn der Europäische Rat die Entscheidung über diese Vorschläge im Mai 1999 noch vertagt hat, besteht zwischen den Regierungsvertretern in der Sache offenbar bereits Einigkeit.

Sowohl national wie auf europäischer Ebene tragen technische Überwachungsvorschriften auch dann zum *Aufbau einer Überwachungsmentalität* bei, wenn sie nur unter den materiellen gesetzlichen Voraussetzungen z. B. nach der Strafprozessordnung genutzt werden dürfen. Weil eine Überwachung der Telekommunikation technisch immer einfacher und umfassender möglich ist, sinkt das Rechtsbewusstsein für die Schwere des Rechtseingriffs. Dies lässt – weil technisch leicht umsetzbar – den Eingriff in das Fernmeldegeheimnis auch völlig Unverdächtiger als weniger gravierend erscheinen. Außerdem droht eine Absenkung des Schutzes der vertraulichen Telekommunikation über europäisch harmonisierte Überwachungsstandards, weil in sie auch die Rechtsvorstellungen von Ländern in Europa eingehen, in denen das Fernmeldegeheimnis keinen vergleichbar hohen Stellenwert hat wie in der Bundesrepublik.

8. Erweiterte Rolle der „Dienste“

Zusätzlich ist zu berücksichtigen, dass der Telekommunikationsverkehr offenbar auch von in- und ausländischen *Geheimdiensten* überwacht wird. Dabei spielt neben dem klassischen Aufgabenfeld dieser Dienste die *Wirtschaftsspionage* eine immer größere Rolle. Gleichzeitig ist eine *Aufweichung* des traditionell in der Bundesrepublik geltenden und von den Alliierten vor dem Hintergrund historischer Erfahrungen eingeführten *Trennungsgebots* zu beobachten. Danach sind Aufgaben und Mittel der Strafverfolgungs- und Polizeibehörden von den Aufgaben und Methoden der Geheimdienste im Interesse einer rechtsstaatlichen Kontrolle strikt zu trennen. Gerade im Bereich der Telekommunikationsüberwachung dürfen Polizei und Staatsanwaltschaft nicht zum verlängerten Arm des Verfassungsschutzes oder anderer „Dienste“ werden. Umgekehrt hat das Bundesverfassungsgericht den Informationsfluss vom Bundesnachrichtendienst zu den Strafverfolgungsbehörden bei der verdachtslosen Rasterfahndung in der grenzüberschreitenden Telekommunikation an enge Voraussetzungen geknüpft und dem Gesetzgeber aufgegeben, einen verfassungskonformen Zustand herzustellen.

III. Forderungen

Vor diesem Hintergrund fordern die *Datenschutzbeauftragten Berlins, Bremens, Nordrhein-Westfalens, Schleswig-Holsteins sowie der Datenschutz- und Informationszugangsbeauftragte Brandenburgs* eine grundlegende Änderung der deutschen Kommunikationspolitik. Nicht der unbedingte Wille, nirgendwo „abhörfreie Zonen“ entstehen zu lassen, sondern der aktive Schutz des Grundrechts der Bürgerinnen und Bürger auf freie und unbeobachtete Telekommunikation müssen im Vordergrund stehen. Deutschlands Weg in die Informations- und Kommunikationsgesellschaft ist rechtsstaatlich und demokratisch nur zu verantworten, wenn er mit klaren Garantien für die Grundrechte verbunden ist.

Der Bundesgesetzgeber muss über die vom Bundesverfassungsgericht angeordnete Modifikation des G-10-Gesetzes hinaus ein Gesetz zur *Sicherung der freien Telekommunikation* verabschieden. Grundlage muss eine *Evaluierung* der bisherigen Eingriffe in das Telekommunikationsgeheimnis sein. Mit ihrer Hilfe sind die bestehenden, in den vergangenen Jahren ständig erweiterten Überwachungsbefugnisse der Strafprozessordnung, des G-10 sowie des Außenwirtschaftsgesetzes auf ihre Notwendigkeit nach objektiven Kriterien zu prüfen.

Folgende Maßnahmen sind unverzichtbar:

1. Verpflichtung zur Datensparsamkeit und Datenvermeidung

Je weniger Daten personenbezogen verarbeitet werden, desto geringer sind die Eingriffsmöglichkeiten. Wer Angebote zur Telekommunikation macht, sollte außerdem verpflichtet werden, den Kundinnen und Kunden eine Option zur anonymen Nutzung des Telekommunikationsnetzes (z. B. durch Einsatz von Guthabenkarten auch bei häuslichen Festnetzanschlüssen) zur Verfügung zu stellen. Hilfreich könnte hierfür die Einführung der Möglichkeit sein, förmliche Audits zur Bewertung besonders datenschutzfreundlicher Telekommunikationsdienste durchzuführen.

2. Verschlüsselung als Standardleistung anbieten

Wer Telekommunikation anbietet, sollte verpflichtet werden, kostenlos Verschlüsselungmöglichkeiten als Universaldienstleistung anzubieten, ohne dass damit die generelle Verpflichtung zur Bereitstellung von Abhörschnittstellen für die Polizei und die Geheimdienste verbunden ist.

3. „Mediennutzungsgeheimnis" einführen

In das Teledienstedatenschutzgesetz des Bundes (und entsprechend auch in den Mediendienstestaatsvertrag der Länder) sollte ein ausdrückliches Mediennutzungsgeheimnis aufgenommen werden, um die verfassungsrechtliche Ausstrahlungswirkung des Kommunikationsgeheimnisses nach Artikel 10 GG auf einfachgesetzlicher Ebene klarzustellen. Ebenso wenig wie Zeitungsleserinnen und -leser es hinnehmen müssen, dass registriert wird, welche Zeitung sie in Papierform täglich lesen, ist eine Überwachung ihrer Medienpräferenz akzeptabel, wenn sie die Zeitung im Internet (als „webzine") lesen.

4. Mitwirkungspflichten bei Abhörmaßnahmen begrenzen

Die Pflicht zur Durchführung von staatlichen Überwachungsmaßnahmen muss durch Änderung des Telekommunikationsgesetzes und der entsprechenden Begleitgesetze auf diejenigen begrenzt werden, die öffentliche, lizenzpflichtige Telekommunikationsdienste erbringen. Nebenstellenanlagen in Hotels, Betrieben und Krankenhäusern usw. wären dann ausgenommen.

5. Überwachungsbefugnisse evaluieren

Überwachungsmaßnahmen bei der Telekommunikation müssen erstmals einer echten Effektivitätskontrolle unterzogen werden, auf deren Grundlage der Gesetzgeber ständig die Notwendigkeit der Beibehaltung bestimmter Befugnisse zu Eingriffen in das Kommunikationsgeheimnis in bestimmten Zeitabständen überprüfen sollte. Die gegenwärtig vorgeschriebene Geheimhaltung der entsprechenden Statistiken (§ 88 Abs. 5 Satz 3 TKG) ist nicht länger zu rechtfertigen.

6. Datenschutzfreundliche Techniken fördern

Die Bundesregierung wird aufgefordert, die Bürgerinnen und Bürger beim Schutz ihres Telekommunikationsgeheimnisses gegen illegales Abhören durch in- oder ausländische private Dritte zu unterstützen. Hierfür kommt in Betracht:

a) Der verstärkte Mitteleinsatz für die Erforschung und Entwicklung datenschutzfreundlicher Telekommunikationstechniken im Netz- und im Endgerätebereich.
b) Die Förderung von Tests auf Praktikabilität und Wirksamkeit entsprechender Techniken und ihrer kundenfreundlichen Markteinführung.

7. Berufliche Schweigepflichten wirksam schützen

Die Bundesregierung wird aufgefordert, eine geschlossene Konzeption für den besonderen Schutz der Telekommunikation von *Berufsgruppen, die besonderen Verschwiegenheitspflichten* unterliegen wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen usw. vorzulegen.

8. Strafrechtlichen Schutz des Kommunikationsgeheimnisses endlich ernst nehmen

Die Bagatellisierung von *Straftaten gegen den Schutz der Privatsphäre* ist zu beenden, z. B. durch:

a) stärkere polizeiliche Prävention gegen illegales Abhören
b) die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik
c) eine Effektivierung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen
d) die Prüfung, ob nicht ähnlich wie in anderen Bereichen Hackerangriffe straffrei bleiben sollten, wenn dabei festgestellte Sicherheitslücken in Telekommunikationsnetzen sofort angezeigt werden.

C. Beschlüsse der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation

Gemeinsamer Standpunkt zum Datenschutz bei Gebäude-Bilddatenbanken

angenommen auf der 25. Sitzung der Arbeitsgruppe am 29. April 1999 in Norwegen

– Übersetzung –

Computer haben die Fähigkeit, Informationen aus einer Reihe von Quellen einschließlich öffentlicher Register zu verknüpfen und zugänglich zu machen. Im Zusammenhang mit der Entwicklung von Geographischen Informationssystemen (GIS), die die Ortsbestimmung ermöglichen, und digitaler Fotografie- bzw. Bilderstellung kann dies das leichte Auffinden großer Informationsmengen durch Verknüpfung mit Adressen oder Planangaben (-koordinaten) ermöglichen. Darin liegt eine wachsende Bedrohung für die Privatsphäre einzelner Bürger. Eine aktuelle Entwicklung ist die systematische Sammlung digitaler Bilder von Gebäuden zum Aufbau von Gebäude-Bilddatenbanken ganzer Städte für kommerzielle Zwecke. Während es wichtige und legitime Anwendungen für Geographische Informationssysteme und digitale Aufnahmen von Gebäuden gibt, z. B. für Planungszwecke, muss die Position der Betroffenen hinsichtlich der kommerziellen Nutzung dieser Datenbanken gestärkt werden.

So setzen gegenwärtig beispielsweise Unternehmen in mehreren Ländern mobile Digitalkameras ein, die auf Kleintransportern montiert sind, um Bilder aller Gebäude in größeren Städten aufzuzeichnen. Die Daten können dann auf CD-ROM gespeichert und der Feuerwehr, der Polizei und Notfalldiensten zur Vorbereitung ihrer Einsätze angeboten werden. Es liegt aber auf der Hand, dass eine solche Datenbank auch für kommerzielle Zwecke genutzt werden kann. Die Bilder können mit Hausnummern, Namen und Adressen von Eigentümern und Bewohnern zur Beurteilung der Bonität (Scoring) oder Risiken durch Banken und Versicherungen auf Grund des Gebäudezustandes oder einer Einstufung der Wohngegend bzw. für Zwecke der Direktwerbung verknüpft werden. Die Daten können für fernsehgestützte Bilddatenbanken oder für Planungszwecke von Transportunternehmen (Lieferfirmen,Taxis usw.) verwendet werden. Sie werden oft mit Daten verknüpft, die mit Hilfe von Satelliten erhoben werden (Global Positioning System – GPS), und können dann genutzt werden, um realistische digitale Stadtpläne zu erzeugen und eine neue Generation Geographischer Informationssysteme zu unterstützen. Obwohl gegenwärtig – abhängig vom eingesetzten System – Probleme der Speicherkapazität und Verarbeitungsgeschwindigkeit auftreten können, wird sich dies wahrscheinlich ändern.

Es muss deutlich gemacht werden, dass eine totale Registrierung aller Gebäude in einer Stadt oder in einem Land zu einer Verarbeitung personenbezogener Daten führen wird, da ein Großteil der Informationen sich auf natürliche Personen bezieht, die durch Zuordnung zu spezifischen Elementen als Ausdruck ihrer physischen, wirtschaftlichen, kulturellen oder sozialen Identität bestimmbar sind (vgl. Artikel 2 a) und c) der Richtlinie 95/46/EG) und die direkt oder indirekt mit Verzeichnissen verknüpft werden können. Deshalb unterliegt die Schaffung von Bilddatenbanken dieser Art den nationalen Datenschutzgesetzen in Übereinstimmung mit der

EG-Datenschutzrichtlinie. Wo dies nicht bereits der Fall ist, sollte die nationale Gesetzgebung dem Betroffenen zumindest ein Widerspruchsrecht gegen die systematische Sammlung und Speicherung derartiger Bilddaten über seine Wohnumgebung für kommerzielle Zwecke einräumen. Die Tatsache, dass diese Informationen bereits zu einem gewissen Grad öffentlich zugänglich sind, schließt sie nicht von der Anwendung der Datenschutzgesetze aus. Darüber hinaus kann die Veröffentlichung solcher Datenbanken Sicherheitsprobleme für die Betroffenen (Eigentümer, Mieter oder Bewohner) verursachen. Es gibt einen Unterschied zwischen einem einzelnen Bürger, der für private Zwecke Aufnahmen eines bestimmten Gebäudes macht, und einem Unternehmen, das systematisch Bilder aller Gebäude in einer Stadt für kommerzielle Zwecke sammelt. Insbesondere muss der Betroffene das Recht haben, einer Einstellung dieser Daten in das Internet oder ihrer Speicherung auf elektronischen Datenträgern (z. B. CD-ROM) jederzeit zu widersprechen.

Gemeinsamer Standpunkt zu intelligenten Software-Agenten

angenommen auf der 25. Sitzung der Arbeitsgruppe am 29. April 1999 in Norwegen

– Übersetzung –

Ein Software-Agent wird definiert als ein Software-Produkt, das anstelle seines Benutzers agiert und versucht, ohne einen direkten Eingriff oder eine direkte Überwachung des Benutzers bestimmte Objekte zu finden oder bestimmte Aufgaben zu erledigen. Agenten können in verschiedener Weise bei der Telekommunikation verwendet werden. An erster Stelle können sie dazu benutzt werden, die Funktionalität eines Telekommunikationsnetzes zu erweitern. Es ist möglich, ein Netzwerk effizienter zu benutzen, wenn die Ressourcen an die Anforderungen der einzelnen Nutzer angepasst sind. Agenten können diese Aufgabe übernehmen, indem sie die Nutzer repräsentieren.

Eine andere Anwendung bezieht sich auf inhaltliche Mehrwertdienste, die mit Mitteln der Telekommunikation verbreitet werden: Agenten können im Auftrag des Nutzers verwendet werden, um Informationen (z. B. im Internet) zu selektieren und zu sammeln, sowie als Mittler gegenüber anderen Teilnehmern bei elektronischen Transaktionen auftreten. Im Augenblick stehen die ersten Dienste dieser Art zur Verfügung, ausgehend von einer einfachen „Push-Technologie“, die Informationen auf der Basis individuell spezifizierter Interessen dem Benutzer ins Haus bringt, bis hin zu komplizierten Systemen, die es gestatten, die Nutzung des Netzes zu personalisieren und die Aktivitäten der Nutzer nachzuvollziehen.

Die Entwicklung der Agenten-Technologie wird in intelligenten Software-Agenten gipfeln, Software-Programmen, mitunter mit dedizierter Hardware gekoppelt, die dazu bestimmt ist, komplette Aufgaben im Auftrag der Nutzer zu erledigen. In ihrer Rolle als Repräsentant einer Person wird eine Vielzahl personenbezogener Informationen erzeugt und durch die Operationen der Agenten verbreitet werden. Der Schutz der Privatsphäre und die Vertraulichkeit der Netzaktivitäten werden eines der größten Probleme sein, mit denen die Nutzung intelligenter Agenten in der Zukunft konfrontiert sein wird.

Dieser gemeinsame Standpunkt zielt darauf ab, eine erhöhte Aufmerksamkeit für die Risiken für die Privatsphäre zu erzeugen, die mit der Nutzung von Agenten verbunden sind, und die Systemdesigner zu ermutigen, Maßnahmen zum Schutz der Privatsphäre einzubauen. Die Risiken für die Persönlichkeitsrechte, die mit der Nutzung von Agenten verbunden sind, können wie folgt zusammengefasst werden:

1. Erstens: Risiken, die mit der Tatsache zusammenhängen, dass ein Agent im Auftrag eines Nutzers handelt. Nutzerprofile stellen einen wesentlichen Anteil der Aktivitäten von Agenten dar. Typischerweise umfasst das Nutzerprofil Informationen über Identität und Kommunikationspartner sowie eine Vielzahl von Informationen über persönliche Präferenzen. Wenn ein Agent im Netz operiert, werden personenbezogene Daten mit der Umgebung ausgetauscht und möglicherweise an nicht autorisierte dritte Parteien weitergegeben.
2. Zweitens: Risiken, die mit fremden Agenten verbunden sind, die im Auftrag anderer Teilnehmer handeln. Agenten oder allgemeiner ihre Nutzer, könnten mit Agenten konfrontiert werden, die im Auftrag anderer Teilnehmer handeln. Diese könnten freiwillig personenbezogene Daten von Individuen sammeln, indem sie eine Verkehrsanalyse durchführen, in Datenbanken eindringen, die Informationen über die Individuen enthalten, oder das Nutzerprofil eines Agenten zugänglich machen. Derartige Agenten können sogar verkleidet auftreten oder andere Agenten ausschalten.

Empfehlungen:

Maßnahmen müssen ergriffen werden, um das Auftreten von Risiken für die Privatsphäre durch intelligenten Software-Agenten zu reduzieren. Die Arbeitsgruppe empfiehlt, dass Folgendes Berücksichtigung findet, wobei die Anforderungen, die die Datenschutzprinzipien stellen, insbesondere diejenigen, die sich aus dem Zweck ergeben, für den der Agent erstellt worden ist, berücksichtigt werden müssen:

1. Software-Hersteller sollten in einem frühen Designstadium die Auswirkungen der Nutzung intelligenter Agenten für die Privatsphäre des Einzelnen bedenken. Dies ist notwendig, um die Konsequenzen, die in naher Zukunft entstehen könnten, unter Kontrolle zu halten.
2. Entwickler von Agenten sollten sicherstellen, dass die Nutzer die Kontrolle über ihre Systeme und die darin enthaltenen Informationen nicht verlieren. Sie sollten dem Nutzer ein Maximum an Transparenz über die Funktionsweise des Agenten verschaffen. Wenn Kontroll- und Feedbackmechanismen sowie Sicherheitsvorkehrungen hinzukommen, wird dies den Nutzern von Agenten helfen, Vertrauen bei der Nutzung der Agententechnologie zu verbessern.
3. Entwickler von intelligenten Agenten sollten geeignete Mittel zur Verfügung stellen, durch die die Privatsphäre der Nutzer geschützt und die Kontrolle der Betroffenen über die Nutzung ihrer personenbezogenen Daten aufrechterhalten werden kann.
4. Technische Maßnahmen sowie Privacy Enhancing Technologies (PET) werden in Verbindung mit den Software-Agenten empfohlen. Die folgenden Maßnahmen werden vorgeschlagen:
   - Entwicklung einer Trusted-Third-Party-Struktur für die Verifizierung und Authentifizierung aller Agenten
   - Zugangskontrollmechanismen
   - Werkzeuge, die dem Nutzer die Kontrolle über die Aktionen von Agenten Dritter Teilnehmer verschaffen, die personenbezogene Daten sammeln
   - Mechanismen, die aufgezeichneten Aktivitäten nachzuvollziehen
   - Integritätsmechanismen, um die Integrität der gespeicherten oder ausgetauschten Daten sicherzustellen und die Integrität der Arbeitsmethoden der Agenten oder der zertifizierten Komponenten wie digitale Signaturen zu kontrollieren.

Diese Maßnahmen müssen in die Agenten integriert werden. Die Maßnahmen können auch genutzt werden, um eine Infrastruktur vertrauenswürdiger Komponenten aufzubauen.

5. Anhand einer Checkliste für datenschutzfreundliche Designkriterien sollten die Entwickler, Lieferanten oder Provider eines Agenten den Agenten oder die Umgebung des Agenten mit geeigneten Privacy Enhancing Technologies ausrüsten. Rahmenbedingungen für die Zertifizierung der Datenschutzfreundlichkeit von Software-Agenten sind notwendig.

Gemeinsamer Standpunkt zur Sprechererkennung und Stimmerkennungstechnologien in der Telekommunikation

angenommen auf der 25. Sitzung der Arbeitsgruppe am 29. April 1999 in Norwegen

– Übersetzung –

Unter den gegenwärtig entwickelten biometrischen Identifikationsmethoden ist die Sprechererkennung wahrscheinlich die fortschrittlichste und von besonderer Relevanz für die Telekommunikation.

Sprechererkennung ist eine Methode, die Eigenschaften der Stimme einer Person zu analysieren, um

- die Stimme eines unbekannten Sprechers zu identifizieren;
- zu verifizieren, dass ein Sprecher derjenige ist, der er behauptet zu sein (Authentifikation);
- die Stimme einer Person in einer Umgebung mit vielen Sprechern zu erkennen.

In allen Fällen wird die Stimme einer Person gemessen und mit einem zuvor aufgenommenen und gespeicherten Muster oder Stimmabdruck der Stimme verglichen.

Die besten Ergebnisse beim Erkennen der Personen werden in Bezug auf die Fehlerraten erzielt, wenn die gleichen Wörter für die Eingabe und das Muster verwendet werden (text dependent systems). Zu denken ist an ein vorher festgelegtes Passwort oder eine Identifikationsnummer. Nach der Eingabe wird dieses mit dem gespeicherten Stimmabdruck verglichen.

In anderen Systemen werden die Sprecher veranlasst, zufällig ausgewählte Wörter zu wiederholen, die mit dem Muster verglichen werden (text prompted systems). Der Vorteil ist hier, dass das System nicht fehlgeleitet werden kann durch Fälscher, die auf Band gespeicherte Stimmabdrücke missbrauchen.

In „text independent systems“ wird eine Person gebeten zu sprechen, und ihre Äußerungen werden mit den gespeicherten Mustern verglichen, die völlig verschiedene Wörter enthalten. Dies beinhaltet einen erheblich höheren Zufallsfaktor, und von daher ist der Vergleich schwieriger, besonders wenn Hintergrundgeräusche vorliegen oder Telefonleitungen mit hohem Geräuschpegel verwendet werden. Auf der anderen Seite ist das Potential hoch: In Verbindung mit einer großen Sammlung von Stimmmustern ermöglichen textunabhängige Systeme die Identifizierung vieler verschiedener Personen in verschiedenen Umgebungen.

Die Sprechererkennung kann genutzt werden für die Identifikation und Authentifikation sowohl für den Zugang zu Netzen und Anlagen als auch für den Zugang zu

Diensten, die über das Netz verbreitet werden. Offensichtlich haben Telekombetreiber ein Interesse an verbesserter Stimmidentifizierung und Authentifizierung zu verschiedenen Zwecken, z. B. Abrechnungsbetrug zu bekämpfen oder neue Funktionen und Dienste zu vermarkten. Was Dienste betrifft, die über Telekommunikationsdienste verbreitet werden, wird die Identifikation von Kunden zunehmend als wesentlich für Online-Entscheidungen betrachtet, bei denen ein Individuum beteiligt ist. Es muss bemerkt werden, dass anders als die meisten anderen biometrischen Identifikationsmethoden die Sprechererkennung keine neue Infrastruktur erfordert, sie kann vielmehr in die bestehenden Telekommunikationsnetze integriert werden.

Die Nutzung der Sprechererkennung ist noch beschränkt auf bestimmte Anwendungen. Die Kosten dieser Technologie werden erwartungsgemäß allerdings schnell sinken, während die Qualität der Systeme wächst. In naher Zukunft können Massenanwendungen erwartet werden.

Die Datenschutzbeauftragten haben bei anderer Gelegenheit festgestellt, dass anonyme Methoden für den Zugang zu Telekommunikationsnetzen und anonyme Zahlungsmethoden zwei wesentliche Elemente echter Online-Anonymität sind.

Die Internationale Arbeitsgruppe ist besorgt über das Risiko, dass diese Techniken in der Telekommunikation eingesetzt und genutzt werden können, ohne Kenntnis der Nutzer und ohne Mittel, sie zu umgehen.

Empfehlungen

1. Die Einführung und Nutzung von Sprechererkennungstechnologien in Telekommunikationsnetzen sollte auf Umstände beschränkt werden, bei denen die Authentifikation wesentlich ist.
2. Da diese Identifikationsmethode unvermeidlich eine bestimmte Fehlerquote hat, sollte sie nicht eingeführt werden, ohne dass Schadensersatzansprüche zur Verfügung stehen.
3. Die informierte Einwilligung der Betroffenen sollte eingeholt werden, bevor Sprachanalysetechnologien angewandt werden. Grundsätzlich sollte diese Technologie auch mit deren Einwilligung nicht angewandt werden, um den geistigen oder emotionalen Zustand einer Person zu ermitteln.
4. Den Betroffenen sollte die Möglichkeit gegeben werden, anonym zu bleiben, wo dies angemessen ist.
5. Provider sollten die Betroffenen informieren, wenn ihre Stimmmuster in einer Datenbank gespeichert werden. Diese Information sollte auch klarstellen, unter welchen Umständen die Daten genutzt werden sollen.
6. Anbieter, in deren Auftrag eine Identifikation anhand einer Sprechererkennung stattfindet, sollten den Betroffenen über ihre Identität und den Zweck informieren, für den die Identifikation erforderlich ist.

D. Arbeitspapier der Datenschutzbeauftragten der Europäischen Union (Gruppe nach Art. 29 der Datenschutzrichtlinie der EU)

Empfehlung 1/99

Über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware

Von der Arbeitsgruppe am 23. Februar 1999 angenommen
(WP 17 – 5093/98 – DE endgültig)

DIE GRUPPE FÜR DEN SCHUTZ DER RECHTE VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.Oktober 1995,

gestützt auf Artikel 29 und 30 Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf die Artikel 12 und 14 Absatz 3,

EMPFIEHLT:

1. Die Gruppe fordert die Software- und Hardwareindustrie auf, Internetprodukte zu erarbeiten, die den Schutz der Privatsphäre gewährleisten und die zur Einhaltung der europäischen Datenschutzvorschriften notwendigen Mittel beinhalten.

   Eine Voraussetzung für die rechtmäßige Verarbeitung personenbezogener Daten ist die Unterrichtung des Betroffenen, damit er von der jeweiligen Verarbeitung Kenntnis hat. Daher ist die Gruppe insbesondere über alle Arten von Verarbeitungsvorgängen besorgt, die gegenwärtig über Software und Hardware im Internet ablaufen, ohne dass die Betroffenen hiervon Kenntnis haben, die für sie also „unsichtbar" sind.

   Typische Beispiele für eine solche unsichtbare Verarbeitung sind das „Chattering" auf HTTP-Ebene, automatische Hyperlinks zu Dritten, aktive Inhalte (wie Java, ActiveX oder andere nutzerorientierte Scripttechniken) sowie die Cookie-Merkmale, die zurzeit in den üblichen Browsern vorhanden sind.

2. Alle Internet-Software- und Hardwareprodukte sollten den Internetbenutzer darüber informieren, welche Daten sie sammeln, speichern und übertragen wollen und aus welchem Grund sie erforderlich sind.

   Ferner sollten Internet-Software- und Hardwareprodukte dem Datenbenutzer ermöglichen, später jederzeit problemlos Zugang zu den über ihn gesammelten Daten zu erhalten.

   Dies bedeutet beispielsweise:

   – bei einer Browser-Software, dass sie bei der Herstellung der Verbindung mit einem Webserver (Senden einer Anfrage oder Erhalt einer Webseite) den Benutzer darüber aufklärt, welche Informationen zu welchem Zweck übertragen werden sollen;

– bei von einer Webseite an den Benutzer gesendeten Hyperlinks, dass der Browser des Benutzers ihm diese – unabhängig von der Methode – alle anzeigt;

– bei Cookies, dass der Benutzer darüber unterrichtet wird, wenn die Internetsoftware ein Cookie empfangen, speichern oder senden will. Diese Mitteilung sollte in allgemein verständlicher Sprache erklären, welche Information zu welchem Zweck in diesem Cookie gespeichert werden soll und wie lange das Cookie gilt.

3. Die Konfiguration von Hardware- und Software-Produkten sollte keine Standardeinstellung beinhalten, die das Sammeln, Speichern oder Versenden der im Client vorgehaltenen Daten zulässt. Zum Beispiel:

   – Die Browsersoftware sollte standardmäßig so konfiguriert sein, dass nur die unbedingt zur Herstellung der Internetverbindung erforderlichen Informationen verarbeitet werden. Cookies sollten nie standardmäßig gespeichert oder gesendet werden.

   – Bei der Installation eines Browsers sollte dessen Funktion für die Speicherung und den Versand der Daten über die Identität oder das Kommunikationsverhalten des Benutzers (Profil) nicht automatisch mit derartigen, zuvor schon im Rechner des Benutzers abgespeicherten Daten versorgt werden.

4. Internet-Hardware- und Softwareprodukte müssen dem Betroffenen die freie Entscheidung über die Verarbeitung seiner personenbezogenen Daten ermöglichen und zwar mit benutzerfreundlichen Tools zur Selektion (d. h. Ablehnung oder Änderung) für den Empfang, die Speicherung bzw. den Versand client-persistenter Informationen anhand bestimmter Kriterien (u. a. Profile, Bereich oder Identität des Internetservers, Art und Dauer der gesammelten, gespeicherten bzw. versandten Informationen usw.). Der Benutzer sollte klare Anweisungen über die Verwendung von Soft- und Hardware zur Implementierung dieser Optionen und Tools erhalten. Zum Beispiel:

5. Die Browser-Software sollte dem Benutzer Konfigurationsoptionen bieten, damit er vorgeben kann, welche Daten sie sammeln und übertragen soll oder nicht.

6. Im Falle der Cookies bedeutet dies, dass der Benutzer immer die Option haben muss, das Senden oder Speichern eines Cookies insgesamt zuzulassen oder abzulehnen. Ferner sollte er entscheiden können, welche Informationsbestandteile eines Cookies beibehalten oder entfernt werden sollen, z. B. je nach der Gültigkeitsdauer des Cookies oder der sendenden oder empfangenden Webseiten.

7. Internet-Software- und Hardwareprodukte sollten es den Benutzern ermöglichen, client-persistente Informationen einfach und ohne Beteiligung des Senders zu entfernen. Der Benutzer sollte klare Anweisungen darüber erhalten, wie dies zu tun ist. Falls die Information nicht entfernt werden kann, muss zuverlässig sichergestellt werden, dass sie nicht übertragen und gelesen wird.

   – Cookies und andere client-persistente Informationen sollten entsprechend eines bestimmten Standards im Client-Computer gespeichert werden und leicht und selektiv zu löschen sein.

HINTERGRUND

Momentan ist es unmöglich, das Internet zu verwenden, ohne ständig auf Funktionalitäten zu stoßen, die die Privatsphäre verletzen und, für den Betroffenen unsichtbar, alle möglichen Verarbeitungsprozesse personenbezogener Daten vornehmen. Mit anderen Worten, der Internet-Benutzer weiß nichts davon, dass seine personenbezogenen Daten gesammelt und weiterverarbeitet wurden und für ihm unbekannte Zwecke genutzt werden könnten. Der Betroffene hat keine Kenntnis von dieser Verarbeitung und keine diesbezügliche Entscheidungsfreiheit.

Ein Beispiel für diese Technik ist das so genannte Cookie, das man definieren könnte als einen Computer-Informationseintrag, der von einem Webserver an den Computer des Benutzers gesandt wird, um ihn bei späteren Besuchen auf der gleichen Webseite wieder identifizieren zu können.

Browser sind Softwareprogramme, die u. a. dafür geschrieben wurden, das im Internet vorhandene Material graphisch anzuzeigen. Ein Browser kommuniziert zwischen dem Computer des Benutzers (Client) und dem entfernten Computer, auf dem die Informationen gespeichert sind (Webserver). Häufig senden die Browser mehr Informationen an den Webserver als zur Herstellung der Kommunikation eigentlich erforderlich ist. Die klassischen Browser teilen dem angewählten Webserver automatisch die Art und Sprache des anwählenden Browsers mit, die Bezeichnungen weiterer auf dem Benutzer-PC installierter Softwareprogramme und Betriebssysteme, die Seite, von der der Verweis kommt, Cookies usw. Solche Daten können von der Browser-Software auch unbemerkt systematisch an Dritte übertragen werden.

Mit diesen Techniken lassen sich so genannte Clicktrails über den Internet-Benutzer anlegen. Clicktrails beinhalten Informationen über das Verhalten einer Person, deren Identität, Suchweg oder Auswahlverhalten beim Besuch der Webseite. Sie enthalten die Links, die der Benutzer aufgerufen hat und die auf dem Webserver protokolliert sind.

Die europäischen Datenschutz-Richtlinien 95/46/EG und 97/66/EG enthalten detaillierte Bestimmungen für den Schutz der Rechte von Personen hinsichtlich ihrer personenbezogenen Daten. Beide Richtlinien sind für die in dieser Empfehlung behandelten Belange von Bedeutung, da es hier um die Verarbeitung der personenbezogenen Daten der Internet-Benutzer geht. Cookies oder Browser können Daten enthalten oder weiterverarbeiten, die eine direkte oder indirekte Identifizierung des einzelnen Internet-Benutzers ermöglichen.

Die Anwendung der Bestimmungen über faire Verarbeitung, rechtmäßige Gründe für die Verarbeitung und das Recht des Betroffenen, über die Verarbeitung seiner eigenen Daten zu bestimmen, führten zur vorstehenden Empfehlung.

Besondere Sorge bereiten der Gruppe die Risiken, die die Verarbeitung personenbezogener Daten von Personen in sich birgt, die hiervon keinerlei Kenntnis haben. Die Software- und Hardwareentwickler sind daher aufgerufen, die Grundsätze dieser Richtlinien zu berücksichtigen und zu respektieren, um die Privatsphäre der Internet-Benutzer angemessen zu schützen.

Brüssel, 23. Februar 1999

Für die Gruppe

Der Vorsitzende

Peter HUSTINX