

2. Telekommunikation

2.1 Neue Telekommunikationsanlage für Bremen

Für die bremische Verwaltung soll im Jahr 2004 mit der Installation einer neuen TK-Anlage begonnen werden. Dazu wurde frühzeitig vom Referat 36 des Senators für Finanzen (SfF) eine dienststellenübergreifende „Arbeitsgruppe Telekommunikation“ („ATK“) einberufen, um die Anforderungen an die neu zu beschaffende TK-Anlage zu definieren. Von Anfang an war neben dem Gesamtpersonalrat (GPR) auch meine Dienststelle an der Arbeit in dieser Arbeitsgruppe beteiligt.

Moderne Telefonanlagen bieten neben den vielen verschiedenen Möglichkeiten der Kommunikationsunterstützung auch zahlreiche Möglichkeiten, die über sie transportierten Kommunikationsflüsse zu steuern und auch auszuwerten. Die Auswertungen können dabei nicht nur global geführt werden, sondern bis herunter auf einzelne Arbeitsplätze und somit auch auf einzelne Mitarbeiter. Aufgrund dieser komplexen Auswertungs- und Kontrollmöglichkeiten ist es wichtig, die datenschutzrechtlichen Anforderungen zu beachten. Während für Personen, die telefonisch in Kontakt mit der Bremer Verwaltung treten, vornehmlich die Bestimmungen des Telekommunikationsgesetzes einschlägig sind, sind bezüglich der Arbeitnehmer in der Bremer Verwaltung auch für den Arbeitnehmerdatenschutz relevante Regelungen zu beachten. Innerhalb der Bremer Verwaltung gilt derzeit die mit dem GPR abgestimmte „Dienstvereinbarung über den Betrieb und die Nutzung von Telekommunikationsanlagen (Fernsprechanlagen)“ vom 07. Juni 1991, die die Belange der Telefonie in der öffentlichen Verwaltung in Bremen regelt. Zuständig für den Bereich der Sprachtelefonie ist der Senator für Finanzen, Referat 36. Es besteht unter den Beteiligten Einigkeit, dass die bestehende Dienstvereinbarung nicht mehr den modernen Anforderungen an ein Regelwerk für Sprachtelefonie genügt und sie zu überarbeiten ist. In ersten informellen Gesprächen, denen ein von der Arbeitsgruppe „ATK“ in Zusammenarbeit mit externen Dienstleistern erarbeiteter Anforderungskatalog an die zukünftige TK-Anlage zugrunde lag, habe ich bereits den SfF über die Anforderungen, z. B. an ein verwaltungsweites elektronisches Telefonbuch, an die Protokollierung von dienstlichen und privaten Telefonaten zu Abrechnungszwecken und die damit verbundene notwendige Anpassung der bestehenden Dienstvereinbarung informiert. Die wesentlichen Entwicklungen werden aber erst 2004 anstehen.

2.2 Gefahren von Funknetzen

Die 1996 von Bob Allen (damals CEO von AT&T) geäußerte Vision „Anytime, Anywhere“ zu kommunizieren und Zugriff auf benötigte Informationen zu erhalten, ist mittlerweile Realität geworden. Die mobilen Kommunikationsmöglichkeiten gehen dabei weit über das simple Telefonieren hinaus. Mobiles E-Mailing und andere komplexe Dienste sind problemlos nutzbar geworden.

Notwendige Basis für alle mobilen Dienste ist eine Vernetzung der mobilen Kommunikationsgeräte. Dafür existieren neben den Mobilfunknetzen zunehmend andere Technologien. Für die Kommunikation über kurze Distanzen mit Peripheriegeräten, z. B. Bluetooth, und für die drahtlose Vernetzung von Computern untereinander die WLAN-Technik. Gerade die WLAN-Technik wird sehr gern genutzt, wenn es darum geht, „mal eben schnell“ Rechner zu verbinden, um Daten auszutauschen, oder kostengünstig neue DV-Arbeitsplätze in alten Gebäuden zu schaffen, in denen keine ausreichende Verkabelung vorhanden ist. Denkmalschützer sind froh über solche Technik, aber aus Sicht des Datenschutzes bereitet sie doch einige Kopfschmerzen. Denn gerade die einfache und flexible Möglichkeit einer schnellen Verbindung von mehreren Rechnern bringt auch viele Gefahren für die in den Rechnern gespeicherten und zwischen diesen Computern übertragenen Daten mit sich. So sind Funknetze räumlich nicht auf Gebäude begrenzt, sie sind ein offenes Medium. Außerhalb von Gebäuden, in denen Funknetze installiert werden, sind deren Funkwolken zu orten und die übertragenen Daten aufzufangen. Wenn nicht entsprechende Vorkehrungen getroffen werden, kann man sich darüber hinaus nicht sicher sein, dass nur autorisierte Teilnehmer im Funknetz sind und somit Zugriff auf die entsprechenden Daten und Anwendungen haben. Diese Gefahren werden oft bei Funknetz-Installationen vernachlässigt. Oft wird auch vergessen, dass durch eine unbedachte Anbindung von Rechnern via Funk an bestehende, drahtgebundene Unternehmensnetzwerke schwach oder gar nicht gesicherte Hintertüren in eben diesen Unternehmensnetzwerken geöffnet werden: Die Absicherung der Netzwerke gegen das Internet wird gelegentlich, z. B. mittels teurer Firewall-Lösungen, realisiert, aber das Funknetz ist „offen wie ein Scheunentor“.

Ich arbeite im Rahmen des „Arbeitskreises Technik“ an einer Orientierungshilfe „Datenschutz in drahtlosen Netzen“ mit, die Mitte 2004 veröffentlicht werden soll. Neben der Beschreibung allgemeiner Gefahren von Funknetzen soll darin auf die Themen WLAN, Bluetooth, Infrarot-Kommunikation, Funkmäuse und Funktastaturen sowie Personal Digital Assistant (PDA) eingegangen werden.

2.3 Orientierungshilfe Kryptografie

Das Bundesdatenschutzgesetz (BDSG) und auch alle Landesdatenschutzgesetze schreiben verschiedene technische und organisatorische Maßnahmen vor, die von den verantwortlichen Stellen zu treffen sind. Im Bremischen Datenschutzgesetz (BremDSG) sind diese Regelungen in § 7 „Datenvermeidung, Vorabkontrolle, technische und organisatorische Maßnahmen“ festgeschrieben. Neben anderen Punkten wird hier die Kontrolle des Zugriffs (Zugriffskontrolle, BremDSG § 7 Satz 4 Nr. 3) und der Weitergabe (Weitergabekontrolle, BremDSG § 7 Satz 4 Nr. 4) personenbezogener Daten verlangt. Diese Anforderungen können mit dem Hilfsmittel der Kryptografie erfüllt werden. Kryptografie ist die Wissenschaft, die sich damit befasst, wie Daten vor den Augen unbefugter Dritter verborgen werden. So können mit ihrer Hilfe Daten auf Datenträgern verschlüsselt werden ebenso wie Daten, die von einem Punkt zu einem anderen übertragen werden müssen, auf der Strecke verschlüsselt werden können. Dabei sind, je nach Sensibilität der Daten, geeignete Ver- und Entschlüsselungsverfahren zu wählen, damit gewährleistet ist, dass Unbefugte keinen Zugriff auf die Daten erhalten können oder um sicherzustellen, dass Daten wirklich von einem bestimmten Absender kommen und dass sie zwischen Versand und Empfang nicht verfälscht worden sind. Da es im Bereich der Verschlüsselung sehr viele verschiedene geeignete und weniger geeignete Methoden gibt, hat der „Arbeitskreis Technik“ (AK Technik) der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe erarbeitet. Neben der Beschreibung der technischen Grundlagen und ihrer Bedeutungen bzw. Auswirkungen (Algorithmen, Schlüssellängen im Zusammenhang mit symmetrischen und asymmetrischen Verschlüsselungsverfahren, Angreifbarkeit der Verschlüsselung durch Wahl „schlechter“ Methoden oder fehlerhaft implementierter Algorithmen, etc.) ist es notwendig zuerst eine Kategorisierung der Daten vorzunehmen, die einer besonders gesicherten Behandlung bedürfen, also höchst sensibel sind. Es sind dies Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualeben, Dienst- und Arbeitsverhältnisse sowie steuerliche und soziale Verhältnisse (vgl. § 3g BDSG, § 2b BremDSG). Damit ist der Rahmen für den höchsten Schutzbedarf abgesteckt, der den Einsatz kryptografischer Methoden erfordert. In der von den Datenschutzbeauftragten erarbeiteten Broschüre werden Grundszenarien (Zugriffskontrolle, Weitergabekontrolle) dabei ebenso diskutiert wie allgemeine Lösungsansätze, wie z. B. das Tunneln unsicherer Netze oder der Einsatz digitaler Signaturen. Zum Schluss der Orientierungshilfe wird auf in verschiedenen Szenarien auftretende IT-Sicherheitsprobleme und mögliche Lösungswege unter Anwendung kryptografischer Verfahren, sowohl bezogen auf die eingesetzten bzw. einzusetzenden Infrastrukturen (z. B. Internet, Virtual Private Networks) als auch bestimmte Anwendungsfälle eingegangen. Die Orientierungshilfe kann von meiner Internetseite unter www.datenschutz.bremen.de heruntergeladen werden.

2.4 Erhebliche datenschutzrechtliche Defizite bei der Novellierung des Telekommunikationsgesetzes

Am 15. Oktober 2003 wurde von der Bundesregierung ein Entwurf für ein neues Telekommunikationsgesetz (TKG) beschlossen. Dieser Entwurf beinhaltet wesentliche Verschlechterungen für den Datenschutz:

Der Gesetzesentwurf berechtigt die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (Angaben, die beim Aufbau und bei der Abwicklung von Telekommunikationsverbindungen anfallen, also etwa eine angerufene Telefonnummer oder den Zeitpunkt des Anrufs) ungekürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern, wobei auch alle Zielrufnummern enthalten sind. Der Innenausschuss des Bundesrates geht noch einen Schritt weiter in seinen Forderungen. Er will aus Gründen der inneren Sicherheit sogar eine zwölfmonatige Speicherungsfrist vorsehen. Ich habe zu diesen Bestrebungen schon in meiner Pressemitteilung vom 21. November 2003 erklärt: „Das Recht, mit seiner Umwelt unbeobachtet und frei zu kommunizieren, gehört zu den entscheidenden Grundrechten in der Informationsgesellschaft. Eine umfassende Speicherung von Verkehrsdaten auf Vorrat ist damit unvereinbar“.

Weiterhin sollen sich in Zukunft die Käufer auch beim Erwerb eines vertragslosen Prepaid-Handys ausweisen und registrieren lassen. Schon seit längerem kritisieren die Datenschutzbeauftragten eine Zwangsidentifizierung beim Erwerb von Prepaid-Handys als gesetzeswidrig. Durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 2302) sehen sich die Datenschutzbeauftragten nunmehr in dieser Auffassung bestätigt. In diesem Urteil betont das Gericht, dass eine Pflicht eines Prepaid-Anbieters, personenbezogene Kundendaten zu erheben, einen staatlichen Eingriff in das verfassungsrechtlich gewährleistete Recht der Kunden auf informationelle Selbstbestimmung darstellt, der nicht erforderlich ist.

Schließlich können nach der Novellierung des TKG die Strafverfolgungsbehörden und die Nachrichtendienste bei der Verfolgung jedweder Strafdaten ohne richterliche Anordnung von den Diensteanbietern Passwörter und Geheimzahlen anfordern, mit denen die Inhalte oder näheren Umstände einer Telekommunikation geschützt werden.

Aufgrund der erheblichen verfassungsrechtlichen Bedenken hinsichtlich dieser gesetzgeberischen Vorhaben hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Frühjahr die EntschlieÙung „Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation“ (Ziff. 18.8 dieses Berichts) und im Herbst die EntschlieÙung „Gravierende Verschlechterung des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes“ (Ziff. 18.14 dieses Berichts) gefasst. Hierin habe ich mit den anderen Datenschutzbeauftragten gefordert, die datenschutzrechtlichen Defizite zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

2.5 Wissenschaftliche Untersuchung der Telefonüberwachung

Im Mai dieses Jahres hat das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg ein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten zur „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach §§ 100a, 100b der Strafprozessordnung (StPO) und anderer verdeckter Ermittlungsmaßnahmen“ vorgelegt. Es handelt sich bei diesem Projekt um eine Studie, die aus einer empirischen Perspektive Fragestellungen des strafprozessualen Instruments der Überwachung der Telekommunikation aufgreift. Die Untersuchung basiert auf Strafaktenanalysen, schriftlichen Befragungen und Expertengesprächen mit Polizisten, Staatsanwälten und Richtern. Da durch die Aktenanalyse aber auch in den Befragungen und Gesprächen personenbezogene Daten erhoben und verarbeitet wurden, war für das Forschungsvorhaben ein abgestimmtes Datenschutzkonzept unerlässlich. Dieses Datenschutzkonzept enthält u. a. Festlegungen zu den Fragen des Zugangs von Mitarbeitern, Mitarbeiterverpflichtungen, der Anonymisierung, der Aktenentnahme zur Bearbeitung und zu Kopierbeschränkungen.

Das Gutachten des Max-Planck-Institutes dokumentiert, dass die Zahl der Ermittlungsverfahren, in denen Telekommunikationsüberwachungen angeordnet wurden, sich in dem Zeitraum von 1996 bis 2001 um 80 % erhöht hat. Auch die Anzahl der staatsanwaltschaftlichen Eilanordnungen (welche anstelle des Richtervorbehaltes nur als absolute Ausnahme vorgesehen sind) ist deutlich angestiegen. Weiterhin werden erhebliche Defizite in der Praxis aufgezeigt. Als ein großes Manko der Telekommunikationsüberwachung wird in dem Gutachten die Umsetzung des Richtervorbehaltes im Zusammenhang mit der damit verbundenen Begründungsanforderung beschrieben. Lediglich 24 % der Beschlüsse waren substantiell begründet. Das führt zu einem Mangel an Transparenz, Nachvollziehbarkeit und Kontrolle. Aus diesem Grund wird in dem Gutachten auch eine Verbesserung der richterlichen Kontrolle gefordert. Daneben wird die Einrichtung externer Kontrollsysteme und der Ausbau der Rechtsschutzmöglichkeiten vorgeschlagen. Weiterhin wird festgestellt, dass in den wenigsten Fällen die Anschlussinhaber über die Maßnahme benachrichtigt wurden. Nach § 101 StPO sind die Beteiligten von der getroffenen Maßnahme des § 100a StPO jedoch zu unterrichten. Zu teilweise vergleichbaren Ergebnissen kommt auch ein Forschungsprojekt der Universität Bielefeld.

Angesichts des gravierenden Eingriffes in das Telekommunikationsgeheimnis durch die Telekommunikationsüberwachung können derartige Defizite nicht einfach hingenommen werden. Die 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Konsequenzen aus der Untersuchung des Max-Planck-Institutes in eine EntschlieÙung gefasst (Ziff. 18.13 dieses Berichts). Die Datenschutzbeauftragten machen darauf aufmerksam, dass die Telefonüberwachung im Ermittlungsverfahren ultima ratio bleiben muss. Ein Eingriff in das Recht auf unbeobachtete Kommunikation kann nur bei Verfolgung schwerwiegender Straftaten gerechtfertigt sein. Der gesetzliche Richtervorbehalt darf nicht gelockert werden. Vielmehr muss die Qualität der Entscheidung verbessert werden. Erhebliche Verstöße gegen das Begründungserfordernis können nicht ungeahndet bleiben, sondern müssen ein Beweisverwertungsverbot nach sich ziehen. Die Strafverfolgungsbehörden sollten durch Berichtspflichten dazu angehalten werden, ihren gesetzlich festgeschriebenen Pflichten, wie z.B. der Benachrichtigungspflicht, nachzukommen.

Weiterhin hat die 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2003 eine Entschließung zur Transparenz der Telefonüberwachung gefasst (Ziff. 18.6 dieses Berichts). Hierin hat sie die Beibehaltung der Jahresstatistik über zu Strafverfolgungszwecken durchgeführte Überwachungsmaßnahmen, die von den Betreibern der Telekommunikationsanlagen zu führen ist, gefordert. Die Jahresstatistik dient der Information der Allgemeinheit über Ausmaß und Entwicklung der Telekommunikation. Nur so kann die Transparenz der Überwachungsmaßnahmen ermöglicht werden. In dem Entwurf des Telekommunikationsgesetzes hat dieses Anliegen Berücksichtigung gefunden.

2.6 Gesetz zur Bekämpfung des Missbrauchs von 0190er-/0900er- Nummern in Kraft

Immer wieder werde ich von Bürgern mit Fragen zum Missbrauch von 0190er- und 0900er-Nummern konfrontiert. Auch der Datenschutzausschuss der 15. Legislaturperiode hat sich mit diesem Thema beschäftigt und mich aufgefordert, dieses Thema weiterhin zu verfolgen. Deshalb berichte ich an dieser Stelle über den Fortgang.

Das Gesetz gegen den Missbrauch von 0190er-/0900er-Nummern ist am 15. August 2003 in Kraft getreten (BGBl. I 2003, S. 1590 f). Durch das Gesetz soll insbesondere vor Dialern geschützt werden, die in der Vergangenheit erheblichen Missbrauch erzeugt haben. Dialer sind kleine Anwahlprogramme, die einen Rechner über eine bestimmte Telefonnummer mit einem Internetserver verbinden. Das Heimtückische hieran: Viele der Dialer installieren sich unbemerkt und bauen eine Standardverbindung ins Internet auf. Dabei nutzen sie regelmäßig eine teure 0190er- oder 0900er-Nummer, was sich meist erst mit der nächsten Telefonrechnung beim Betroffenen schmerzlich bemerkbar macht. Diesem Missbrauch soll durch das neue Gesetz nun ein Riegel vorgeschoben werden: Entgelte, die für 0190er- und 0900er-Nummern erhoben werden dürfen, sind mit 30 € pro Einwahl und 2 € pro Minute begrenzt. 0190er- und 0900er-Verbindungen müssen nach spätestens einer Stunde automatisch getrennt werden (es sei denn, es wurde ausdrücklich ein längerer Zeitraum vereinbart). Außerdem dürfen Dialer nur eingesetzt werden, wenn diese vor Inbetriebnahme bei der Regulierungsbehörde für Telekommunikation und Post registriert worden sind. Die Registrierung erfolgt, wenn das Anwahlprogramm bestimmte Mindestvoraussetzungen erfüllt und der Registrierungsverpflichtete schriftlich versichert, dass eine rechtswidrige Nutzung ausgeschlossen ist. Nicht registrierte oder die Mindestanforderungen nicht erfüllende Dialer dürfen nicht mehr eingesetzt werden. Die Regulierungsbehörde hat eine Datenbank zu den registrierten Dialern ins Internet gestellt, um dem Verbraucher eine Prüfungsmöglichkeit zu geben, ob der Dialer auch tatsächlich registriert ist. Ein nicht registrierter Dialer ist rechtswidrig und es erwächst damit für den Nutzer keine Zahlungspflicht. Zudem können rechtswidrig genutzte 0190er- und 0900er-Nummern von der Regulierungsbehörde entzogen und Geldbußen von bis zu 100.000 € verhängt werden.

Darüber hinaus kann man sich durch Software gegen Dialer schützen. Es besteht auch die Möglichkeit eine 0190er/0900er-Anschlussperre bei seinem Anbieter einrichten zu lassen, bei der sämtliche dieser Rufnummern gesperrt werden.