

1. Vorwort

1.1 Von den alten Ägyptern lernen

„Oh, ihr Lebenden! Ein Weiser ist der, der sich anhört, was die Vorfahren gesagt haben!“ Mit dieser Inschrift wandte sich vor Jahrtausenden der hohe ägyptische Beamte Rech-mi-Re an jene, die in Theben sein Grab besuchten. Diese Worte möchte man in Abwandlung auf das erst vor fast 25 Jahren verkündete Volkszählungsurteil des Bundesverfassungsgerichts an den Bundesinnenminister Schäuble richten. In das Urteil ist das Recht auf informationelle Selbstbestimmung „gemeißelt“. In der westlichen Welt kamen Zeiten, in denen die Besucher des Grabes die Inschrift nicht mehr lesen konnten. Das Wissen um die Bedeutung der Hieroglyphen war verloren gegangen. Es sollten fast 2000 Jahre verstreichen, bis die Inschrift wieder gelesen und verstanden werden konnte. Man kann nur hoffen, dass diese Leseschwäche nicht nur im Amte des Bundesinnenministers, sondern auch in anderen Bereichen der Politik in Bezug auf die verfassungsrechtlichen Grundsätze des Volkszählungsurteils schneller vorübergehen möge.

1.2 Mehr Respekt vor der Verfassung

In den letzten Jahren hat es in besonderem Maße eine ganze Reihe von Entscheidungen des Bundesverfassungsgerichts mit datenschutzrechtlicher Relevanz gegeben (vgl. Ziff. 9.9, 9.15 und 15.2 dieses Berichts). Die Gesetzgeber des Bundes und einiger Länder haben dabei oft erfahren müssen, dass sie das Recht auf informationelle Selbstbestimmung in ihren Gesetzen nicht ausreichend beachtet haben. Übrigens sind diese verfassungswidrigen Gesetze oft entgegen der Warnungen der Datenschutzbeauftragten des Bundes und der Länder verabschiedet worden. Dabei ist eine gewisse Erosion bei der Beachtung des Datenschutzes durch den Gesetzgeber festzustellen, denn viele der neu auf den Weg gebrachten gesetzlichen Regelungen mit Eingriffen in das informationelle Selbstbestimmungsrecht liegen nicht im verfassungsrechtlichen Rahmen. Bedauerlicherweise werden solche Gesetzentwürfe oft bei der Befassung im Bundesrat nicht kritisiert, vielmehr wird von hier mit Mehrheit versucht, die gesetzlichen Eingriffe noch zu verschärfen. Viele Bürgerinnen und Bürger, die sich mit einem Anliegen an mich wenden, fragen häufig vorab resignierend, ob ich denn in ihrer Angelegenheit überhaupt noch etwas tun könne. Ein Bürger brachte es mit den Worten auf den Punkt: „Ich habe nichts zu verbergen, aber ich habe das Gefühl, ich kann auch nichts mehr verbergen“. Das Vertrauen der Bürgerinnen und Bürger, dass der Staat mit ihren Daten respektvoll umgeht, ist im Schwinden, wie sonst ist z. B. die Flut der Anfragen bei mir im letzten Jahr zu erklären, bis wann man noch einen Ausweis ohne darin gespeicherte Fingerabdruckdaten beantragen könne.

1.3 Überreaktionen der Innenpolitik des Bundes

Der scheidende Bundeswirtschaftsminister Clement soll auf die Frage, was er jetzt mache, seinerzeit geantwortet haben: „Ich werde meine Freiheit genießen, soweit es Otto Schily zulässt“.

Gerade auf dem Feld der Innenpolitik kommen die öffentlich gemachten Ideen, die mit verfassungsrechtlich bedenklichen Eingriffen verbunden sind, in immer kürzeren zeitlichen Intervallen.

Hatte schon der ehemalige Innenminister Schily erklärt, er habe mit seinen gesetzgeberischen Initiativen alles getan, um den Terrorismus in Deutschland zu verhindern, brachte Bundesinnenminister Schäuble es fertig, in nicht vorstellbarer Vielfalt die Ängste der Bürger vor Terrorismus und Kriminalität zu schüren. Ihm gelang es, europäische Gremien (vgl. Fluggastdatenabkommen mit den USA oder die Vorratsdatenspeicherung) wie auch die Mehrheit des Bundestages dazu zu bewegen, durch ein Klima der Verunsicherung alle Bundesbürger als potentielle Gefahrenquelle zu diskreditieren, der nur mit präventiven nachrichtendienstlichen und polizeilichen Mitteln permanenter Überwachung Einhalt geboten werden könne. Erneute massive Eingriffe in die Freiheitsrechte, insbesondere in das Recht auf informationelle Selbstbestimmung, waren die Folge.

Der frühere Bundesinnenminister Baum formulierte es so: "Wir sind auf einer Rutschbahn, in der ständig auf eine Ausnahmesituation mit AusnahmeGesetzen reagiert wird. Zur Logik des Sicherheitsstaates gehört die Maßlosigkeit".

Erschreckend ist, wie dabei oft die Öffentlichkeit für dumm verkauft wird. Viele der vorgeschlagenen Maßnahmen sind gegen gut organisierte Terroristen wirkungslos. Sie treffen aber ins Herz einer freien Gesellschaft. Der Staat mischt sich immer mehr in alle Lebensbereiche seiner Bürger ein. Es gibt trotzdem keine absolute Sicherheit. Nehmen wir z. B. die Pässe, die nunmehr sicherheitstechnisch hochgerüstet sind mit elektronisch gespeicherten, biometrischen Gesichtserkennungs- und Fingerabdruckdaten. Die neuen Pässe wurden eingeführt, um den Identitätsmissbrauch zu verhindern, ein Phänomen, das es nach der frühen Einführung der fälschungssicheren Ausweise als Problemfeld nachweisbar nicht gab. In Wahrheit wird die Möglichkeit eines Identitätsdiebstahls aber erhöht, weil erst durch den neuen Pass biometrische Merkmale wie das Bild eines Passinhabers mit hoher Qualität weltweit verfügbar gemacht werden. Erst jüngst zeigte die Sendung „Panorama“ wie einfach es ist, in Mitgliedsstaaten der EU für Bürger aus anderen Ländern (Drittstaaten) EU-Pässe zu besorgen. Sie zeigte z. B. eine Agentur in St. Petersburg, deren Geschäftsfeld es ist, für Fremde Original-EU-Pässe zu beschaffen. Dafür haben wir jetzt Pässe, die – ist der Code erst mal geknackt - es ermöglichen, unsere Fingerabdrücke an jedem beliebigen Ort der Erde zu reproduzieren. Gerade im Ausland muss der Pass häufig auch aus der Hand gegeben werden, in vielen Hotels z. B. über Nacht, so dass die biometrischen Merkmale ausgelesen und für andere Zwecke verwendet werden können. Und welche Sicherheit ist gewonnen, wenn sich allein in Deutschland mehrere hunderttausend Personen illegal aufhalten? Nein, viele beschleicht der Verdacht, hier soll ein anderer Staat vorbereitet werden.

Ein weiteres erschreckendes Beispiel ist die Vorratsdatenspeicherung, ein System, das nicht einmal die sicherheitsfanatischen USA praktizieren. Die rechtliche Einschätzung der in 2007 eingeführten Regelungen zur Vorratsdatenspeicherung sind unter Ziff. 4.1 und 21.4 dieses Berichts zu finden. Vor der Abstimmung zur Vorratsdatenspeicherung im Bundestag habe ich mit einem Schreiben an die Bremer Bundestagsabgeordneten versucht, diese dazu zu bewegen, dem Gesetz ihre Zustimmung zu verweigern. Meine wesentlichen Argumente sind auch in meiner Pressemitteilung vom 8. November 2007 enthalten, die Sie auf meiner Homepage finden (www.datenschutz-bremen.de/pressemitteilung.php?pressid=8595).

Das Unbegreifliche an der ganzen Entwicklung ist, dass alle Maßnahmen, von denen jetzt die Bevölkerung in Gänze getroffen wird, mit dem Argument „Terrorismusbekämpfung“ eingeführt, schon in naher Zukunft ganz anderen Zwecken dienen können. Das Rad, gespeicherte Daten für weitere neue Zwecke zu nutzen, wird immer ein Stück weiter gedreht. Schon jetzt wurde z. B. bei der Debatte um die Einführung der Vorratsdatenspeicherung deutlich, dass politische Kräfte sich dieser Daten gern bemächtigt hätten, um die Daten für die Verfolgung von Raubkopien der Musikindustrie zur Verfügung zu stellen. Das Gleiche erleben wir bei anderen jüngst geschaffenen technischen Infrastrukturen, die die Totalüberwachung eines Alltagsbereichs unserer Bürger zulassen. Auch mit der in Mautbrücken eingebauten Technik kann man mehr, nämlich die Beobachtung des gesamten Verkehrs auf den Bundesautobahnen, auch hier gibt es politische Bestrebungen, die Zweckbindung der Daten für die Abrechnung der Autobahngebühr aufzuweichen.

Zum Glück war bei vielen dieser Entwicklungen bisher das Bundesverfassungsgericht Bewahrer der Verfassung und leider nicht der Bundestag. Aber auch diese Entscheidungen können natürlich nicht das ganze Ausmaß der technischen Ausforschung des privaten Lebens durch öffentliche und staatliche Stellen mit den daraus resultierenden Folgen verhindern. Der Staat ist mittlerweile in der Informationsgesellschaft angekommen, aber er muss noch lernen, dass man mit dem Brotmesser nur Brot schneidet.

1.4 Kurangebot „Überwachungsfreie Ruheräume“

Aber auch einzelne Geschäftsbereiche der Wirtschaft rüsten auf. Mir gegenüber wird häufig Klage geführt über eine permanente „Bombardierung“ des Einzelnen durch technische Geräte, denen der Mensch sich immer mehr wehrlos ausgesetzt fühlt. So nimmt z. B. die Flut von Spam-Mails, unerwünschten SMS oder unnötigen Anrufen von Sprachcomputern laufend zu. Die gesellschaftlich erwartete oder vom Arbeitgeber verlangte ständige Erreichbarkeit wird zu nicht gewünschten wirtschaftlichen oder gelegentlich sogar kriminellen Aktivitäten von „Trittbrettfahrern“ mitgenutzt. Eine Vielzahl weiterer neuer Möglichkeiten tut sich durch in Handys integrierte Navigationssysteme und insbesondere die Funkchiptechnologie (RFID) auf. Alles in allem befürchte ich, nicht lange nach der Debatte über rauchfreie Zonen wird es eine Debatte über die Notwendigkeit zur Schaffung überwachungsfreier Räume geben.

1.5 Das Bankgeheimnis und die Metapher vom Schweizer Käse

Gesetzliche Regelungen, die den unmittelbaren elektronischen Zugriff auf Datensysteme der privaten Wirtschaft erlauben, nehmen zu. Eine Entwicklung, die übrigens zeigt, wie sinnvoll es ist, Datenschutzkontrolle – wie in Bremen von Anbeginn - in eine Hand zu geben. Auch bestärkt es mich in meiner seit Jahren geäußerten Auffassung, dass Regelungen für den rechtlich zulässigen Abgleich von Daten verschiedener verantwortlicher Stellen in einem „Black-Box-Verfahren“ eine Grundregelung im allgemeinen Datenschutzrecht haben sollten. Exemplarisch für diese eingangs genannte Entwicklung steht das Kontoabrufverfahren nach § 24 c Kreditwesengesetz (KWG) und §§ 93, 93 b Abgabenordnung (AO).

Die Zahl der Kontenabfragen öffentlicher Stellen stieg laut Presseberichten im Jahr 2007 bundesweit auf fast 100.000. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) stellte danach im vergangenen Jahr einen Anstieg um 15 Prozent im Vergleich zu 2006 fest. In insgesamt 93.560 Fällen sollen Behörden die Kontostammdaten abgefragt haben. Hinter dieser Zahl stehen insgesamt rund 200 Millionen Zugriffe auf Datenbanken der Kreditinstitute, denn jede Einzelabfrage nach passenden Kontoverbindungen löst eine virtuelle Suche in den Systemen aller rund 2.000 Banken hierzulande aus.

Eine Steigerungsrate ähnlich stark wie bei der Telefonüberwachung, die nicht mit einer Mehrung von Kontoeröffnungen erklärt werden kann. Sie kann vielmehr mit der Einführung einer voll elektronischen Abfrage zusammenhängen. Ich habe diesen Bereich erstmalig vor zwei Jahren untersucht und die Ergebnisse öffentlich gemacht (vgl. 28. JB, Ziff. 15.1). Das war noch die Einführungsphase. Eine Untersuchung der Rechtmäßigkeit vermehrter Abrufe kann in Bremen allerdings erst nach einer Wiederbesetzung des zuständigen Referats 50 in meinem Hause erfolgen.

In den thematischen Zusammenhang gehört auch der Beschluss des Bundesverfassungsgerichts zum Kontenabrufverfahren, mit dem die Karlsruher Richter unterstrichen haben, dass die angegriffenen gesetzlichen Bestimmungen die Abfrage von Kontostammdaten der Bankkunden und sonstiger Verfügungsberechtigter nicht "routinemäßig" oder gar "ins Blaue hinein" erlauben. Vor diesem Hintergrund sind die Planungen des Bundesministeriums für Finanzen kritisch zu betrachten, die zeigen, wo die Entwicklung hingeht. Die täglichen elektronischen Abrufmöglichkeiten sollen von jetzt 100 auf bis zu 5.000 Abrufe erweitert werden.

Darüber hinaus hat das Bundesverfassungsgericht den Gesetzgeber verpflichtet, den § 93 der Abgabenordnung nachzubessern, weil in der beanstandeten gesetzlichen Regelung der Kreis der zum Datenabruf berechtigten Behörden außerhalb der Finanzverwaltung nicht präzise festgelegt ist. Zukünftige Aufgabe wird es sein, gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) die Einhaltung der Vorgaben, etwa der Benachrichtigung sowie der Regelung, dass die Zugriffe lückenlos zu protokollieren sind, zu kontrollieren.

1.6 Besondere Regelungen zum Arbeitnehmerdatenschutz fehlen weiter

Die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die elektronische Überwachung von Beschäftigten am Arbeitsplatz oder z. B. die Erhebung des Gesundheitszustandes und psychologische Testverfahren bei der Einstellung, erfordern einen besonderen Schutz des Betroffenen durch bundeseinheitliche gesetzliche Regelungen. Dies fordern die Datenschutzbeauftragten des Bundes und der Länder seit Jahren, erneut in einer Entschließung im März 2007 (vgl. Ziff. 21.5 dieses Berichts).

1.7 Aus dem dunklen Keller kommt das Kabel fürs Internet

Den Stand der Verbreitung von Internetanschlüssen in deutschen Haushalten gibt die Übersicht „Indikatoren der Informationsgesellschaft“ unter Ziff. 24.4 dieses Berichts wieder. Sie zeigt, dass

bereits mehr als die Hälfte der Deutschen sich mit den Problemen des Internets auseinandersetzen muss.

Früher begab man sich in den Wilden Westen, um Abenteuer zu erleben, heute kann man sich in ein Dschungel-Camp begeben, aber am interessantesten ist es immer noch im Internet. Die Risiken sind vielfältig, sie einzuschätzen, übersteigt die Vorstellungskraft und trotzdem, alle Welt tummelt sich dort, ob Otto-Normalverbraucher, Firmen oder Verwaltung, alle bewegen sich auf den unsicheren elektronischen Datenwegen. Ausgeklügelte Methoden beim Online-Banking leiten Überweisungen fehl, manche Menschen bedienen sich mit kriminellen Programmen gar selbst und buchen bei anderen mal rasch alles ab, was auf dem Konto ist, Viren-Attacken auf Computer, Spam-Mail, Mail-Angriffe, die Unternehmen für Tage lahm legen, heimliches Mitlesen oder das Ausspähen von Daten – um nur einige Erscheinungsformen zu nennen – schrecken die Nutzer zwar nicht ab, lassen sie aber oft nicht ruhig schlafen.

Einige Internet-Nutzer sind zu allem Überfluss dazu übergegangen gleich selbst ihre meist überschaubare kleine Idylle frei Haus in Bloggs, Bildern oder Videoclips zu liefern. Diese gelegentlich exhibitionistischen Darstellungen lassen mich aber keineswegs daran zweifeln, am Gedanken des Datenschutzes festzuhalten. Es ist nämlich etwas grundsätzlich Verschiedenes, ob sich jemand selbst in aller Öffentlichkeit auszieht oder ob dort jemand gegen seinen Willen entblößt wird.

Wir müssen uns nur von dem Gedanken verabschieden, dass das Internet ein sicheres Netz mit hohem Datenschutzstandard ist oder werden könnte. Dafür ist es überhaupt nicht konzipiert, es beginnt und endet eben oft in dunklen Kellern. Viele Surfer müssen feststellen, dass sie für all die bunten kostenlosen Internetangebote in Wahrheit oft mit ihren persönlichen Daten bezahlen müssen. Als Faustformel kann man empfehlen: „Mache nichts im Internet, was Du nicht auch vor allen Augen in der Öffentlichkeit tun würdest“.

Gleichwohl wollen viele Menschen sich nicht ungefragt mit einer Datenselbstbedienung Dritter abfinden. Eine aktive Netzgemeinde wehrt sich vielerorts gegen das allzu dreiste „Absaugen“ von Daten. Von Computer-Freaks herausgefundene und in Presseberichten publizierte Nachrichten wie „Weltherrschaft via Vista, Experten halten Microsofts neues Betriebssystem für indiskret“ bleiben nicht ohne Erfolg, das haben damals die Reaktionen auf den kleinen ET im Windows Mediaplayer „....nach Hause telefonieren“ gezeigt. Auch der Internetbranche wird bewusst, dass sie in punkto Datenschutz die Rechnung ohne den Wirt gemacht hat. Jedenfalls ist in den letzten Jahren festzustellen, dass sich führende Unternehmen mehr um Datenschutz und Datensicherheit in ihren Angeboten und Produkten kümmern und dies in ihren Erklärungen nachvollziehbar machen. Auch das Bundesministerium der Justiz durfte auf diesem Gebiet erste Erfahrungen sammeln (zum Urteil des BVerfG in diesem Zusammenhang vgl. Ziff. 4.4 dieses Berichts).

Anzumerken ist, dass ich natürlich eine Vielzahl von Bürgerbeschwerden erhalte, die sich auf Datenschutzverstöße im Internet beziehen. Nicht in allen Fällen kann ich tatsächlich helfen, weil mir zum einen eine hierfür ausreichende personelle Ausstattung fehlt, zum anderen oft der technische Aufklärungsaufwand in keinem Verhältnis zum ungewissen Erfolg steht.

1.8 Deine Internet-Suchmaschine kennt Dich

Derzeit steht bei den EU-Innenpolitikern die geplante Fusion zwischen Google und dem US-amerikanischen Online-Werbevermarkter DoubleClick auf dem Prüfstand. Beide Unternehmen gehören in ihren jeweiligen Geschäftsbereichen zu den Marktführern. DoubleClick ist einer der größten Anbieter auf dem Markt für Online-Banner-Werbung. Google ist bei den Suchmaschinen die Nummer Eins und Marktführer in Sachen kontextbezogener Webseiten- und Suchmaschinenwerbung. Nicht erst jetzt diskutieren die Datenschutzbeauftragten die Auswirkungen der umstrittenen Übernahme. Schon die bloße zunehmende Abhängigkeit von einer solchen Suchmaschine wie Google bei Wissenschaft, Politik und Verwaltung zwingen zu einer gesellschaftspolitischen Debatte. So liegt es auf der Hand, dass dann, wenn bestimmte Informationen gezielt auf die hinteren Seiten einer Suchmaschine verbannt werden oder gar ganz geblockt werden, wie z. B. für die VR China, dies Einfluss auf die Meinungsbildung hat. Die Abhängigkeit bei der Entscheidungsfindung von Suchmaschinen nimmt in allen gesellschaftlichen Bereichen zu. Eine gesellschaftliche Kontrolle dieser Suchmaschinen gibt es jedoch nicht.

Google macht mit seinem Werbesystemen Milliardenumsätze, die sich der börsennotierte Gigant natürlich nicht durch gesetzliche Vorgaben beschneiden lassen möchte. Wer "googeln" will, muss Werbung akzeptieren, so lautet Googles Grundsatz. Dabei werde lediglich die IP-Adresse gespeichert.

Eine Datenpanne, die dem Mitbewerber AOL Anfang August 2006 unterlief, spricht eine andere Sprache. Die Suchverläufe von mehr als einer halben Million AOL-Nutzern wurden damals versehentlich online gestellt. IP-Adressen wurden nicht genannt, dafür alle Suchanfragen mit Datum und Uhrzeit sowie die angeklickten Webseiten. Insidermeldungen zu Folge stammten dabei die Daten nicht von AOL, sondern von Google, weil AOL keine eigene Suchmaschine einsetze, sondern über Google für sich suchen lässt. Fazit war, dass mittels der veröffentlichten Daten aus den Suchläufen es mit einfachen technischen Mitteln gelang, einzelne AOL-Kunden mit Namen und Anschrift zu identifizieren. Damit waren bereits ohne IP-Adresse Rückschlüsse auf das Surfverhalten und die Interessen konkreter Nutzer möglich. Der Öffentlichkeit wurde zum ersten Mal deutlich, dass alles aufgezeichnet wird, was die Benutzer tun. Google gelingt das, indem jedem Surfer beim erstmaligen Besuch der Google-Webseite eine eindeutige Identifikationsnummer zugewiesen wird, die in einer kleinen Textdatei, einem Cookie, auf seiner Festplatte gespeichert wird. Die Daten, die unter dieser Nummer eifrig gesammelt werden, dienen dazu, Profile anzulegen, um die Nutzer mit gezielter Werbung einzudecken.

Mit der Fusion von Google und DoubleClick verbinden sich die beiden größten globalen Datenbanken mit Daten von Konsumenten. Hinzu tritt, dass Google auch noch andere personenbeziehbare Internet-Dienstleistungen anbietet, wie Google Mail, Google Talk oder Google Kalender (näheres vgl. Ziff. 4.2 dieses Berichts). Ein Google-Slogan lautet: "Kein Aufwand, keine Kosten: Einfache und leistungsstarke Tools zur Kommunikation und Zusammenarbeit für Organisationen und Schulen". Aber hat das börsenorientierte Unternehmen tatsächlich etwas zu verschenken?

Darüber hinaus hat Google Presseberichten zufolge im April 2007 einen Patentantrag für eine Methode eingereicht, mit der sich die psychologischen Profile von Millionen Menschen erzeugen

lassen, indem ihre Aktivitäten bei Online-Spielen heimlich verfolgt werden. Aus dem Online-Verhalten ließen sich Aufschlüsse über Persönlichkeit und Vorlieben der Spieler ziehen, um diese Profile an Interessenten zu verkaufen, die in Spielen werben wollen.

Das Patent wurde nach dem Bericht der britischen Zeitung Guardian in den USA und in Europa eingereicht. Der Newsticker von www.heise.de meldete am 12. Mai 2007: Der Patentbeschreibung zufolge eigneten sich Rollenspiele wie „World of Warcraft“ oder „Second Life“ am besten für die Erzeugung psychologischer Profile, da hier die Spieler mit anderen interagieren und Entscheidungen treffen, die denen ähnlich sein könnten, die sie im wirklichen Leben treffen. Aus den Dialogen könne man herauslesen, ob ein Benutzer beispielsweise vorsichtig, höflich, aggressiv, verletzend oder ruhig sei, zudem ließen sich aus dem Spielverhalten auch Persönlichkeitseigenschaften wie kooperatives, aggressives, riskantes Verhalten schließen. Damit könne man Werbung gezielter schalten, so der Patentantrag. Wer beispielsweise viel Zeit auf Erkundungen verwendet, könnte Interesse an Urlaubsangeboten zeigen, wer viel mit anderen Spielern spricht, wäre vielleicht der Handy-Werbung gegenüber empfänglich. Wer länger als zwei Stunden am Stück spielt, könne auf Werbung für Pizzas, Kaffee oder Getränke ansprechen.

Beobachtet würden nicht nur Online-Spiele, sondern auch Spiele auf Konsolen mit einer Internet-Verbindung. Auch aus gespeicherten Spielinformationen ließen sich Informationen gewinnen. Eine Personenbeziehbarkeit ist auch hier nicht ausgeschlossen. Damit werden z. B. auch künftige Arbeitgeber an diesen Psychogrammen der überwiegend jugendlichen Spieler interessiert sein. Da bleibt es ein schwacher Trost, dass nach Auskunft von Google das Unternehmen keine baldige Anwendung der beschriebenen Technik beabsichtige. Es soll sich dabei nur um einen von vielen Patentanträgen handeln, die Google gestellt habe.

Aber damit nicht genug, letzten Meldungen zufolge will Google in das Mobilfunkgeschäft einsteigen. Entwickelt wird ein Handy-Betriebssystem namens Android, das in Zusammenarbeit mit über 30 Technologie- und Telekomkonzernen entwickelt werden soll, teilte das Unternehmen mit. Die Handydaten gekoppelt mit Google-Earth und Google weiß, wo Sie sind und was Sie dort wahrscheinlich suchen.

Wir, die Datenschutzbeauftragten in der EU sind daher gut beraten, wenn wir weiterhin die Entwicklung im Auge behalten. Ich habe auf dieses Thema erneut öffentlich hingewiesen (vgl. BN/WK vom 20 Juni 2007, „Datenschützer kritisieren Google: Suchmaschine speichert Recherchen 18 Monate/Benutzerverhalten wird transparent“). Die Auseinandersetzung mit Google um die Speicherfristen (vgl. Ziff. 4.2 dieses Berichts) kann daher nur ein erster Schritt gewesen sein.

1.9 Kinderschutz

Die Wogen in der öffentlichen Meinung schlagen zu recht hoch, wenn Kindesvernachlässigungen bis hin zum Tod der Kinder als Folge bekannt werden. Seit dem Fall „Kevin“ in Bremen hat es eine ganze Reihe ähnlich gelagerter Fälle in anderen Bundesländern gegeben, die mich alle nur fassungslos machen, wie Eltern es fertig bringen, so mit hilflos ihnen ausgelieferten Geschöpfen umzugehen. Die Politik erfährt daher von mir jegliche Unterstützung, wenn es darum geht, Wege zu finden, diese

Gräueltaten zu verhindern. Allerdings muss auch gesagt werden, dass alle bisher öffentlich bekannt gewordenen Fälle nicht deshalb geschehen konnten, weil es den zuständigen Stellen an Informationen fehlte. Ich bin daher nicht bereit, daran mitzuwirken, ein ausuferndes Überwachungsinstrument (womöglich basierend auf heimlichen Hinweisen, Verdächtigungen oder gar Verleumdungen) gegenüber allen Eltern aufzubauen, sondern es muss darum gehen, gezielt Problemgruppen in eine konkrete Begleitung zu nehmen, wobei hier zum Beispiel Drogenabhängigkeit, Alkoholismus und psychische Erkrankungen Indiz sein können. Aber auch hier ist es meine Aufgabe, darauf zu achten, dass deren Grundrecht auf informationelle Selbstbestimmung gewahrt wird.

Am 19. Dezember 2007 hat die Ministerpräsidentenkonferenz in Berlin getagt und sich intensiv mit den Problemen der Kindesvernachlässigung und -misshandlung beschäftigt. Dabei hat die Bundesregierung erklärt, zusammen mit den Ländern zu prüfen, welche Änderungen erforderlich sind, um einen reibungslosen Informationsaustausch zum Schutz gefährdeter Kinder in überforderten Familien zu gewährleisten. Ich bin bereit, die Senatorin für Arbeit, Frauen, Gesundheit, Jugend und Soziales bei diesem Prozess zu begleiten, um festzustellen, ob und gegebenenfalls welcher gesetzgeberische Handlungsbedarf für den Aufbau eines angemessenen Informationsaustausches (Frühwarnsystem) erforderlich ist. Dabei muss aber im Auge behalten werden, dass alle Stellen, die ein Behandlungs- oder Hilfeangebot an diesen kritischen Kreis von Eltern und deren Kinder machen, bei Schaffung einer gesetzlichen Übermittlungspflicht wohlmöglich gerade von Eltern dieser Klientel nicht mehr aufgesucht werden, um die Leiden der Kinder zu vertuschen, was das Elend der betroffenen Kinder noch vergrößern dürfte. Ich bin daher der Meinung, dass alles, was über den gesetzlichen Status quo hinaus geregelt werden soll, abgewogen und mit den beteiligten Berufsgruppen diskutiert werden muss.

Unter Zugrundelegung der vorgenannten Prämissen habe ich die verschiedenen Projekte des Ressorts auf diesem Gebiet begleitet, im Einzelnen vgl. unter Ziff. 12.3 dieses Berichts.

1.10 Der 30. Bericht

Die Zahl 30 dieses Datenschutzberichtes ist nicht gleichbedeutend mit „30 Jahre Datenschutz im Lande Bremen“, denn dieser Termin liegt erst im Sommer 2008. Der erste Datenschutzbericht für das Land Bremen musste nämlich bereits nach einem halben Jahr geschrieben werden. Zum 25-jährigen Bestehen des Datenschutzes in Bremen hatte ich noch eine CD herausgebracht mit vielen Artikeln und multimedialen Darstellungen. Einen Teil davon konnte ich später auf meine Homepage übertragen, zu finden unter: www.datenschutz-bremen.de/ds25.php. Ob es mir im Sommer 2008 gelingen wird, auch nur in irgendeiner Form dieses Jubiläum zu begehen, erscheint äußerst fraglich angesichts der angespannten personellen und finanziellen Situation meiner Dienststelle (vgl. Ziff. 20.4 dieses Berichts). Ideen gäbe es genug und vielleicht kommt bis dahin noch ausreichende Unterstützung.

1.11 19.000 Zugriffe pro Monat

Das ist kein Druckfehler: Die Internetseiten des LfDI Bremen wurden 2007 monatlich im Durchschnitt 19.000-mal besucht, das erbrachte die Statistik des Providers. Da war selbst ich sehr überrascht. Im Jahr also über 200.000 Besuche. Ich werte dies als ein Zeichen dafür, dass der Datenschutz bei den Bürgern Hochkonjunktur hat. Die Statistik zeigt darüber hinaus auch, dass eine wesentliche Entlastung der Arbeit mit dem Angebot auf der Homepage verbunden ist.

1.12 Datenpannen

Sei es, dass die Steuerdaten von über 20 Millionen Briten durch eine Datenpanne verloren gingen, sei es, dass der amerikanische Geheimdienst NSA die Telefonverbindungsdaten von 200 Millionen Amerikanern rechtswidrig gesammelt hat oder sei es, dass ein Offizier der Royal Navy sein Notebook mit Informationen über 600.000 Bewerber und Angehörige der Marine verloren hat, es sind nicht die Skandale, die zu mehr Datenschutz führen. Hierfür braucht man einen langen Atem und ein sich kontinuierlich entwickelndes, die technischen Gefahren mit einbeziehendes System von Verantwortung, verbunden mit einem organisierten Risikomanagement. Ich versuche, diesen Prozess seit Jahren in der Bremer Verwaltung fest zu verankern. Die genannten Datenskandale machen m. E. nur deutlich, welche Datenmengen sich mittlerweile in staatlichem Besitz befinden.