

1. Vorwort

1.1 Blick auf das Jahr 2008

Der Blick auf das Jahr 2008 fällt nachdenklich aus. Ja, der Datenschutz konnte viele Erfolge verzeichnen: Der Bericht gibt eine ganze Reihe davon wieder. Datenschutzjubiläen, wie 25 Jahre Volkszählungsurteil, gelungene Veranstaltungen mit Schülerinnen und Schülern in Bremerhaven am europäischen Datenschutztag, das in Bremen abgeschlossene „Profilier-Projekt“ zu den neuen Formen und Gefahren der Identitätsausbeute mit hoher Resonanz in der Bremer Bevölkerung, sind nur einige. Aber auch viele zähe, sich jetzt schon über Jahre hinziehende Verhandlungen mit Spitzenverbänden der Wirtschaft, so dass häufig die Verhandlungsergebnisse schon bald wieder von der technischen Entwicklung überrollt werden, ein Bundesgesetzgeber, der die Ränder der Verfassung immer wieder austestet und vom Bundesverfassungsgericht wiederholt zurückbeordert werden musste und, nicht zu vergessen, die Datenschutzskandale, beginnend im Frühjahr mit dem Bekannt werden der Arbeitnehmerüberwachung bei Lidl, gefolgt von illegaler Überwachung mit Verbindungsdaten bei der Telekom.

Ja, die Telekom ist wohl mit Abstand der größte Verlierer im Jahr der Datenpannen und des Datenklaus, denn der Telekom kamen wohl die meisten Daten abhanden. Auch wenn diese Daten bei verschiedenen Callcentern, Adresshändlern oder im Internet auftauchten und die Staatsanwaltschaft die Daten an diesen Orten beschlagnahmte, muss doch davon ausgegangen werden, dass der größte Teil der Daten verloren bleibt, denn es ist wahrscheinlich, dass weitere Kopien existieren, die unter der Hand vermarktet wurden. Das Kind „Vertrauen“ ist in den Brunnen gefallen, auch wenn das Management sich jetzt intensiv bemüht, den Datenschutz im Unternehmen auf Vordermann zu bringen.

Auch beim Datenskandal eines Berliner Bankhauses reibt man sich ungläubig die Augen: Jeder 5-Euro-Schein wird schwer bewacht und sicher verpackt in gepanzerten Fahrzeugen transportiert. Große Mengen sensibler Kundendaten hingegen gibt man zum Versand bei der Post auf.

Erschreckend ist, dass gerade Unternehmen mit besonderen Geheimhaltungsregeln, nämlich dem Telekommunikations- und dem Bankgeheimnis, die älter als die allgemeinen Datenschutzvorschriften sind, durch besonders laxen Umgang mit geschützten Daten auffielen.

Nicht umsonst schaffte das Wort „Datenklau“ es immerhin auf Platz 3 der Top Ten der Worte des Jahres. Bei den Datenschutzbeauftragten wie bei den -aufsichtsbehörden sorgten die mit dem Wort verbundenen Datenskandale im zweiten Halbjahr für Hochkonjunktur. Sicherlich, die Bevölkerung ist von den Datenschutzthemen aufgerüttelt, aber wir, die wir wissen, dass es nur die Spitze des Eisbergs ist, die sichtbar wurde, allein wenn wir in die Tiefen des Internets schauen, wissen nicht, ob wir uns über das Erreichte freuen können, denn die permanente und rapide informationstechnologische Entwicklung macht einen Datenschutz auf Augenhöhe der technischen Entwicklung fast ausgeschlossen, jedenfalls so lange, wie sich nicht die Systementwickler und Datenverarbeiter selbst mit an die Spitze der Datenschutzbewegung setzen.

Auch wenn die Datenschutzskandale zu beklagen sind, wenn viele Betroffene dadurch auch materiellen Schaden genommen haben, hat doch all das dazu beigetragen, dass die Unterstützung des Datenschutzes seitens der Politik wie der Bürgerinnen und Bürger stark zugenommen hat.

Wesentlich anders als bei Teilen der Wirtschaft und im Bund sieht die Situation zurzeit im öffentlichen Bereich in Bremen und Bremerhaven aus. Zwar wird hier und da immer wieder vergessen, den Datenschutz schon in der Projektphase zu implementieren, in einzelnen Bereichen muss auch noch zäh für ein Datenschutzbewusstsein gerungen werden, aber in vielen Bereichen auch der Führungsebenen finden nicht mehr wie früher lange Diskussionen über das „Ob“ statt, sondern es wird immer häufiger gefragt, was für einen guten Datenschutz zu tun ist, und dann wird das auch zügig umgesetzt. Auch im Bereich der inneren Sicherheit werden in letzter Zeit nicht wie in anderen Bundesländern dauernd die gesetzlichen Befugnisse für Eingriffe in das Recht auf informationelle Selbstbestimmung erweitert, sondern, wie in diesem Jahr geschehen, es wurde die verfassungswidrige Regelung zum Kfz-Kennzeichenscan im Bremischen Polizeigesetz umgehend ersatzlos gestrichen.

Nicht zu unterschätzen sind die Pionierleistungen, die Bremen, auch in Abstimmung mit meinem Haus, bundesweit auf dem Gebiet des E-Governments auf den Weg gebracht hat und dessen Früchte einer sicheren Kommunikation seit geraumer Zeit geerntet werden können. Es ist nicht zu verkennen, ein Teil der Probleme mit dem Datenschutz rührt daher, dass im Land Bremen gespart werden muss und daher auch die informationstechnischen Projekte unter engen personellen und sachlichen Bedingungen vorangetrieben werden müssen. Oft geht es darum, dass ein System bis zu einem bestimmten Termin funktionstüchtig bereitstehen muss. Und in dieser Not wird dann auch am Datenschutz gespart. Die Aufgabe des Landesdatenschutzbeauftragten ist es aber nicht, sich damit abzufinden, und deshalb lasse ich in solchen Fällen, auch wenn es der Verwaltung häufig „auf die Nerven geht“, nicht locker, bis der Datenschutz nachgebessert wurde. So wurden z. B. in den letzten Jahren schrittweise für einzelne Module im Stadtamt Bremen Datenschutzkonzepte erstellt, nun zeichnet sich in diesem Jahr ab, dass auch das fehlende Bindeglied, das Rahmendatenschutzkonzept, seiner Vollendung zustrebt. Ein Thema, mit dem sich der parlamentarische Ausschuss für den Datenschutz leider immer wieder beschäftigen musste, strebt damit seiner Lösung zu.

Mit dem Referat 36 der Senatorin für Finanzen, das als zentrale Schnittstelle die IT-Infrastruktur des Landes Bremen maßgeblich gestaltet, hat im Berichtsjahr eine enge Kommunikation mit meiner Dienststelle stattgefunden. Komplexe Veränderungen der Infrastruktur, wie die Auslagerung bremischer Verfahren zum Dienstleister Dataport, die Zentralisierung der E-Mail-Kommunikation und die Einführung eines neuen Verzeichnisdienstes (Active Directory), erforderten neben der Klärung von Grundsatzfragen und der Festlegung datenschutzrechtlicher Anforderungen in Konzepten auch einen ständigen Austausch während des Einführungsprozesses. In dem Spannungsfeld zwischen Wirtschaftlichkeit, Effizienz, technologischer Qualität und Datenschutz ist es trotz massiven Zeitdrucks gelungen, einvernehmlich konstruktive Lösungen zu finden.

1.2 Kurzer Rückblick auf die Projekte der letzten acht Jahre

In den vergangenen Jahren habe ich neben den Beratungs- und Kontrollaufgaben immer parallel weitere Ziele zur Effektivierung und Leistungsverbesserung meiner Dienststelle und des Datenschutzes verfolgt.

- Begonnen habe ich mit der Verstärkung der Internetpräsenz durch den Auf- und Ausbau der Homepage des Landesbeauftragten für Datenschutz. Durch diese Maßnahme habe ich eine spürbare Entlastung bei Standardanfragen erreicht.
- Maßgeblich habe ich mich an der konzeptionellen Entwicklung der bis Mitte 2008 landeseigenen Gesellschaft „datenschutz nord“ beteiligt.
- Dann kam das Jubiläumsjahr 2003: Mit der Herausgabe der CD-ROM „25 Jahre Datenschutz im Land Bremen“ habe ich zwei Ziele verbunden. Zum einen den Rückblick auf die Entwicklung im legislativen Bereich im Land Bremen - ich erinnere nur an die bundesweit richtungsweisenden Datenschutzregelungen im Bremischen Polizei- wie auch im Bremischen Verfassungsschutzgesetz -, einem Rückblick auf die Arbeit des parlamentarischen Datenschutzausschusses (alle Vorsitzenden waren bereit, das jeweils in einer Legislaturperiode Erreichte darzustellen), einem Rückblick auf die Arbeit der Senatskommissare für den Datenschutz und einem Rückblick auf die vor mir amtierenden Datenschutzbeauftragten, die mit beachteten Beiträgen auf die Situation im Datenschutz eingingen oder aber einen real-futuristischen Ausblick auf die Zukunft des Datenschutzes warfen. Zum anderen enthielt die CD-ROM erstmalig in elektronischer Form die bis dahin erschienenen Jahresberichte. Damit war es einfach geworden, auf die doch häufigen Anfragen auf Übersendung von Datenschutzberichten zu reagieren, nicht nur, dass die Erstellung der CD mit allen Jahresberichten günstiger war als der Druck eines Berichts auf Papier, auch das Porto für den Versand war deutlich geringer. Im gleichen Jahr habe ich dann die elektronisch erfassten Berichte auch auf meine Homepage übernommen.
- Ein seit Inkrafttreten der Vorschriften über die behördlichen Datenschutzbeauftragten 2003 verfolgtes Projekt ist die Durchführung von Workshops mit den behördlichen Datenschutzbeauftragten, um so deren Eigenständigkeit zu stärken. Die Workshops werden zwei- bis dreimal im Jahr durchgeführt, enthalten einen Schulungsteil, den meine Dienststelle durchführt, und sind verbunden mit einem daran anschließenden Erfahrungsaustausch. Die im Rahmen der Unterrichtung über die Aufgaben gehaltenen Vorträge werden – ergänzt um die Ergebnisse der Diskussion – auf meiner Homepage veröffentlicht, um so behördlichen Datenschutzbeauftragten, die nicht teilnehmen konnten oder die erst neu hinzugekommen sind, die Möglichkeit zu geben, sich auf diese Weise zu informieren. So stehen unter der Rubrik „Hilfestellungen“ bereits eine ganze Reihe von im Hause erarbeiteten Orientierungshilfen und Merkblättern für die Aufgaben der behördlichen Datenschutzbeauftragten zur Verfügung.
- Das nächste von mir in den Jahren 2002/2003 angegangene Projekt mit dem Titel „Selbstverteidigung im Internet“ zielte darauf ab, den Bürger bei der Wahrnehmung seines informationellen Selbstbestimmungsrechts im Internet zu unterstützen. Es reicht nämlich nicht aus, wenn man seine Rechte kennt, im Internet muss man sie auch durchsetzen können. Datenschutz sollte bei einem in der Familie gemeinsam genutzten PC beginnen, u. a. mit der Vermeidung von Datenverlusten durch Virenattacken weitergehen und sich fortsetzen bei der Abwehr von Hackerangriffen und von Ausforschungsprogrammen, die sich im Rechner einnisten. Es waren daher Verhaltensregeln und insbesondere technische Maßnahmen, wie zum Beispiel die richtige Einstellung des Internetbrowsers und der Firewall und anderer Sicherheitssoftware Themen, die bei dieser Aktion im Vordergrund standen. Wegen der sich laufend ändernden

Technik und der immer wieder neu hinzukommenden Gefahren durch Attacken aus dem Internet auf die Rechner wird dieser Bereich meiner Homepage regelmäßig angepasst und ergänzt.

- Im folgenden Jahr wurde das Projekt um weitere Facetten rund um den heimischen PC ergänzt. Mit dem Projekt „Family-PC“ wurden die, wenn auch begrenzten Möglichkeiten zur Erreichung von Datenschutz etwa durch die Einrichtung verschiedener Benutzergruppen für einzelne Familienmitglieder oder der Einstellung des Browsers dargestellt, damit nicht jeder weitere Nutzer des PC schauen kann, welche Internetadressen der Vorgänger in den letzten Wochen oder gar Monaten angewählt hat.
- Dann folgte das Projekt „datenschutz4school“, mit dem ich Schülerinnen und Schüler auf der Ebene ihres alltäglichen Tuns abhole und sie für Fragen des Datenschutzes interessiere. Die Darstellungen sind animiert, die einzelnen Kapitel werden durch die Bremer Stadtmusikanten begleitet. Am Ende können innerhalb der Anwendung durch das richtige Beantworten von Datenschutzfragen gewonnene Punkte in einer Slotmaschine verspielt werden. Die Besten können sich in einer Top Ten-Liste mit Namen, Schule und Punktzahl eintragen. Im Moment liegt das Schulzentrum Grenzstraße mit 6 Einträgen vorn. Da „datenschutz4school“ gerade auch im Unterricht zum Einsatz kommen soll, ist auch eine Lehrhilfe hinterlegt, mit der den Lehrkräften die Methodik und die Lernziele erläutert werden. Zurzeit zählen wir 23 000 Zugriffe, die tatsächlichen Zugriffszahlen dürften deutlich höher liegen, weil oft ganze Klassen über Proxy-Server die Anwendung nutzen.
- Dann musste das Projekt „Erste Homepage für die Bremer Informationsfreiheit“ angegangen werden. Im Frühjahr 2006 wurde das Bremer Informationsfreiheitsgesetz verabschiedet. Es gelang parallel zum Inkrafttreten, die Internetseite „www.informationsfreiheit.de“ zu starten und so den in Bremen und Bremerhaven lebenden Bürgerinnen und Bürgern eine erste Anlaufstelle für alle Fragen rund um die Informationsfreiheit zu geben. Der Senat hat erst wesentlich später dazu etwas auf seiner Homepage angeboten. Ich nenne dieses Projekt an dieser Stelle, weil die finanziellen, insbesondere aber die personellen Ressourcen aus dem Bereich des Datenschutzes geschöpft werden mussten.
- In 2008 konnte endlich die Doppelbroschüre Datenschutz/Informationsfreiheit mit den für Bremen geltenden einschlägigen Gesetzesregelungen und versehen mit Vorwort und Erläuterungen zu beiden Bereichen angeboten werden. Der Bedarf war, wie sich zeigte, groß, die ersten 700 Exemplare waren schnell vergriffen, es mussten noch in 2008 1000 Broschüren nachgedruckt werden. Durch Sponsoring konnten die Kosten pro Heft minimiert werden.
- Schließlich habe ich im Berichtsjahr das Projekt „Profile“ entwickelt, um die Bürgerinnen und Bürger in ihren verschiedenen Rollen als Konsumenten, Arbeitnehmer, Reisende oder Internetsurfer auf die mit der aktuellen technischen Entwicklung einhergehenden neuen Gefahren für ihr Recht auf informationelle Selbstbestimmung aufmerksam zu machen und als „Erste Hilfe“ benannte Abwehrstrategien aufzuzeigen. Näheres finden Sie im Beitrag unter Ziff. 1.3 dieses Berichts und natürlich auf meiner Datenschutz-Homepage. Die einzelnen Beitragsteile wurden jeweils auf den Verbraucherseiten einer Bremer Tageszeitung vorgestellt.

Natürlich können nicht alle Internetprojekte gleichmäßig auf dem neuesten Stand gehalten werden, aber immerhin ist es gelungen, meine Homepage in Abständen von ca. drei Jahren zu aktualisieren.

Das ist angesichts der rasch fortschreitenden technischen Entwicklung das Äußerste, was hinnehmbar ist.

1.3 Mit Datenschutz gegen heimliche Profilbildung

In einer zunehmend technisch geprägten Welt lassen sich die allgegenwärtigen IT-Systeme in ihrer Komplexität durch den Einzelnen immer schwerer beherrschen. Alle Bürgerinnen und Bürger, die moderne Techniken anwenden – bei Kommunikation, Mobilität, Einkauf oder bloßer Information –, geben gewollt oder ungewollt Daten über sich preis und hinterlassen jede Menge digitaler Spuren. Ob Internetsuchmaschine oder „Blog“, Bahncard oder Rabattkarte, ob Fernsehen via DSL, Handy oder Navigationsgerät: Menschen erzeugen Daten, die – systematisch gesammelt und zu sogenannten Profilen gebündelt – sie dann ein Leben lang verfolgen können. Aber die wenigsten Menschen sind sich im Klaren darüber, dass sie damit „gläsern“ und zum Opfer von Datenjägern werden können. Die Profilbildung (Profiling) geschieht nämlich meistens ohne Wissen der Betroffenen.

Im vergangenen Halbjahr habe ich daher in Teamarbeit das Projekt „Profile“ entwickelt und in den sieben Wochen vor Weihnachten auf der Datenschutz-Homepage www.datenschutz.bremen.de sukzessive freigeschaltet. Das Projekt hat den Anspruch, den Bürgerinnen und Bürgern bewusst zu machen, dass es solche „Profiler“ gibt – und ihnen zu zeigen, wie sie sich dagegen soweit wie möglich schützen können. Die jüngsten Fälle von Datenmissbrauch machen deutlich: Es ist für die Bürgerinnen und Bürger völlig egal, ob ihre Daten legal erfasst oder illegal abgesaugt werden. Denn die „Profile“, die man daraus erstellen kann, und die darauf aufbauende Datennutzung sind längst zu einer lukrativen Wirtschaftsbranche geworden. Nur wenn die Betroffenen lernen, die Erzeugung solcher Daten zu vermeiden oder aber ihre Spuren zu löschen, haben sie eine Chance, Herr ihrer Daten zu bleiben.

In dem Projekt werden daher, mit provokanten Überschriften versehen, nüchterne technische Sachverhalte ansprechend dargestellt und dabei nicht nur die nachweisbaren, sondern auch mögliche, mit der Entwicklung verbundene künftige Risiken angesprochen. Überschriften wie „Verkaufen Sie sich nicht, wenn Sie einkaufen“, „Alles unter Kontrolle – Sie auch“ oder „Gläserne Bürger machen Demokratie zerbrechlich“ verdeutlichen dies. Zu jeder der sieben Einheiten wurde eine „Erste Hilfe“ für die Bürgerinnen und Bürger veröffentlicht, in der sowohl besonders risikoreiches Verhalten als auch Möglichkeiten der Gefahrenabwehr dargestellt werden.

In Kooperation mit der Redaktion der Bremer Tageszeitungen („Weser-Kurier“ und „Bremer Nachrichten“) erschien – parallel zu den Veröffentlichungen auf meiner Homepage -- eine siebenteilige Artikelserie der Redaktion auf der Verbraucherseite unter dem Logo „VERRATEN UND VERKAUFT“. Mit dieser Serie ist es gelungen, mehr oder weniger umfassend und bundesweit erstmalig die neuen technischen Entwicklungen, mit denen die Bürgerinnen und Bürger konfrontiert sind, zusammenfassend darzustellen und die damit verbundenen Datenschutzrisiken aufzuzeigen.

Die mit der Serie gestiegenen Zugriffszahlen auf meine Homepage verdeutlichen das Interesse der Bevölkerung. Ich hoffe, dass ich die Bürgerinnen und Bürger ein bisschen wachrütteln konnte. Vielleicht haben sie so erst die notwendigen Sicherheitseinstellungen an ihrem neuen PC vorgenommen, der auf dem Gabentisch lag, bevor sie sich mit den Worten „Ich bin schon drin“ ins World Wide Web begeben haben.

Themen der Serie (in Klammern das Erscheinungsdatum) sind:

Google und andere Suchmaschinen	(06.11.2008)
ID-Management	(13.11.2008)
Location Based Services	(20.11.2008)
RFID	(27.11.2008)
Konvergenz von Techniken & Netzen	(04.12.2008)
Ubiquitäres Computing	(11.12.2008)
Soziale Netzwerke - Web 2.0	(18.12.2008)

1.4 Kein Datenschutz ohne Datensicherheit

Ein ausreichender Datenschutz ohne Datensicherheit wäre nicht zu denken. Das Ziel ist immer das gleiche: Sicherheit für Unternehmensdaten, Sicherheit für personenbezogene Daten, Sicherheit für Unternehmensinfrastrukturen, Sicherheit für Verwaltungsinfrastrukturen, Sicherheit für nationale Infrastrukturen. Auch die Methoden, um die Ziele zu erreichen, sind weitgehend deckungsgleich. Soweit der einfache Teil der Betrachtung, denn die Anzahl der möglichen Anwendungen und deren Einsatzkontexte sind unbegrenzt. Extrem schwierig wird es, wenn es darum geht festzulegen, welche konkreten Methoden angemessen sind, um das Ziel „Sicherheit“ zu erreichen. Zumal ständig und permanent neue Sicherheitsgefahren mit immer noch zunehmender Geschwindigkeit auftauchen.

Da den Überblick zu behalten, ist selbst für Spezialisten nicht einfach. Da gibt es Innentäter und Außentäter, zeit- und sicherheitskritische Anwendungen, über mehrere Standorte verteilte Anwendungen, die auch noch vollständig mobil zu nutzen sind, und irgendwie hängt alles auch immer mit dem Internet zusammen. Hier ein paar Zahlen, die ich ähnlich auf dem 16. BremSec-Forum in Bremen vorgetragen habe.

Umfragen zeigen:

- Die gegenüber deutschen Unternehmen aufgedeckten Straftaten im IT-Bereich summieren sich auf einen Schaden von 6 Milliarden Euro pro Jahr,
- fast 50 % aller deutschen Unternehmen haben in den vergangenen beiden Jahren Schäden durch Wirtschaftskriminalität erlitten,
- rund 50 % aller Täter stammen aus dem eigenen Unternehmen,
- früher handelte es sich mehr um „Fun-Täter“, heute wird der wirtschaftliche Vorteil gesucht.

Die Gefahrenlage:

- Die Anzahl von Schadprogrammen sowie die Summe der Schwachstellen in IT-Produkten (Hardware, Software) verdoppeln sich mindestens jährlich,
- fast jede zehnte E-Mail ist mit Malware (Viren, Würmer) verseucht,
- mehr als 90 % aller E-Mails weltweit sind Spams.
- der Trend geht zu unauffälligen Spionageprogrammen (Trojaner, Bot-Netze), die für kriminelle Zwecke eingesetzt werden,
- mobile Endgeräte verschieben Unternehmensgrenzen und stellen ein qualitativ neues Risiko dar,

- die generellen Möglichkeiten von Angriffen auf zentrale IT-Strukturen steigen durch zunehmende Nutzung von Standardsystemen und -software in kritischen Bereichen.

Doch trotz der gestiegenen Risiken für die IT verzichten gerade mittelständische Unternehmen auf geeignete Schutzmaßnahmen! (Ergebnisse einer Umfrage von PWC unter 8200 IT-Verantwortlichen aus 63 Ländern)

- Die sicherheitsbezogenen IT-Vorfälle stiegen um 22,4 %,
- ca. 24 % erlitten dadurch finanziellen Schaden (Vorjahr: 7 %),
- Befragte aus Deutschland bezifferten den jeweils erlittenen Schaden im Einzelfall auf bis zu 500 000 € und bestätigten Ausfallzeiten von bis zu 8 Stunden.

Aber

- nur etwa 13 % der Investitionen fließen in den IT-Bereich (Vorjahr: 15 %),
- nur jedes 3. Unternehmen hat tatsächlich einen IT-Notfallplan,
- weltweit will jedes 2. Unternehmen mehr in IT-Sicherheit investieren, in Deutschland nur jedes 3. Unternehmen.

(Diese Darstellung beruht auf Auswertungen von Publikationen der NIFISeV und PriceWaterhouseCoopers/Martin-Luther-Universität, Wirtschaftskriminalität 2007.)

Für Unternehmen und Verwaltungen bleibt oft nichts anderes übrig, als auf externe Dienstleister zurückzugreifen, um etwaige Risiken zu bewerten und sich dagegen abzusichern. Ansonsten stehen viele IT-Verantwortliche oft allein auf weiter Flur, obwohl die grundsätzlichen Fragestellungen überall die gleichen sind. Da macht es Sinn, sich, wie auf dem BremSec-Forum geschehen, zu treffen und zu hören, aber auch zu berichten, welche Probleme man wie bearbeiten kann. Das sichert einen leichten Informationsfluss von Know-how-Trägern und dient insgesamt der Sache: „IT-Sicherheit und Datenschutz“. Ich unterstütze daher solche Initiativen nach Kräften, denn in solchen Netzwerken lassen sich die wachsenden Probleme am besten kommunizieren und Lösungen diskutieren.

1.5 Datenschutz steht heute vor ganz neuen Herausforderungen

Früher ging es darum, die Betreiber von Großrechenanlagen/Rechenzentren und darauf folgend um Arbeitsplatzcomputer für einen verantwortungsbewussten Umgang mit der Technik und den dort gespeicherten Daten zu gewinnen. Heute befinden sich mannigfaltige Geräte, die personenbezogene Daten erzeugen und verarbeiten, in vielen Händen: Neben den Unternehmen und staatlichen Stellen jetzt auch in privaten Haushalten und dort mit Handy oder PC bereits in den meisten Kinderzimmern. Dabei ist den wenigsten bekannt, wie und wo ihre Daten tatsächlich verarbeitet werden, z. B. im Inland oder Ausland. Das aber kann für den Schutz ihrer Daten von zentraler Bedeutung sein.

Schauen wir beispielhaft auf den Einkaufsvorgang: Wurde früher mit Bargeld bezahlt und wurden vielleicht noch Rabattmarken geklebt, ist es heute die EC-Karte mit elektronischem Chip, die Rabattkarte mit Magnetstreifen und demnächst der in alle Waren implantierte RFID-Chip, die zum Einsatz kommen. Wurde früher vom Käufer eine Erkundigung über die Ware noch persönlich oder zumindest vor Ort erfragt, wird eine solche Auskunft heute in der Regel von einem Callcenter erteilt, je nach Uhrzeit des Anrufs mit Sitz in Europa oder in Asien. Gehen solche Anrufe ohne Rufnummernunterdrückung raus, lässt sich leicht feststellen, von welchem Ort der Anruf erfolgt und

wem der Telefonanschluss gehört. Vielleicht hat der Händler vor dem Verkauf noch eine SCHUFA-Anfrage getätigt, dann erfolgt in der Regel auch dorthin eine Rückmeldung über die Abwicklung des Geschäfts. Noch weit datenintensiver ist der Onlineeinkauf. Fazit: Schon beim einfachsten Vorgang werden an vielen Stellen elektronische Datenspuren hinterlassen.

Zur rapide zunehmenden Verbreitung der DV-Technik gesellt sich eine andere Entwicklung: Heute gibt es nicht nur mehr Technik, sie ist auch zunehmend viel leistungsfähiger, immer komplexer und zudem sind die unterschiedlichen Systeme vielfach miteinander verknüpft oder werden in einen Leistungsrahmen integriert. Gemeint ist die möglichst umfassende Vernetzung aller nur denkbaren Kommunikations- und Datenaustauschtechniken: Internet und E-Mail, Telefon- und Telefax-Dienste, Rundfunk und Fernsehen – alles soll jederzeit an jedem Ort jedermann zur Verfügung stehen und zwar immer in einer „zweigleisigen“ Form: Zu jedem (passiven) Datenempfang gehört zwingend auch die Möglichkeit der aktiven Datenübermittlung. Die bislang auf einzelne Zwecke spezialisierten Kommunikationssysteme sollen zu einer einzigen digitalen Informations- und Kommunikationsplattform zusammenwachsen. Microsoft-Chef Bill Gates proklamierte vor Jahren schon den „Informationshighway“, jetzt stehen auch die dafür erforderlichen komplexen Endgeräte zur Verfügung.

Voraussetzung dafür war und ist, dass die Endgeräte zu immer größeren „Alleskönnern“ werden. Das Handy zum Beispiel ist nicht mehr nur Telefon, sondern kann auch Faxe, Bilder oder Videosequenzen senden, ist Fotoapparat, Videokamera, elektronischer Terminkalender und Radio, zeigt Filme und Fernsehen, verfügt über Internettauglichkeit mit vielfältigen Funktionen, kann gleichzeitig auch noch Navigator und vieles mehr sein. Diese Geräte werden in der Regel so ausgeliefert, dass alle Funktionen uneingeschränkt aktiviert sind. Im Internetbrowser zum Beispiel werden die zuvor aufgerufenen Internetadressen gespeichert, in der SMS-Funktion nicht nur die empfangenen, sondern auch die gesendeten und sogar die gelöschten Nachrichten gespeichert; Entsprechendes gilt für die E-Mail-Funktion und die Rufnummernunterdrückung ist natürlich auch nicht aktiviert.

Diese Geräte lassen sich für den unerfahrenen Einzelnen meistens nur schwer bändigen. Nicht nur, dass die Menüstruktur oft datenschutzfreundliche Einstellungen erschwert, auch die Funktionen sind oft so rudimentär, dass sich zum Beispiel Dateninhalte in Verzeichnissen nur einzeln löschen lassen, obwohl die Nutzenden gern den Inhalt des ganzen Verzeichnisses gelöscht hätten. Einige Daten werden auf der SIM-Karte, andere auf dem Festspeicher im Handy, dritte in einem zusätzlichen Mobilspeicher (beispielsweise MiniSD-Karte) gespeichert. Wer ein solches Gerät etwa nach einem Jahr Gebrauch weitergeben will, hat seine liebe Mühe, alle persönlichen Daten zu löschen. Mit dem Ausbau der SIM-Karte allein ist es jedenfalls nicht getan. Irgendetwas wird dabei immer vergessen, und seien es die eingetragenen Geburtstage im Organizer.

Warum mache ich eine solche Aufzählung, die sich übrigens noch beliebig verlängern ließe und die nicht nur für das Handy gilt, sondern entsprechend zugleich für viele andere Geräte? Nun, weil sich daran gravierende Mängel der jetzigen technischen Entwicklung festmachen lassen:

- Die voreingestellten Konfigurationen sind oft ohne Sinn für Datenschutz auf maximale Kommunikationsmöglichkeiten ausgerichtet.
- Die Anforderungen, die die Produktautomatisierung an die Nutzenden stellt, sind sehr hoch. Letztere sind für einen sachgemäßen Umgang nicht adäquat ausgebildet oder unterrichtet und, was die Datenschutzgefahren betrifft, oft ahnungslos.

- Einfache technisch unterstützte Datenschutzfunktionen wie „löschen“ oder „unterdrücken“ werden oft nicht oder nicht hinreichend mitentwickelt, viele Anbieter stellen ihren Kunden keinen ausreichenden Basisschutz zur Verfügung.
- Nicht geregelte Marktmechanismen führen dazu, dass Geräte oft nicht ausreichend getestet und daher mit Sicherheitslücken ausgeliefert werden. Der Endverbraucher wird zum Versuchskaninchen und muss sich beispielsweise selbst durch Updates um die Sicherheit seiner Geräte kümmern.
- Hinzu kommt, dass, bedingt durch die Multifunktionalität der Geräte, bei einzelbestimmter, nicht verändernder Kennung sich noch viel einfacher umfassende Profile bilden lassen.

Ergebnis: Es entstehen alltägliche Datenspuren, die wir ungewollt, unbemerkt und damit größtenteils unwissend hinterlassen. Einen Teil dieser Entwicklung habe ich genauer und ausführlicher in meinem Projekt „Profile“ auf meiner Homepage beschrieben (vgl. Ziff. 1.3 dieses Berichts). Eine der großen gesellschaftlichen Herausforderungen zur Einlösung des Rechts auf informationelle Selbstbestimmung ist die Bändigung dieser Technik, ohne sie dabei in ihrer Entwicklung zu behindern. Es kann nicht allein Aufgabe des Bundesverfassungsgerichts sein, immer wieder von der Verfassung verbriefte Grundrechte vor informationstechnisch basierten Eingriffen zu sichern. Die technischen Entwicklungen aller IT-Systeme sind künftig daran zu messen, ob das neu abgeleitete „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“ in angemessener Weise umgesetzt wurde. Eine Schwerpunktaufgabe der Datenschutzbeauftragten von Bund und Ländern wird es sein, diesem neuen Grundrecht Wirkung zu verschaffen und dessen Umsetzung zu kontrollieren. Es ist daher notwendig, dass mit Politik und Wirtschaft ein breiter Dialog über diese Fragen entsteht.

Das geltende Datenschutzrecht liefert für verschiedene Probleme der Entwicklung in den letzten Jahren nur sehr eingeschränkte Lösungen. Schon bei der Betrachtung des komplexen Systems der elektronischen Gesundheitskarte stößt man schnell an die Grenzen geltenden Rechts, gleiches gilt für neue Produkte wie „digitale Straßenansichten“ oder die Kommunikationsplattformen der sogenannten „Sozialen Netzwerke“. Erst recht gilt dies für die oben beschriebenen technischen Entwicklungen, die unter anderem mit Begriffen wie „Informationshighway“, „Konvergenz der Systeme“, „Ubiquitous Computing“, „RFID“, „Location Based Services“ oder „Smart Dust“ beschrieben werden. Die datenschutzrechtlichen Begriffe wie „Herr der Daten“ oder „verantwortliche Stelle“ lassen sich nicht mehr klar definieren, allenfalls mit den Geboten der „Datensparsamkeit“ oder der „Datenvermeidung“ lässt sich hier noch ein Stück weit operieren. Der überwiegende Teil der Datenschützer ist sich daher einig, dass das geltende Recht den technischen Entwicklungen angepasst werden muss.

Ich habe zusammen mit den Datenschutzbeauftragten des Bundes und der Länder hierauf verschiedentlich hingewiesen (vgl. Ziff. 20.3 dieses Berichts) und auch meine Bereitschaft erklärt, an konstruktiven Lösungen mitzuwirken. Anders als das Bundesverfassungsgericht können aber die Datenschutzbeauftragten nicht aus der Verfassung neue Grundrechte entwickeln oder, wie der Gesetzgeber, neues Recht kreieren; sie sind an das geltende Recht gebunden, auch eine verfassungsrechtlich gebotene moderne Auslegung hat dabei ihre Grenzen.

Gleichwohl muss ich mich nicht auf eine bloße Rechtsanwendung beschränken. Vielmehr sehe ich es auch als meine Aufgabe, den Gesetzgeber auf Entwicklungen hinzuweisen, die zur Gewährleistung eines effektiven Datenschutzes einer Korrektur bedürfen (vgl. Ziff. 20.3 dieses Berichts) Die seit Jahren angemahnten Regelungen gegenüber dem Bund für einen Arbeitnehmerdatenschutz sind ein

Beispiel dafür, die jüngst gemachten Vorschläge zum Adresshandel ein anderes. Für die in diesem Artikel beschriebenen technischen Entwicklungen gibt es allerdings keine rechtlichen Patentlösungen. Notwendig ist daher eine breite Diskussion, die die verschiedenen, zum Teil konkurrierenden gesellschaftlichen Ziele formuliert. Erst dann kann damit begonnen werden, die hierfür erforderlichen Rahmenbedingungen zu schaffen. Die Fortentwicklung des Rechts ist dabei ein Schritt.

Aber auch – wie es so schön heißt – der Faktor Mensch muss Berücksichtigung finden. Die Technik darf nicht zu viel von ihm verlangen. Schon jetzt muss sich Untersuchungen zufolge jeder Bundesbürger zwischen sechs und acht Passwörter oder PIN merken. In den nächsten Jahren wird sich die Zahl auf durchschnittlich zwölf erhöhen. Das überfordert viele und führt zu neuen Sicherheitslücken. Zu berücksichtigen ist dabei, dass manche Karten, die nur mit einer PIN einsatzfähig sind, lediglich einmal im Jahr oder weniger zum Einsatz kommen. Hier sind sichere und intelligente Lösungen gefragt. Auch die Menüführung komplexer IT-Geräte sollte ein eigenes Feature „Datenschutz“ haben.

Viele Sicherheits- und Datenschutzprobleme bei IT-Produkten sind – wie oben skizziert – auf unsichere Grundeinstellungen der Systeme zurückzuführen. So wurden vor nicht allzu langer Zeit noch WLAN-Komponenten zunächst ohne, später ohne aktivierte Verschlüsselungsfunktion ausgeliefert. Dem Normalanwender war es daher nicht oder nur unter Schwierigkeiten möglich, einen sicheren Betrieb seines WLAN (Funknetz zum Internet) zu gewährleisten. Hacking, unzulässigen Downloads und Datenmissbrauch wurden damit Tür und Tor geöffnet. So hat denn auch eine im Auftrag von Frontal21 durchgeführte Untersuchung ergeben, dass bei bis zu 45 % von ca. 4000 in Deutschland überprüften DSL-Anschlüssen die Rechner direkt über eine öffentliche IP-Adresse erreichbar waren, also per DSL-Modem ungeschützt an das Internet angebunden waren. Eine rechtliche Handhabe zur Erzwingung technischer Sicherheit für die Käufer gab und gibt es aber nicht. Wichtig ist daher, dass die Hersteller und die für den Betrieb der Systeme verantwortlichen Unternehmen verpflichtet werden können, für eine sichere technische Grundausstattung zu sorgen.

Zugleich muss ein Wettbewerb entstehen, verständliche Benutzungshinweise und einfach zu bedienende Hard- und Software für die Anwender zu erstellen. Es muss möglich sein, auf einfache Weise ein für die eigenen Daten angemessenes Schutzniveau einstellen zu können. Die Hersteller von informationstechnischen Systemen müssen für Aufklärung sorgen, damit für den Einzelnen auch klar ist, welche Datenverarbeitungsprozesse im Hintergrund ablaufen. Nur wenn diese nachvollziehbar sind, kann der Einzelne beurteilen, ob er dies in Kauf nehmen will oder nicht. Die Anbieter müssen die Nutzer auch darüber informieren, welche Risiken mit der Nutzung von informationstechnischen Geräten oder der Inanspruchnahme von elektronischen Dienstleistungen verbunden sind. Eine umfassende Information und Beratung tragen dazu bei, Transparenz zu schaffen. Transparenz ist aber eine Voraussetzung für die eigenverantwortliche Wahrnehmung der informationellen Selbstbestimmung.

Eines ist unstrittig: Die Informations- und Kommunikationstechnik birgt das Potenzial zu einer totalen Überwachung. An immer mehr Stellen werden immer mehr Daten über uns gesammelt. Damit einhergehen eine zunehmende Überwachung, Registrierung, Bewertung sowie eine zum Teil unterschwellige Steuerung der Betroffenen. Die Rede ist hier nicht vom Überwachungsstaat, sondern von der „Überwachungsgesellschaft“. Diese Entwicklung ist aber weder unausweichlich noch steht sie mit einer freiheitlich verfassten Gesellschaft im Einklang. Datenschutz ist nicht einfach bloß der Schutz

von Daten, sondern der Schutz der informationellen Selbstbestimmung. Ein guter Datenschutz ist damit ein Garant für eine verfassungskonforme Informationsgesellschaft, die den Menschen im Vordergrund sieht und die Technik als ein Instrument zur Unterstützung seiner freien und selbstbestimmten Entfaltungsmöglichkeiten. Auch das gehört zum Schutz unserer verfassungsmäßigen Ordnung und solange die technische Entwicklung sich nicht selbst ausreichend in die Pflicht nimmt, muss die Gesellschaft für Erhalt oder Einführung notwendiger Rahmenbedingungen Sorge tragen.

1.6 Datenschutzrechtliche Gesetzesinitiativen

In Zentrum der Weiterentwicklung datenschutzrechtlicher Bestimmungen steht im Berichtsjahr nicht der öffentliche Bereich, auch wenn es hier z. B. durch die Änderungen im BKA-Gesetz oder im Personalausweisgesetz durchaus bemerkenswerte Weichenstellungen gegeben hat.

Auskunfteien-Regelungen: Ende Juli hat das Bundeskabinett einen Gesetzentwurf beschlossen, mit dem das Bundesdatenschutzgesetz (BDSG) um Regelungen zur Auskunfteientätigkeit ergänzt werden soll (BT-Drs. 16/10529). Neben der Schaffung eines spezifischen Erlaubnistatbestands für Datenübermittlungen an Auskunfteien ist dabei die erstmalige Regelung zum sogenannten Scoringverfahren von zentraler Bedeutung. Dabei handelt es sich um ein mathematisch-statistisches Verfahren zur Berechnung eines Zahlwertes, der Auskunft darüber gibt, mit welcher Wahrscheinlichkeit der Betroffene seinen finanziellen Vertragspflichten nicht nachkommen kann. Hierzu werden nicht nur Angaben über das tatsächliche Zahlungsverhalten sowie die Einkommens- und Vermögensverhältnisse der jeweils Betroffenen – soweit verfügbar – einbezogen, sondern auch soziodemographische Daten wie Alter, Wohnumfeld oder von Dritten angekaufte oder aus allgemein zugänglichen Registern entnommene Daten, wie zum Beispiel Kfz-Daten des Kraftfahrzeugbundesamtes. Auf der Grundlage dieses vielschichtigen Zahlenmaterials wird die Bonität des Einzelnen bewertet. Dem Betroffenen wird damit die Möglichkeit genommen, allein durch rechtstreues Verhalten sein Erscheinungsbild gegenüber Vertragspartnern zu beeinflussen. Insbesondere die Einbeziehung soziodemographischer Daten birgt die Gefahr, dass über den Betroffenen ein falsches Bild mit erheblichen nachteiligen Auswirkungen für die Bonitätswertberechnung entsteht. Für den Betroffenen muss daher wenigstens klar sein, welche Informationen mit welcher Gewichtung in einen Scorewert eingeflossen sind, nur so kann er bei einem negativen Scorewert ggf. Korrekturen anbringen. Der Gesetzentwurf sieht daher vor, dass die Informations- und Auskunftsrechte der Betroffenen ausgebaut werden.

Adresshandel-Regelungen: Nach dem sog. Datenschutzgipfel und vielem Hin und Her hat Anfang Dezember des Berichtsjahres die Bundesregierung reagiert und neben dem vorgenannten Gesetzentwurf einen weiteren Gesetzentwurf zur Änderung der Regelungen zum Adresshandel auf den Weg gebracht (BT-Drs-Nr. 4/09). Mit der Novellierung des Bundesdatenschutzgesetzes will die Bundesregierung aus den jüngst bekannt gewordenen Datenschutzverstößen im Bereich der Privatwirtschaft die Konsequenzen ziehen. Die uneingeschränkte Streichung des Listenprivilegs und die Pflicht zur Einholung einer Einwilligung des Betroffenen bei der Übermittlung seiner Daten an Dritte oder bei der Nutzung für Werbezwecke für Dritte sind erforderlich, um das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu stärken. Das habe ich sowohl mit der Konferenz der Datenschutzbeauftragten (vgl. Ziff. 20.10 dieses Berichts) wie auch mit den obersten Aufsichtsbehörden für den Datenschutz (vgl. Ziff. 21.5 dieses Berichts) in Entschlüssen bzw.

Beschlüssen angemahnt. Der Gesetzentwurf der Bundesregierung trägt dem allerdings nur bedingt Rechnung, löst zudem weitere Forderungen der Datenschützer, wie die Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren oder die lückenlose Dokumentation der Herkunft der Daten, nicht ein.

Arbeitnehmerdatenschutz-Regelungen: Medienberichten zufolge beschäftigen sich in den Betrieben mittlerweile ganze Abteilungen mit dem Aufspüren, Analysieren und Auswerten von Protokolldateien. Es ist bekannt, dass durch den Einsatz von Videotechnik, durch die elektronische Überwachung des E-Mail-Verkehrs und des Surfverhaltens, durch funk- oder biometriegesteuerte Zugangssysteme, durch Skill-Datenbanken und vieles mehr, Arbeitnehmer immer mehr einer feinmaschigen Kontrolle und Überwachung ausgesetzt sind. Die modernen informationstechnischen Systeme ermöglichen eine immer größere Überwachungsdichte, wobei die bislang zielgerichtete Überwachung von Arbeitnehmern zunehmend ungezielt und zeitlich wie räumlich allgegenwärtig wird. Dabei erfolgt sie häufig so subtil, dass sie von den Betroffenen weder in Art noch in Umfang erkannt wird. Rechtliche Regelungen sind zum Teil gar nicht oder nur verstreut an verschiedenen Regelungsorten vorhanden und wurden, was vielen Beschäftigten nicht bekannt ist, zum Teil erst durch Rechtsprechung ergänzt. Nach den derzeitigen Regelungen und der Rechtsprechung des Bundesarbeitsgerichts ist eine verdeckte Überwachung von Beschäftigten, sei es mit Videokameras, Überwachungssoftware o. ä., grundsätzlich nicht zulässig, weil sie deren Persönlichkeitsrecht erheblich verletzt. Viele Beschäftigte kennen ihre Rechte nicht und eine Kontrolle der Einhaltung bestehender Regelungen durch z. B. betriebliche Datenschutzbeauftragte findet oft nicht statt. Ich brauche dafür gar nicht auf den Fall Lidl zurückgreifen, meine Berichte der letzten Jahre unter der Rubrik „Videoüberwachung“ enthalten genügend Belege für diese Tendenzen. Wenn Beschäftigte von derartigen Überwachungen etwas erfahren, wenden sie sich sehr häufig nicht an mich, weil sie Angst davor haben, ihren Arbeitsplatz zu verlieren oder sonst im Betrieb benachteiligt zu werden. Es ist daher zu begrüßen, dass jetzt neben der seit Jahren bestehenden Aufforderung des Bundestages, gesetzliche Arbeitnehmerdatenschutzregelungen zu erarbeiten, durch eine Bundesratsinitiative erneut Bewegung in die Sache gekommen ist (BR-Drs. 665/08). Sie kommt allerdings wohl im Bund zu spät für diese Legislaturperiode.

1.7 Wenn das mal seine Adresse war

„Adressen, Adressen, Adressen, ich will, doch ich kann keine vergessen“, so mag der Computer einer Auskunftsei programmiert gewesen sein, als er als Vor-Voradresse die Anschrift der JVA in Bremen auswies und deshalb der ehemalige Strafgefangene eine unbedingt benötigte behindertengerechte Wohnung nicht bekam. Auch die unter der in den USA geführten Internetseite „Rotten Neighbor“ könnte durchaus für Mietsuchende nachteilige Auswirkungen haben. Dort sind zum Teil widerwärtige Informationen über eine Vielzahl Bremer Bürger hinterlegt (Näheres vgl. Ziff. 4.6 dieses Berichts). Jüngere Stimmen in der Literatur meinen, Privatheit und auch das damit verbundene informationelle Selbstbestimmungsrecht seien Relikte des zwanzigsten Jahrhunderts. Dem ist zu entgegnen: Auch unsere Verfassung ist aus dem vergangenen Jahrhundert, ja, und sie ist auch mit Blick auf die sich verändernden gesellschaftlichen Umstände immer wieder neu zu interpretieren, aber ein Verzicht auf diese Werte kommt wohl nicht infrage. Die Kontrolle über die als „eigene Bereiche“ eingestuftes Angelegenheiten ist nicht nur in der eigenen Wohnung, sondern auch – wie der Fall des Mietsuchenden zeigt – im Bereich der personenbezogenen Daten außerordentlich wichtig.