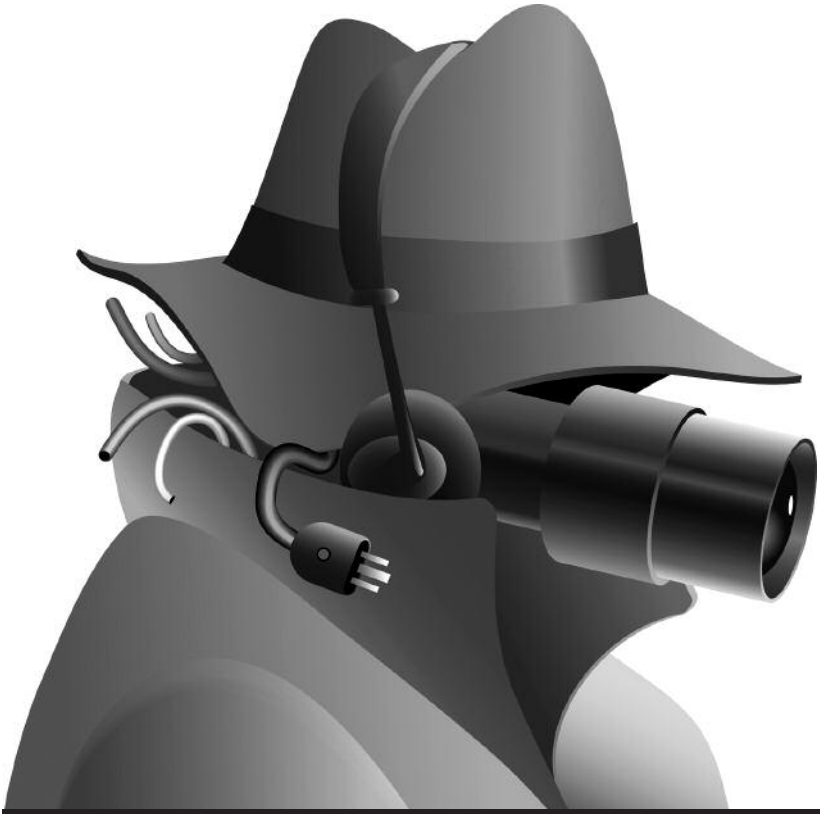
TAUWETTER

... franziskanische Zeitschrift für Gerechtigkeit, Frieden und Bewahrung der Schöpfung



Big brother is watching me

Zwischen Freiheit und Sicherheit

| Nr. 4 | Dezember 2009 | 24. Jahrgang | ISSN 1618-0550 |

IMPRESSUM

Redaktion Tauwetter

Peter Amendt ofm, Stefan Federbusch ofm, Markus Fuhrmann ofm, Jürgen Neitzert ofm,
Verantwortlich im Sinne des Presserechts: Jürgen Neitzert ofm, Köln

Sie erreichen uns

Redaktion Tauwetter
Immermannstr. 20
Postfach 24 01 39
40090 Düsseldorf
Redtauwetter@aol.com
www.tauwetter-online.de

Dankeschön

Tauwetter finanziert sich ausschließlich aus Spenden.
Wir möchten uns an dieser Stelle ausdrücklich bei allen bedanken, die mit ihrem Beitrag diese franziskanische Zeitschrift mit dem Schwerpunkt „Gerechtigkeit, Frieden und Bewahrung der Schöpfung“ unterstützen.

Redaktion Tauwetter
Stadtsparkasse Düsseldorf (BLZ 300 501 10)
Kontonummer: 10 130 896
IBAN: DE 43 3005 0110 0010 1308 96
SWIFT/BIC: DUSSDEDDXXX

Editorial

Der 11. September 2001 markiert einen Einschnitt in der Frage von Bürgerrechten und Sicherheit. Nach den Anschlägen islamistischer Terroristen in den USA wurden in der Folge von zahlreichen Staaten eine Fülle von Sicherheitsgesetzen erlassen, die eine Einschränkung der Bürgerrechte mit sich brachte. Im Gegensatz zu anderen europäischen Staaten sind wir in Deutschland bislang von größeren Anschlägen verschont geblieben. Keines der großen Sicherheitsgesetze ist ohne Bedenken der jeweiligen Opposition verabschiedet worden, keines ist ohne Überprüfung durch das Bundesverfassungsgericht geblieben.

Da es sich um einen Grundwertekonflikt zwischen Freiheit und Sicherheit handelt, ist die sinnvolle Balance zwischen diesen Werten immer wieder auszuhandeln und auszutarieren. Aus der franziskanischen Perspektive ist zu fragen, welche Schritte tatsächlich zu Gerechtigkeit und Frieden führen.

Die Beiträge dieser Tauwetter-Ausgabe gehen dem in drei Facetten nach: der erste Artikel verdeutlicht den grundlegenden Wandel im Verständnis und im Umgang mit Privatsphäre, der durch die Nutzung der neuen Medien anzutreffen ist. Der zweite stellt in Form einer Glosse dar, wie stark wir als Bürger bereits der Überwachung unterliegen. Der dritte betrachtet die verschiedenen Sicherheitsgesetze der letzten Jahre und wirft einen kritischen Blick auf den Datenschutz. Die Artikel wurden bereits vor der Bundestagswahl verfasst, haben aber durch die Koalitionsvereinbarungen eine neue Aktualität bekommen.

Zur Weihnachtszeit legen wir wieder einen Spendenbeleg bei. Tauwetter ist kostenlos, doch bitten wir um Spenden, um Druck und Versand unserer nächsten Ausgaben zu ermöglichen. Ein herzliches Vergelt's Gott allen, die uns dabei helfen.

Die Tauwetter-Redaktion wünscht allen Leserinnen und Lesern ein frohes und gesegnetes Weihnachtsfest sowie einen guten Start ins Jahr 2010!

Mit Franziskus pax et bonum – Frieden und viel Gutes!

Inhalt

Selbstinszenierung in der virtuellen Welt

Von der freiwilligen Aufgabe der Privatsphäre

Stefan Federbusch ofm

Die Frage „Wer bin ich und was macht mich aus?“ gehört zu den grundlegenden Fragen jeder menschlichen Biografie. Eine Identität bekommt der Mensch dabei nicht qua Geburtsurkunde mitgeliefert, sondern muss sie sich im Laufe seines Lebens erarbeiten und immer wieder neu gestalten. Identität bildet sich u.a. durch die verschiedenen Rollen, die ich „spiele“ oder die andere mir zuschreiben. Im Rahmen einer multioptionalen Gesellschaft ist jeder herausgefordert, sich seine eigene Bastelbiografie zu erstellen. Jede Rolle ist dabei eine gewisse Inszenierung auf der Bühne des Alltags. Ich spiele die Rollen, um ich selbst zu sein. Diese Selbstdarstellung ist Grundlage des sozialen Vertrauens. Wieweit sie eher auf privater oder eher auf öffentlicher Bühne stattfindet, bleibt mir selbst überlassen. Feststellbar ist jedoch, dass sich bestimmte Darstellungsformen in den letzten Jahren zunehmend in die Öffentlichkeit verlagert haben. In den diversen Castingshows des Fernsehens (Deutschland sucht den Superstar, Germans Next Topmodel usw.) lässt sich beobachten, welche Anstrengungen Menschen unternehmen und was sie alles mit sich machen lassen, um sich eine vermeintliche Identität zu beschaffen.

Schutz der Privatsphäre im Grundgesetz

Den Vätern (und Müttern) des Grundgesetzes war nach der Erfahrung der NS-Diktatur der Schutz der Privatsphäre ein hohes Gut. Die Grundrechte sehen einen weitgehenden Schutz der persönlichen Belange vor (Briefgeheimnis, Unverletzlichkeit der Wohnung usw.). Derzeit scheinen wir in einer Phase, in der viele bereit sind, ihren Persönlichkeitsschutz freiwillig aufzugeben und die virtuelle Welt als öffentliche Bühne zu bespielen. Wo diese Entwicklung hinführt und welche Folgen sie hat, bleibt abzuwarten.

Die virtuelle Welt als Bühne der Selbstinszenierung

In der Öffentlichkeit der virtuellen Welt lautet die Maxime: „broadcast yourself". Internet-Portale wie YouTube, SchülerVZ, StudiVZ und MySpace sind die neuen Bühnen der Selbstinszenierung. Sie zeigen uns die derzeitigen Formen einer öffentlichen Zurschaustellung von Identität. Dabei geht es weniger darum, das „wahre" Selbst zu entdecken als mehr darum, ein interessantes Selbst zu erschaffen. Für viele junge (und nicht mehr ganz so junge) Menschen ist die virtuelle Welt zu ihrer zweiten Natur geworden. Ihr Denken und Fühlen bewegt sich in dieser Welt. Positiv lässt sich konstatieren, dass das Internet zu einer neuen und intensiven Kommunikationsplattform geworden ist, das zu einem regen Austausch genutzt wird. Durch die negative Brille betrachtet signalisieren sie den Trend zu Exhibitionismus und Voyeurismus als neuen Megatrend. Die jüngeren Menschen können mit Intimität und Privatsphäre im klassischen Sinn nicht mehr viel anfangen. Dass das Internet eine gefährliche Bühne darstellt, die auch zum Schaden der Nutzer ausfallen kann, scheint sie nicht weiter zu stören. Es ist hinreichend bekannt, dass sich Personalchefs bei Bewerbungen gerne einen Überblick verschaffen, was sich im Internet über die betreffende Person findet (etwa bei 123people.de). Bilder von wilden Partys und anderen persönlichen Ereignissen sind dann nicht gerade von Vorteil.

Selfmarketing via Internet

Jeder Mensch hat Bedürfnisse und Wünsche. Bedürfnisse lassen sich mittels Konsums rasch erfüllen (für die meisten jedenfalls). Bedürfnisse rangieren auf der ökonomischen Ebene. Mit Wünschen ist es schon schwieriger, da sie eher psychologischer Natur sind. Der letztlich tiefste Wunsch ist der nach Anerkennung. Dafür tun Menschen sehr viel und gehen sie bewusst oder unbewusst sehr weit, manchmal zu weit. Als soziale Wesen bekommen wir Anerkennung nur von Anderen, sind auf andere diesbezüglich angewiesen. In unserer Gesellschaft geht der soziale Trend eher dahin, unverwechselbar zu sein. In unserer globalisierten Welt finden wir zwar einerseits sehr gleichmachende Konsummuster wieder (fast jeder Jugendliche geht zu McDonalds), andererseits fördert sie die Individualisierung. „I want to make a difference", sagen die Amerikaner. Es soll etwas geben, was mich von anderen unterscheidet. Das Selbstwertgefühl bildet sich aber daraus, wie Andere mich beurteilen. Also muss ich etwas tun, das von Anderen – wenn schon nicht bewundert, aber doch – anerkannt wird. Im Bereich der Arbeit wird Selfmarketing die Bedingung für geschäftlichen Erfolg. Je nachdem, wie gut ich mich verkaufen kann, wird sich dies auf meine Karriere und mein Einkommen auswirken. Sich zur eigenen Marke zu machen, ist die Kunst, die Kinder und Jugendliche heute in der virtuellen Welt lernen. Die sozialen Netzwerke im Internet dienen der eigenen Positionierung. Was in dieser Welt geschieht wird für manche wichtiger als das, was in der realen Welt läuft.

Gefahren des Datenmissbrauchs

Im Juli 2009 haben die Verbraucherzentralen mehrere soziale Netzwerke im Internet wegen Datenschutzmängeln abgemahnt. Die Plattformen Facebook, Lokalisten, Myspace, Wer-kennt-wen und Xing benachteiligten ihre Nutzer, kritisierte der Bundesverband der Verbraucherzentralen in Berlin. Deshalb forderten die Verbraucherschützer sie zu Unterlassungserklärungen auf und zur Verbesserung der Standards. Die Anbieter müssten sicherstellen, dass Daten nur verwendet werden, wenn die Nutzer auch einwilligen. Während der Anbieter Facebook die

Kritik zurückwies, hat das Karriereportal Xing daraufhin sofortige Veränderungen angekündigt. Forenbeiträge von Ex-Mitgliedern würden gelöscht. Auch sei man bereit, die Allgemeinen Geschäftsbedingungen gemäß den Forderungen zu aktualisieren.

Dass die Kritik berechtigt war, zeigte sich im Oktober 2009, als ein 20-Jähriger aus Erlangen die Daten von über 1 Mio. Nutzern des Internet-Netzwerks SchülerVZ kopiert und illegal weiter gegeben hat. Vom Betreiber des Netzwerks versuchte er, 80.000 Euro zu erpressen. Er hatte auch Daten von StudiVZ und MeinVZ-Teilnehmern gesammelt, aber noch nicht veröffentlicht. Die Daten hatte der Mann dem Blog Netzpolitik.org zukommen lassen. Dessen Gründer informierte VZnet, den Betreiber von SchülerVZ. Bei einem Treffen in Berlin konnte der Täter festgenommen werden. Zehn Tage später nahm er sich in der Jugendstrafanstalt Plötzensee das Leben.

Ein zwitschernder Ausblick

Microsoft verkündete am 22. Oktober 2009, dass es künftig auch die Nachrichten von Twitter- und Facebooknutzern in seine Suchmaschine Bing aufnimmt. Kurz darauf zog auch Google nach. Junge Inter-netnutzer messen die Relevanz einer Information nach Untersuchung des Harwardprofessors Urs Gasser (in seinem Buch „Generation Internet“) weniger an der Quelle, denn an dem, was in ihrer Facebookgruppe gelesen und geschrieben wird. Bislang existiert nur eine Betaversion von Microsoft unter bing.com/twitter. Kriterien für den Suchfilter sind die Popularität des Twitterers (die Zahl seiner sogenannten Follower / Beobachter), die Zahl der Weiterleitungen (Retweets) und die Aktualität des Tweets (= jüngste Twitter-Einträge).

Twittern bedeutet zu deutsch „zwitschern“. Die Bezeichnung rührt daher, dass es sich um kurze Beiträge von maximal 140 Zeichen handeln. Zentrales Prinzip von Twitter ist, dass jeder die Beiträge anderer abbonieren kann. Er findet sie in seinem Twitterpostfach vor und ist so ständig auf dem Laufenden. Durch diesen Netzwerkcharakter lassen sich Informationen blitzschnell verbreiten. Die Internetseite twitter.com ist

eine der 50 populärsten Seiten weltweit und hat nach eigenen Angaben ca. 24 Millionen Nutzer. Twitter wurde 2006 von dem Softwareentwickler John Dorsey gegründet und hat seinen Firmensitz in San Francisco. Er wollte wissen, was seine Freunde gerade so machen. Ursprünglich war Twitter etwas für „Internet-Junkies". Der typische Nutzung ist 32 Jahre alt, männlich, hat Abitur und arbeitet in der Medien- und Werbebranche. Unter Jugendlichen ist Twitter noch relativ unbekannt. Dies dürfte sich in Kürze ändern. Barack Obama nutzte es im Präsidentschaftswahlkampf 2008. Zunehmend nutzen auch Firmen Twitter, um ihre Kunden über neueste Produkte zu informieren. Die australischen Behörden versandten über Twitter Warnungen vor den großen Buschbränden. Während der Unruhen im Iran im Nachgang zu den Präsidentschaftswahlen bekam Twitter eine wichtige politische Bedeutung als ungefilterter Nachrichtenkanal.

Bisher verzichtet der Mikro-Blogging-Dienst auf Gebühren und Werbung. Er sammelt allerdings Namen und Emailadressen der Nutzer und behält sich vor, diese zu vermarkten. Sollte Twitter einmal aufgekauft werden, gehören auch die Datensätze zur Verkaufsmasse. Die Nutzer könnten eines Tages mit Werbung in ihren Emailfächern zugeschwemmt werden.

Ob Twittern nun dumm macht, weil die Kurzmeldungen das Gedächtnis unterfordern oder die Kreativität durch das ständige schreiben und Kommunizieren fördert, wird die Zukunft erweisen. Zumindest trägt es (wie das Internet und das Handy) sowohl zur Veränderung unserer Gehirnstrukturen als auch unserer Zeitstrukturen im Sinne der Beschleunigung bei.

„Big brother is watching me“

Von der Freiheit und dem informellen Selbstbestimmungsrecht eines „Normal“-Bürgers in Deutschland

Eine Glosse

Stefan Federbusch ofm

Als freier Bürger habe ich die Möglichkeit, mich unsichtbar und unhörbar zu machen. Allerdings nur, wenn ich darauf verzichte, am gesellschaftlichen Leben teilzunehmen und auf Kommunikation unter zu Hilfenahme von Technik. Somit dürfte ich diesen Artikel nicht schreiben, denn der wird zunächst per Mail verschickt, um dann als Veröffentlichung in einer Zeitschrift auch im Internet zu landen.

Lassen wir einen normalen („virtuellen“) Tag Revue passieren:

Angenommen ich hätte ein HANDY (dem ich mich noch widersetze, aber wer weiß wie lange noch), so verriete es unentwegt meinen Aufenthaltsort (sofern ich es mit mir führe). Ich schalte es also ein, da ich einen wichtigen Anruf erwarte. Betriebsbereite Handys übertragen unentwegt an die Basisstation des Netzbetreibers ihre Kennung und Kartennummer. Meine Verbindungen und die Gesprächsdauer dürfen die Telefongesellschaften zu Abrechnungszwecken maximal sechs Monate speichern. Eine Europäische Richtlinie will die Telekommunikations- und Internetdienste nun verpflichten, diese Daten für die Strafverfolgungsbehörden zu speichern, selbst wenn keinerlei unmittelbare Gefahr droht. Der Europäische Gerichtshof prüft derzeit die Rechtmäßigkeit. Kleiner Tip: Nutzen Sie Ihr Handy am besten als Wecker. Es könnte Ihnen als Alibi dienen, nachts daheim gewesen zu sein (zumindest nicht mit ihrem Mobiltelefon unterwegs). Am besten wählen Sie noch UMTS, das macht Ihr Handy besonders gut ortbar.

Da ich jetzt in Hessen wohne, kann mein Telefonanschluss auch per richterlicher Anordnung im Rahmen einer präventiven TKÜ (Telekommunikationsüberwachung) kontrolliert werden. Bundesweit sind 2005 exakt 34.855 Überwachungen für Mobilfunktelefone und 5.398 für Festnetzanschlüsse genehmigt worden. Im Vergleich zu 1995 immerhin eine Steigerung um 600 Prozent!

Theoretisch könnte ich auch von einem so genannten „Imsi-Catcher" erfasst werden, deren Einsatz das Bundesverfassungsgericht im Oktober 2006 als verfassungskonform gebilligt hat. Diese Geräte simulieren die von Handys benötigte Basisstation und erfassen die vom Handy ausgesandten Signale. Dadurch kann der Aufenthaltsort eines Verdächtigen bestimmt werden. Möglich ist es auch, die Telefon- und SIM-Karten-Nummer eines Beschuldigten aus dem Mobiltelefon auszulesen. Nach Angaben der Bundesanwaltschaft setzte sie den Imsi-Catcher seit 2002 viermal ein. Zugegebenermaßen nicht gerade häufig. Das Problem an der Technik ist, dass im Umkreis auch die Handy-Daten Unverdächtiger auf den Catcher umgeleitet werden und die über die Nummer ermittelten Namen der Besitzer abgeglichen werden.

Am Vormittag mache ich mich auf den Weg, um meinen Wohnsitz umzumelden. Dies wird umgehend die GEZ über das Einwohnermeldeamt erfahren. Sie kann dort meinen Datensatz abfragen, zu dem Familienname, Vorname, frühere Namen, Geburtstag, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs und der Familienstand gehören. Ziemlich viel!

Zur Fahrt zum Einwohnermeldeamt nutze ich den öffentlichen Nahverkehr. Das Ticket für die S-Bahn zahle ich bar, könnte es aber ebenso per EC-Karte. Dies würde eine weitere Datenspur legen, nämlich die zu meinem Konto. Diese Spuren ergeben sich eh in jedem Geschäft, in dem ich per Plastikkärtchen zahle. Onlinebanking ist mittlerweile für viele zur Routine geworden.

Wie viele Kameras mich auf meinem Weg von Zuhause bis zum Einwohnermeldeamt aufgenommen haben, wird ihr Geheimnis bleiben. Ihre Zahl in Bahnhöfen und auf öffentlichen Plätzen hat durch den vermeintlichen Terrordruck jedenfalls enorm zugenommen. Was lässt

sich schon dagegen einwenden, sie dienen ja einem gutem Zweck und meinem Schutz.

Schließlich wurde der Libanese Jussif Mohammed E. (der mit seinem Komplizen die Kofferbomben in einem Nahverkehrszug versteckte) durch die Überwachungskamera im Kölner Hauptbahnhof überführt und durch die Verbreitung der Bilder in den Medien nervös. Er telefonierte mit seinem Handy nach Hause und wurde dabei vom libanesischen Geheimdienst abgehört. Einige Stunden später konnte er am Kieler Hauptbahnhof festgenommen werden. Dem Ruf nach noch mehr Videoüberwachung ist kaum zu widerstehen.

Vielleicht sollte ich mal wieder nach Leipzig fahren. Der dortige Bahnhof hat mir imponiert. Was 1996 mit der Videoüberwachung des Bahnhofgeländes begann, dehnt sich mittlerweile auf zwei Drittel (!) der Innenstadt aus. In Regensburg startete 2000 ein Modellversuch mit fest installierten Kameras an sieben ausgewählten Plätzen, in Bielefeld wird seitdem ein Park mit vier Kameras überwacht. Seit 2001 wird in Mannheim gefilmt, seit 2004 in Mönchengladbach, seit März 2006 auf der Reeperbahn in Hamburg.

Ein neuer Reisepass muss her, da der alte abgelaufen ist. Er ist mittlerweile nur noch in der biometrischen Variante zu haben. Ein digitales Gesichtsbild und meine Personendaten sind auf einem RFID-Chip (Radio Frequenca Identification) gespeichert, der theoretisch auch per Funk lesbar ist. Ab März 2007 kamen noch zwei digitalisierte Fingerabdrücke dazu. Die Überlegung, die Brüder in den USA zu besuchen, beinhaltet, dass die US-Behörden damit Zugriff auf ein Datenset aus 34 Elementen bekommen (inklusive Kreditkartennummer), das sie direkt über das Buchungssystem der Fluggesellschaften abrufen können. Dreieinhalb Jahre lang werden diese Daten gespeichert.

Nun bin ich ein „armer" Franziskaner, aber als reicher Mensch könnte es mir passieren, dass mir meine Bankdaten schon mal vorausreisen. Der letztjährige Big-Brother-Preisträger in der Kategorie Wirtschaft, die Swift (Society for Worldwide Interbank Financial Telecommunikation) stellt seit fünf Jahren den US-Behörden die Daten internationaler Banktransaktionen zur Verfügung. Herausgefunden hat dies

unlängst die New York Times. Aber gut, in diesem Bereich ist bei mir wenig zu wollen.

Auch im nächsten Bereich bin ich eher resistent. Noch ein schneller Einkauf am Mittag im großen Shoppingcenter. „Haben Sie eine Kundenkarte?“ Nein, habe ich nicht! Pech für mich, damit entgehen mir wichtige Bonus-Punkte. Pech auch für die Marktforschungsunternehmen, die nun schwieriger nachvollziehen können, wie mein Kaufverhalten ist (und mich daher auch nicht mit Angeboten überziehen, an denen ich eh kein Interesse habe). Es reicht ja schon, wenn ich die Bahncardpunkte sammle und der Deutschen Bahn AG verrate, wie mein Fahrverhalten ist (und dazu beitrage, dass sie Aktiengesellschaft werden kann).

Außerdem nutze ich eine gmx-Emailadresse, die mir der Anbieter freundlicherweise kostenlos zur Verfügung stellt. Für die Nutzung gibt es zur Belohnung zielgerichtete Werbung, ganz nach meinen persönlichen Interessen, die in meinem Nutzerprofil abgefragt worden sind. Also schnell wieder an den Computer und die Mailabfragen tätigen. Dutzende von Spams lassen grüßen und den Genervtheitspegel leicht höher steigen. Ist es nicht schön, derart viel Post zu bekommen! Noch ein Surfing durchs Internet, um die Datenspur etwas zu verbreitern und die Infos in diesen Artikel einfließen zu lassen. Ich könnte auch noch eben bei Ebay mitsteigern oder mit Chatroom meine Meinung kundtun. Was soll ich mir die Mühe machen, all die Cookies zu löschen, die meine Wege durchs Internet dokumentieren.

Der Griff in den Briefkasten fördert mehrere Bettelschreiben unterschiedlicher Organisationen zutage. Und das (wenig) Erstaunliche: Alle haben sie bei meinem Namen denselben Buchstaben falsch geschrieben. So ein Zufall! Da hat wieder jemand Adressen verkauft, ohne mein Einverständnis einzuholen. Wozu auch, ist (bzw. war) ja rechtens.

Am späten Nachmittag ein Arzttermin. Ich nutze das Auto. Der Stopp an der Tankstelle ist unvermeidlich. Auch hier ein freundliches Lächeln für die Überwachungskameras und die Sache mit dem Plastikkärtchen zum Bezahlen hatten wir ja schon. Die Kamera im Parkhaus sei hier nur noch der Vollständigkeit halber erwähnt.

Lang wird es nicht mehr dauern, bis ich durch das Gesundheitswesen zum gläsernen Patienten geworden bin. Meine Krankenkassenkarte wird meine Krankheitsgeschichte erzählen und es dem Arzt angeblich leichter machen, mich medizinisch bedarfsgerecht zu behandeln.

Da das satellitengestützte Navigationssystem sowieso verrät, wo ich mich mit meinem Auto gerade mobil bewege (zusätzlich könnte dies über die Mautstellen erfasst werden, wie es Politiker zur Kriminalitätsbekämpfung bereits vorgeschlagen haben), spricht doch eigentlich nichts dagegen, gleich allen Bürgern einen Mikrochip einzupflanzen, mit dem sie geortet werden können. Das ist zumindest praktischer als die altmodische elektronische Fußfessel. Und mein Provinzial wüsste jederzeit, wo ich mich aufhalte!

Ins Museum könnte ich auch mal wieder gehen (und mich dort „sehen" lassen) und morgen ist Samstag: Ein Live-Spiel im Bundesligastadion ist was Feines. Die Fanüberwachungskameras der Polizei werden sich freuen, dass ich keinen Krawall gemacht habe.

Wie gesagt: alles in allem ein ganz normaler (Überwachungs-) Tag.

„Elektronisches Panoptikum", nennt der Soziologe Ronald Hitzler von der Universität Dortmund das umfassende Netz optischer Apparate und Analyseprogramme, die unser Leben sichten und scannen, Spuren sichern und Daten sammeln. „Das elektronische Panoptikum impliziert nicht einfach das Sammeln von Informationen im Allgemeinen oder das an Neuigkeitswert orientierte Suchen nach Informationen, sondern meint auch die Praxis des unmittelbaren und direkten Erfassens und Speicherns von Daten, um in irgendeiner Weise *Kontrolle* über einen Menschen auszuüben", so Hitzler.

Was waren das doch für glorreiche Zeiten, als 1981 die Volkszählung durchgeführt werden sollte. Ein Aufstand quer durch die Republik. 33 Fragen wurden den Bürgern vorgelegt, angefangen vom Alter, über den Beruf bis zur Fläche der Wohnung und der Höhe der Miete. Etliche Jahre musste die Volkszählung verschoben werden, weil das Bundesverfassungsgericht sie zunächst verhinderte. Erst 1987 fand sie schließ-

lich statt. „Als sei es des Teufels eigenes Werk“, lautete die Spiegel-Titelstory vom 18. Mai 1987.

Was haben sich die Zeiten doch gewandelt. Vom verteufelten „Überwachungsstaat“ wird heute genau das gefordert. Big brother is watching me! Es lebe die Freiheit!

Freiheit und Sicherheit

Über ein schwieriges rechtsstaatliches Spannungsgefüge

Stefan Federbusch ofm

Derzeit geht es in der Gesetzgebung um zwei Rechte, die beide in sich ein hohes Gut darstellen: das Gut der Freiheit und das Gut der Sicherheit. Beide Rechte hat der demokratische Staat sicher zu stellen. Dabei kommt es zwangsläufig zu einer Güterabwägung. Seit dem 11. September 2001 scheint das Pendel stetig weiter zugunsten des Rechts auf Sicherheit auszuschlagen. Kein Politiker möchte sich zurecht dem Vorwurf ausgesetzt sehen, er hätte nicht genug für die Sicherheit seiner Bürger getan. Wenn etwas Gravierendes passiert, ist der Aufschrei groß. Andererseits gilt: die Freiheit zu wahren und zu verteidigen ist eine zentrale Verpflichtung des Bürgers. Zumal dann, wenn sich die Präventionsmaßnahmen des Staates als unverhältnismäßig erweisen. Dieser Eindruck wird durch die Urteile des Bundesverfassungsgerichtes bekräf-

tigt, das zahlreiche Sicherheitsgesetze der vergangenen Jahre als nicht grundgesetzkonform zurückgewiesen hat. Auch der wachsamste Staat kann letztlich Terror und Opfer von Gewalttaten nicht verhindern. In gewissem Sinne sind sie der Preis der Freiheit. Es gibt keine letzte Sicherheit gegen Lebensrisiken. Insofern ist die Balance zwischen den Erfordernissen der Sicherheit und den Notwendigkeiten der bürgerlichen Freiheiten immer wieder neu auszutarieren.

Eine Frage des Menschenbildes

Hinter der ganzen Debatte verbirgt sich (auch) eine Frage des Menschenbildes. Das Grundgesetz billigt jedem Bürger Grundrechte zu. Vor dem Gesetz ist auch der „Terrorist" ein „Bürger" mit Grundrechten. In der allgemeinen gesellschaftlichen und politischen Debatte wird er nur noch als „Feind" wahrgenommen. Natürlich stellt Terrorismus eine Bedrohung des Staates (und der Demokratie) dar, dennoch darf ein „Terrorist" nicht ausschließlich als „Feind" angesehen und behandelt werden. Die Grenze, dem „Feind" die Menschenrechte abzuerkennen, ist sonst nicht mehr weit. Guantánamo ist dafür das unrühmliche Beispiel. Die Nation, die sich am meisten der Verteidigung der Freiheitsrechte rühmt, teilt die Menschheit in bezug auf die Menschenrechte in zwei Klassen. Denjenigen, die aus ihrer Sicht gegen die Freiheit „bomben" und morden, gesteht sie keine Grundrechte zu.

Einschränkung der Grundrechte

Im Namen der Freiheit werden die Grundrechte der persönlichen Freiheit der Bürger derzeit in der Bundesrepublik Deutschland immer weiter eingeschränkt. Das allgemeine Klima und das Argument der Sicherheit nimmt viel vom möglichen Widerspruch. Rasterfahndung, Abhörmaßnahmen, Videoüberwachung, Kontaktsperre, Einsatz der Bundeswehr im Inneren, Erfassung biometrischer Daten, Online-Überwachung, Speicherung von Telefondaten usw.. Bei all diesen Maßnahmen geht es um den staatlichen Einsatz gegen gefährliche Täter, gegen Feinde, gegen die terroristische Bedrohung. Es führt jedoch nichts an der

Erkenntnis vorbei, dass die Zunahme staatlicher Präventionsmaßnahmen die Freiheit des (unschuldigen) Bürgers zunehmend einschränkt. Und was einmal Gesetz geworden ist, wird so schnell nicht wieder aufgegeben.

Datenschutz

Mit dem Volkszählungsurteil vom 15. Dezember 1983 hat das Bundesverfassungsgericht Rechtsgeschichte geschrieben. Damals begann der Datenschutz.

Im Abwägen zwischen terroristischer Bedrohung und Schutz der Grundrechte hat das Bundesverfassungsgericht der Privatsphäre stets einen hohen Stellenwert zugesprochen und damit allzu massive Eingriffe in die Rechte der Bürger verhindert.

Ein Blick auf die Gesetze und Maßnahmen der letzten Jahre:

Elektronische Personalausweise und Pässe

In Zukunft wird es einen elektronischen Personalausweis im Scheckkartenformat geben. Ursprünglich sollte er bereits zum 1. Januar 2009 eingeführt werden. Das Gesetz über den neuen Ausweis wird sich aber bis ins Jahr 2009 verschieben. Nach Auffassung der Unionsparteien gehören in diesen Ausweis verpflichtend die Fingerabdrücke analog zum Reisepass. In elektronischen Reisepässen werden seit November 2007 außer einem biometrischen Bild auch die Fingerabdrücke registriert. Dies hat der Bundesrat im Juni 2007 beschlossen. Bei den Meldeämtern werden die Abdrücke des rechten und linken Zeigefingers genommen. Sie werden aber nur auf dem Chip des Reisepasses gespeichert und bei den Passbehörden wieder gelöscht. Die SPD ist gegen Fingerabdrücke im Personalausweis. Bundesinnenminister Wolfgang Schäuble (CDU) und Bundesjustizministerin Brigitte Zypries (SPD) haben sich im Juni 2008 verständigt, dass es den Bürgern frei steht, ihre Fingerabdrücke abzugeben. Zypries hält die Verpflichtung für einen unangemessenen Eingriff in die Grundrechte der Menschen.

Was die Fälschungssicherheit angeht, entsprechen die derzeitigen Personalausweise einem hohen Standart. Von den 62 Mio. Ausweisen, die derzeit im Umlauf sind, wurden zwischen 2001 und 2007 nur 495 gefälscht.

Ein neues Grundrecht

Lange Diskussionen gab es um das neue „Bundeskriminalamtsgesetz" (BKAG), insbesondere um die sogenannten „Online-Durchsuchungen" von Computern. Dabei geht es um das heimliche Kopieren der gesamten Festplatte eines Computers. Mit dieser Art der Online-Überwachung können sämtliche Aktivitäten des Nutzers eines Rechners protokolliert werden. Dies ermöglicht den Zugang zu sämtlichen gespeicherten Daten inklusive Passwörter und Codes zur Verschlüsselung von Daten. Ende Februar 2008 stellte das Karlsruher Bundesver-fassungsgericht hohe rechtliche Hürden für diese Art der Kontrolle auf. Als Voraussetzung für den Geheim-Check von Festplatten müsse eine konkrete Gefahr für Leib, Leben und Freiheit bestehen sowie für „Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt". Ein abstraktes Risiko terroristischer Anschläge allein rechtfertigt damit eine Online-Durchsuchung noch nicht. Solange keine Hinweise auf konkrete Anschlags-pläne auf den öffentlichen Raum vorliegen, darf dieses Mittel nicht zum Einsatz kommen. Zudem ist eine richterliche Anordnung erforderlich.

Die Karlsruher Richter haben nach dem Urteil zur Volkszählung (Grundrecht auf informelle Selbstbestimmung) erneut ein komplett neues Grundrecht geschaffen: das Grundrecht auf Schutz des persönlichen Computers oder wie es juristisch korrekt heißt: „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme". Sie haben mit ihrem Urteil auch eine bisherige „Schutzlücke" geschlossen. Es weitet das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme vom Personal-Computer auf mobile technische Geräte wie Smartphones und Taschen-PCs (PDA) sowie alle internetfähigen Alltagsgeräte aus. Geschützt ist fortan nicht nur die eigene Wohnung, sondern auch die virtuelle Privatsphäre.

Das Gesetz bedarf der Zustimmung der Länder. Es soll deren Kompetenzen unberührt lassen. Dafür sind umfassende Abstimmungen zwischen Bund und Ländern vorgesehen. Nach dem vorliegenden Gesetz darf die entsprechende Wohnung vorher nicht betreten werden. Die SPD hatte den Einbruch in Wohnungen zur Installation von Spähprogrammen abgelehnt.

Laut Gesetz dürfen „Trojaner" zum Ausspähen des Computers nur von außen – per E-Mail-Anhang auf den Rechner des Verdächtigen gespielt werden. Dazu Sachsen-Anhalts Innenminister Holger Hövelmann (SPD): „Da wäre ein Krimineller schon sehr dämlich, wenn er einen E-Mail-Anhang mit einem Bundestrojaner öffnen würde."

Technisch ist es nicht schwer, sich vor dem staatlichen Online-Zugriff zu schützen; das haben auch BKA-Vertreter schon einräumen müssen. Es genügt beispielsweise, als Betriebssystem eine Linux-Variante zu wählen, die sich von CD-Rom starten lässt. Bei so einem schreibgeschützten Datenträger laufen alle Versuche dauerhafter Infiltration ins Leere.

Die Überprüfung ist damit nicht nur technisch schwierig und langwierig, sie erhöht auch die Gefahr, einen unverdächtigen PC-Nutzer zu erwischen. Zudem ist unverständlich, wieso es erlaubt war, in das Haus der Terrorverdächtigen im Sauerland einzubrechen und eine Chemikalie auszutauschen und es erlaubt ist, Kameras für den „Großen Spähangriff" einzubauen, während es verboten ist, in eine Wohnung einzudringen, um auf dem garantiert richtigen Computer das Spionageprogramm zu installieren.

Damit ist der zweite große Streitpunkt benannt: Die erweiterten Befugnisse der Sicherheitsbehörden bei der Wohnraumüberwachung. Wohnungen von Verdächtigen dürfen zukünftig nicht mehr nur per Wanze, sondern auch per Minikamera ausgespäht werden. Betroffen sind davon auch unbescholtene Bürger, wenn in ihrer Wohnung Verdächtige verkehren.

Ein solches Gesetz käme beispielsweise zur Anwendung im Fall der Terrorzelle vom September 2007 im Sauerland. Islamisten um den Deut-

schen Fritz G. hatten in einem Haus Fässer zur Sprengstoffherstellung gelagert. Um ein elektronisches Überwachungssystem an den Fässern anbringen zu können, fehlte die gesetzliche Grundlage. Bisher ist es bereits möglich, Abhörwanzen in Wohnungen zu installieren. Zukünftig soll neben der akustischen auch eine optische Überwachung mit Kameras möglich sein.

Das BKA-Gesetz

Am 12. November 2008 beschloss der Deutsche Bundestag gegen die Stimmen der Oppositionsparteien das oben genannte neue "Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt". Das Bundeskriminalamt (BKA) darf künftig im Kampf gegen den Terrorismus Computer ausspähen, Wohnungen mit Kameras und Mikrofonen überwachen und Rasterfahndungen durchführen. Am umstrittensten bleibt die Online-Durchsuchung. Nur bei einer konkreten Gefahr und bei schwersten Straftaten dürfen die Ermittler auf Antrag des Präsidenten des Bundeskriminalamtes und mit Genehmigung eines Ermittlungsrichters heimlich in einen Computer eindringen. In dringenden Fällen soll der BKA-Präsident Beweise auch ohne vorherige richterliche Erlaubnis sichern dürfen. Zur „Abwehr einer dringenden Gefahr" darf das BKA auch Wohnungen akustisch und optisch überwachen. Umstritten ist dabei, dass auch Wohnungen Unverdächtiger beobachtet werden dürfen, in denen ein Verdächtiger verkehrt. Das Gesetz ermöglicht der Behörde auch den Einsatz von V-Leuten. Solche Methoden wurden bisher vor allem von den Geheimdiensten genutzt.

Einen Paradigmenwechsel bedeutet das neue BKA-Gesetz insofern, als es der Behörde erlaubt, jetzt auch präventiv tätig zu werden. Bisher beschränkte sich die Behörde mit ihren 5500 Mitarbeitern auf die Aufklärung bereits erfolgter Straftaten. Die Rechtfertigung für den Eingriff in die Grundrechte der Bürger ist somit notgedrungen ungewiss, da nie sicher ist, ob eine Straftat tatsächlich zur Ausführung gekommen wäre.

Das Gesetz fand jedoch im Bundesrat Ende November 2008 keine Mehrheit, obwohl dies im Grundsatz durch die Föderalismusreform und einer entsprechenden Grundgesetzänderung 2006 beschlossen worden war. Hauptstreitpunkt blieb auch hier die auch ohne richterliche Anordnung vorgesehene heimliche Online-Durchsuchung von Computern, das eingeschränkte Zeugnisverweigerungsrecht von Journalisten, Rechtsanwälten und Ärzten (ausgenommen sind nur Anwälte) sowie die Abgrenzung der Kompetenzen zwischen Bund und Ländern. Gegen die Online-Durchsuchung laufen mehrere Verfahren vor dem Bundesverfassungsgericht, die frühestens 2010 entschieden werden. Die Koalition aus CDU und FDP der neuen Bundesregierung sieht vor, dass eine Online-Durchsuchung künftig nur erlaubt ist, wenn die Bundesanwaltschaft einen Antrag stellt und ein Richter des Bundesgerichtshofs zustimmt.

Massenerfassung von Autokennzeichen

Das Bundesverfassungsgericht blieb seiner Linie treu. Es erklärte die automatisierte Massenerfassung von Autokennzeichen nur auf der Basis einer gesetzlichen Regelung für zulässig. Dabei standen die Ländergesetze Hessens und Schleswig-Holsteins auf dem Prüfstand. Sie sehen den automatisierten Abgleich von Autonummern mit den Fahndungsdatenbanken des Bundeskriminalamtes (BKA) vor. Die von den Lesegeräten aufgenommenen Daten werden anschließend wieder gelöscht. Hessen beispielsweise hat 2007 für rund 300.000 Euro neun Autokennzeichenlesegeräte angeschafft, die zwischen Bad Karlshafen und Viernheim im Einsatz sind. Von März bis Oktober 2007 wurden damit etwa 1 Mio. Autokennzeichen überprüft. Dabei gab es 300 echte Treffer, was einer Gesamtmenge von 0,3 Promille entspricht. Bei Zweidrittel der Delikte handelt es sich um fehlenden Versicherungsschutz. Bei dem Rest geht es um Tankbetrügereien und andere Straftaten.

Das Verfahren ist derzeit in 8 Bundesländern Praxis. Datenschützer befürchten, dass sich auf diese Weise „Bewegungsbilder“ von Autofahrern erstellen lassen. Zumal das Verbot solcher Erstellungen nicht ausdrücklich im (hessischen) Gesetz findet. Ein zweiter Angriffspunkt der

Richter ist die Gesetzgebungskompetenz. Die Länder sind für das Polizeirecht zuständig und somit für die „Gefahrenabwehr". Sollte der Kennzeichenabgleich aber vornehmlich der „Strafverfolgung" dienen, dann wäre das eine Angelegenheit des Bundes.

Im Urteil über die „Rasterfahndung" aus dem Jahr 2006 hieß es: „Insbesondere lässt die Verfassung grundrechtseingreifende Ermittlungen ins Blaue hinein nicht zu." Die Frage ist also, wieweit die Sicherheitsbehörden ihre Methoden auf die Masse unschuldiger Bürger ausdehnen darf, wieweit Präventivmassnahmen zulässig sind.

Videoüberwachung in Verkehrsmitteln

Die Videoüberwachung in Bussen und Bahnen nimmt stetig zu. Im Rhein-Main-Verkehrsverbund sind alle neuen S-Bahnen-Wagen mit Video ausgestattet. Der Zentrale Omnibusbahnhof in Hanau wird mit elf Kameras überwacht. Fast zwei Drittel der 57 Busse der Hanauer Straßenbahn GmbH sind mit Video ausgestattet. In Frankfurt sind es 37 von 180 Bussen und 11 von 103 Straßenbahnen. Weitere 54 sind dafür technisch vorgerüstet. In Wiesbaden verfügen ein Drittel der 226 Busse über ein Videosystem. Die Vandalismusschäden sind deutlich zurückgegangen. Auch sieben größere Haltestellen in der Wiesbadener Innenstadt werden kameraüberwacht. In Darmstadt gibt es an den ca. 60 zentralen Haltestellen „Livekameras". Dort werden die Bilder jedoch nicht aufgezeichnet, sondern nur im Bedarfsfall eingesehen; d. h. sie dienen nicht der Personenüberwachung.

Massenspeicherung von Telefon- und Internetdaten

Ebenso setzte das Bundesverfassungsgericht der Nutzung millionenfach gespeicherter Telefon- und Internetdaten im März 2008 enge Grenzen. Das Gesetz (gültig ab 1. Januar 2008) bleibt zwar bis zur endgültigen gerichtlichen Entscheidung in Kraft, aber für ein halbes Jahr dürfen die Daten nur im Rahmen der Verfolgung schwerer Straftaten verwendet werden. Das sind jene Straftaten, bei denen auch das

Abhören von Telefonen zulässig ist (Paragraph 100a der Strafprozessordnung): Mord, Raub, Erpressung, Entführung, Kinderpornografie, schwerer sexueller Missbrauch, Geldwäsche, Betrug, Korruption, Brandstiftung, Einschleusen von Ausländern, Drogendelikte, Steuerhinterziehung und Betrugsdelikte. Die Tat muss „auch im Einzelfall" schwerwiegend, der Verdacht durch „bestimmte Tatsachen" begründet und die Erforschung des Sachverhalts auf andere Weise „wesentlich erschwert oder aussichtslos" sein. Die Karlsruher Richter gingen von einer „erheblichen Gefährdung" des Persönlichkeitsschutzes aus.

34.443 Bürger hatten gegen das von Bundespräsident Köhler unterzeichnete Gesetz Verfassungsbeschwerde eingelegt. Sie sahen ihr „informelles Selbstbestimmungsrecht" verletzt. Eine so zahlreich unterstützte Verfassungsbeschwerde hat es bisher nicht gegeben.

Primäres Ziel ist auch hier der Persönlichkeitsschutz. Die „umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann" könne einen „erheblichen Einschüchterungseffekt bewirken", heißt es in dem 30-Seiten-Beschluss des Ersten Senats.

Das Gesetz, das zurückgeht auf eine EU-Entscheidung, verpflichtet Telekommunikationsunternehmen, bei Telefonaten das Datum, die Uhrzeit, die Rufnummern beider (oder weiterer) Gesprächsteilnehmer, die Dauer sowie bei Mobilfunkverbindungen den Standort zu Beginn des Gesprächs aufzuzeichnen. Die Daten werden für 6 Monate gespeichert. Mit richterlichem Beschluss haben die Strafverfolgungsbehörden Zugriff auf diese Daten – sowohl zur Strafverfolgung als auch zur Gefahrenabwehr.

Ab 1. Januar 2009 gilt dies auch für das Internet. Dann werden die Anschlusskennung, die Zugangsdaten des Computers (IP-Adresse) sowie Beginn und Ende der Internetnutzung gespeichert. Erfasst werden auch die Daten von E-Mail-Verbindungen sowie die Internettelefonie. Nicht gespeichert wird dagegen, welche Webseiten der Nutzer besucht hat.

Zu bedenken ist zum einen, dass die Speicherung der Daten den Telekom-Unternehmen erhebliche Kosten verursacht, die sie an die Kun-

den weiter geben werden, zum anderen stand das Urteil des Europäischen Gerichtshofes über die Zulässigkeit der übergeordneten EU-Richtlinie noch aus. Dort ist eine Klage Irlands anhängig und hat durchaus Aussicht auf Erfolg. Die EU hat sich die Zuständigkeit für die Richtlinie quasi mit einem „Etikettenschwindel" erkauft. Da für die Richtlinie eine Einstimmigkeit notwendig ist, ging man auf den Erlass einer Richtlinie über. Dazu genügt eine Mehrheitsentscheidung, allerdings ist eine andere Zweckbestimmung notwendig: das Funktionieren des Binnenmarktes. Die Speicherung der Verbindungsdaten tragen hierzu allerdings wenig bei.

In der ersten Eilentscheidung hat das Bundesverfassungsgericht den umfassenden Abruf der Daten durch die Strafverfolgungsbehörden verboten. Es akzeptierte vorläufig den Zugriff auf die Daten bei der Verfolgung von schweren Straftaten. Es gab freilich auch hier schon zu erkennen, dass es den vom Gesetzgeber aufgestellten Katalog für viel zu umfangreich hält.

Im Oktober 2008 verfügte das Bundesverfassungsgericht einen zweiten Eilantrag. Das Gericht akzeptierte zwar vorläufig, also bis zur endgültigen Entscheidung, die Speicherung, nicht aber den im Gesetz umfassend vorgesehenen Abruf der Daten durch die Sicherheitsbehörden.

Gleichzeitig kündigte das Gericht an, dass es die damals in Arbeit befindlichen Gesetze von Bund und Ländern, die der Polizei und dem Geheimdienst auch den präventiven Zugriff auf die Daten geben wollen, nicht akzeptieren wird. Die Gesetzgeber im Bund und in den Ländern haben dies nicht genügend berücksichtigt.

Die erste Eilentscheidung, die auf sechs Monate befristet gewesen war, wurde durch die zweite noch einmal um sechs Monate verlängert. Zudem untersagte das Gericht der Polizei in Bayern und Thüringen den uneingeschränkten Abruf von gespeicherten Verbindungsdaten zur Gefahrenabwehr – wie das dort in den neuen Polizeigesetzen vorgesehen ist.

Nach den Worten des Ersten Senats drohten den Bürgern durch die im Gesetz vorgesehene Datennutzung „Nachteile von ganz erhebli-

chem Gewicht". Denn durch den Zugriff auf die Daten könnte die Polizei „weitreichende Erkenntnisse über das Kommunikationsverhalten der Betroffenen" wie auch über völlig unverdächtige Kontaktpersonen erhalten. Das Gericht will verhindern, dass „das Vertrauen in die allgemeine Unbefangenheit des elektronischen Informations- und Gedankenaustauschs" der Bürger in „erheblichem Maß eingeschränkt wird", heißt es in dem Beschluss. Es ordnete deshalb an, dass Vorratsdaten nur zur Abwehr einer „dringenden Gefahr für Leib, Leben oder Freiheit einer Person" oder für „die Sicherheit des Bundes oder Landes" abgerufen werden dürfen. Im Koalitionsvertrag von CDU und FDP ist vorgesehen, dass die Vorratsdatenspeicherung nur noch dann ausgewertet werden darf, wenn „Leib und Leben in Gefahr" sind.

Kritik äußerten sich die Richter an den Zugriffsbefugnissen von Verfassungsschutz und Nachrichtendiensten. Die gesetzlichen Voraussetzungen, unter denen ihnen die Nutzung der Verbindungsdaten erlaubt sein soll, seien „unscharf und konkretisierungsbedürftig", heißt es in der Begründung. Für einen Datenzugriff könnte es bereits ausreichen, dass jemand an einer Veranstaltung einer nicht verbotenen, aber als extremistisch eingestuften Partei oder Gruppierung teilnehme oder nur einen „falschen Ort" aufsuche.

Nackt-Scanner und Flughafenüberwachung

Im Oktober 2008 schlug ein Plan der EU-Kommission hohe Wellen. Auf Flughäfen sollen sogenannte „Nackt-Scanner" zum Einsatz kommen, die auch unter der Kleidung verborgenen Sprengstoff oder Waffen sichtbar machen. Bei der neuen Technik entsteht mit Hilfe elektromagnetischer Strahlen ein dreidimensionales Bild, auf dem der Fluggast ohne Kleidung erscheint. Alle am Körper befestigten Gegenstände werden dadurch sichtbar. Zugleich aber auch Prothesen, Intimschmuck oder künstliche Darmausgänge u.ä. Von fast allen Parteien in Deutschland wurden diese Geräte als Eingriff in die Intimsphäre abgelehnt. Von „Zwangs-Strips", „FKK auf dem Flughafen", „Peep-Shows im Airport" und „unfreiwilligem Entkleidungstheater" war die Rede. Das Europaparlament forderte die EU-Kommission auf, innerhalb von drei Monaten

die Auswirkungen auf Persönlichkeitsrechte und Gesundheit zu prüfen. Auf Grund der massiven Proteste verkündete die Bundesregierung bereits zwei Tage später, dass die Nackt-Scanner nicht eingeführt würden. Bei einer Testung der Geräte soll es jedoch bleiben.

Seit dem 16. Oktober 2009 wird am Frankfurter Flughafen ein System getestet, mit dem Reisende ihre Pässe von einem Automaten kontrollieren lassen können. Voraussetzung ist ein Reisepass mit biometrischen Daten, wie ihn ein Drittel in Deutschland bereits besitzt (bis 2015 für alle Bundesbürger vorgesehen). Ein Scanner liest in fünf Sekunden die Passnummer, den Namen, den Geburtstag und die Länderkennung aus. Diese Daten werden mit dem Fahndungsregister abgeglichen. Der Abgleich geschieht mit einem Datensatz, der zentral im Bundesamt für Sicherheit (BSI) in der Informationstechnik hinterlegt ist. Findet sich kein Eintrag, öffnet sich die erste Schranke und der Reisende tritt vor eine Kamera. Diese fotografiert sein Gesicht und gleicht es mit dem Foto im Reisepass ab. Der Gang durch die Schleuse dauert so nur 15 Sekunden und soll das Sicherheitspersonal für andere Aufgaben entlasten. Die Verantwortlichen versichern, dass die Daten sofort nach der Einreise wieder gelöscht würden. Der Testlauf ist bis März 2010 vorgesehen und dann auf den Flughafen München ausgedehnt werden.

Verbraucherschutz

Am 10. Dezember 2008 verabschiedete das Bundeskabinett einen Gesetzentwurf, der die persönlichen Daten der Bürger besser schützen soll. Bislang galt die Regel: Wenn der Verbraucher nicht ausdrücklich widerspricht, gilt dies wie eine Zustimmung zur Weitergabe und Verwertung seiner teils sehr persönlichen Daten. Jetzt bedarf die Weitergabe der Daten für Werbung, Markt- oder Meinungsforschung der Zustimmung der Betroffenen. Das Selbstbestimmungsrecht wird somit gestärkt. Bisher kamen die Firmen vor allem über Gewinnspiele und Lotterien an die Daten. Aber selbst aus dem Spenderbereich von Gemeinnützigen Organisationen gab es Datenhandel, ein Milliardengeschäft. Bis zu 50 Euro werden für eine gute Adresse von Unternehmen ausgegeben. Das neue Gesetz sieht Bußgelder von bis zu 300.000 Euro

vor. Zudem können Gewinne aus illegalem Datenhandel vom Staat eingezogen werden. Eine Kennzeichnungspflicht über die Herkunft der Daten soll es weiterhin nicht geben. Ebenso ist es Gemeinnützigen Organisationen und Kirchen weiterhin erlaubt, Adressen zur Spendenwerbung zu kaufen, ohne dass die Betroffenen davon informiert und ihre Einwilligung gegeben haben. Ab 2010 können Unternehmen ein Datenschutzauditsiegel erwerben. Es ga-rantiert den Kunden, dass sich das Unternehmen an branchenspezifische Richtlinien zur Datensicherheit hält.

Pannen beim Datenschutz

Im Oktober 2009 hat der Bielefelder Verein Foebud seine „Big-Brother-Awards" verliehen. Es handelt sich um einen Negativpreis für Firmen, die aus Sicht der Jury „die Privatsphäre von Menschen beeinträchtigen". Innenminister Wolfgang Schäuble bekam den Preis in der Kategorie „Lebenswerk" für seine „obsessiven Bestrebungen, den demokratischen Rechtsstaat in einen präventiv-autoritären Sicherheitsstaat umzubauen". Familienministerin Ursula von der Leyen wurde dagegen für das Vorantreiben der Inhaltskontrolle im Internet geehrt. Die Firmen Bahn, Telekom und Lidl erhielten Preise für ihre Spitzelaktionen.

Wie sensibel der Umgang mit Daten ist, zeigt sich gerade bei der Telekom. 17 Mio. Datensätze von T-Mobile- und T-Home-Kunden wurden gestohlen mit Adressen und Telefonnummern. Diese wurden dem Erotikunternehmer Tobias Huch zugespielt, der den Datendiebstahl der Telekom meldete. Den Gewinn, der sich jährlich aus den Daten ziehen lasse, bezifferte er auf bis zu 50 Mio. Euro. Telekom-Chef René Obermann verkündete daraufhin Mitte Oktober 2008 ein umfangreiches Maßnahmenpaket, u.a. einen zusätzlichen Vorstandsposten für Datenschutz. Über ihre Geschäftskundensparte T-Systems verwaltet die Telekom die Daten von zahlreichen Behörden und Großunternehmen (Daimler, Shell, WestLB u.a.) auf ihren Rechnern.

Die Deutsche Bahn AG hat über Jahre hinweg die Emails ihrer Mitarbeiter/innen kontrolliert. Seit 1998 wurden die Mitarbeiter drei mal

ohne ihr Wissen in so genannten Massen-Screenings durchleuchtet. Ziel war es, Mitarbeiter zu identifizieren, die sich über Scheinfirmen selbst Aufträge zuschanzen. Dies führte zur Entlassung von Bahnchef Hartmut Mehdorn. Auch hatte die Bahn 2007 durch das Zurückhalten von Emails in den Lokführerstreik eingegriffen. Der Konzern soll zwei Lokführerinformationsschriften gelöscht haben. Im Oktober 2009 war in der Presse zu lesen, dass die Bahn wegen des Datenskandals ein Bußgeld in Höhe von 1,1 Mio. Euro zahlen soll. Einen entsprechenden Bescheid erhielt die Bahn vom Berliner Datenschutzbeauftragten Alexander Dix.

Ein weiteres Beispiel von Datenklau wurde im August 2008 öffentlich. Der Verbraucherzentrale Schleswig-Holstein war eine CD mit Daten von 17.000 Bürgern zugespielt worden, die auch deren Kontoverbindungen enthielt. Bei allen handelte es sich um Kunden der Süddeutschen Klassenlotterie. Der Leiter eines Call-Centers hatte die Daten gesammelt und für eine fünfstellige Summe weiter verkauft. Die Datensätze wurden dazu missbraucht, Vertragsabschlüsse vorzutäuschen und bei den Opfern Geld abzubuchen. Dies betraf insbesondere Mitglieder der Bonus Club GmbH, die zum Medienkonzern Bertelsmann gehört.

Fast ein wenig amüsant mutet der so genannte „Christstollen-Skandal“ an. In Deutschland sind mehr als 24 Millionen Kreditkarten und 93 Millionen EC-Karten im Einsatz. Mitte Dezember 2008 kamen der Berliner Landesbank (LBB) Zehntausende vertrauliche Kreditkartennummern abhanden. Ein Päckchen mit den Datensätzen landete am 11. Dezember 2008 in der Redaktion der Frankfurter Rundschau. Das Kundenpaket ging auf einer Kurierfahrt des externen Dienstleisters Atos-Worldline verloren. Die Berliner Landesbank hat 1,9 Millionen Kreditkarten ausgegeben, viele davon im Namen von Geschäftspartnern (wie ADAC, Air Berlin und Amazon). Die Kreditkartenabrechnungen waren unverschlüsselt, auf bedruckten Folien (sog. Mikrofiches) unterwegs. Im Paket enthalten waren unter anderem 907 Mikrofiches mit detaillierten Kreditkartenabrechnungen, die die Firma Atos Worldline an die LBB geschickt hat. Es enthielt zudem acht ungeöffnete Briefe mit Geheimnummern von Karten, drei Lieferscheine und eine Rechnung von Atos an die LBB.

Der Datenskandal entpuppte sich kurze Zeit später als Stollen-Diebstahl. Zwei Kurierfahrer hatten ein ursprünglich für die „Frankfurter Rundschau" bestimmtes Paket mit einem Weihnachtsstollen geplündert. Daraufhin versahen die Männer eines von sechs für die Landesbank Berlin (LBB) bestimmten Pakete mit dem Adressetikett des zerstörten Stollenpakets. Der geklaute Christstollen war ursprünglich von einer Stuttgarter Firma per Kurierdienst nach Frankfurt geschickt worden und zunächst in der Sammelstelle in Mainz gelandet, wo auch das Paket der Firma Atos Worldline zwischengelagert war. Beim Sortieren der Pakete fiel den Kurierfahrern dann der Christstollen in die Hände.

Ende Juli 2009 durchsuchte die Polizei insgesamt 28 Wohnungen und Büros von Verdächtigen, die mit sensiblen Kundendaten der Telekom Handel betrieb, vor allem in der Türkei. Drei der Vertriebspartner der Telekom erhielten Abmahnungen, da sie gegen datenrechtliche Bestimmungen verstoßen hatten. Die Großkonzerne haben die Kundenbetreuung und Neuakquisition zunehmend ausgelagert. Sensible Daten werden dafür an die Callcenter weitergegeben, mit der Verpflichtung, diese später zu löschen. Allein die Telekom arbeitet mit etwa 1200 selbständigen Vertriebspartnern. Diese wiederum bedienen sich der Unterstützung von 13.000 Subunternehmen. Die Gefahr des Datenmissbrauchs ist da groß.

Im Oktober 2009 erhielt der Hörfunksender NDR Info 27.000 Datensätze des Finanzdienstleisters AWD zugespielt. AWD mit Firmensitz in Hannover bietet Finanz- und Altersvorsorgeprodukte vom Bausparvertrag bis zur Lebensversicherung an. Die Datensätze enthielten Kundennummer, Adresse, Telefonnummer, Berufsbezeichnung, Geburtstag und Informationen über Lebensversicherungen (Höhe des angelegten Geldes); insgesamt mehr als 60.000 Vertragsangaben. Unklar blieb, woher die Daten stammten.

Beim Online-Buchhändler libri.de standen Ende Oktober 2009 rund 500.000 Rechnungen von Kunden ungesichert im Internet. Ein Kunde hatte den Blog netzpolitik.org auf das Datenleck aufmerksam gemacht, der den Online-Buchhändler umgehend informierte. Dem Kunden war ein Online-Link auf seiner Online-Rechnung suspekt vorge-

kommen. Die Veränderung der sechsstelligen Zahl führte jeweils zu den Rechnungen anderer Kunden – inklusive Anschrift, Rechnungsnummer und bestellten Artikeln. Die Kundendaten sind allerdings nicht in den Umlauf gelangt, so dass ein Schaden abgewendet werden konnte.

Dies sind nur einige von zahlreichen Skandalen im Bereich Datenschutz, die in den vergangenen Jahren publik wurden. Die zwangsläufige Speicherung von Daten in fast allen Lebensbereichen ist ein sensibles Thema. Eine absolute Sicherheit wird es hier nicht geben. Der Wertekonflikt Freiheit versus Sicherheit lässt sich nicht auflösen und wird uns in Zukunft verstärkt beschäftigen. Wie eingangs bereits gesagt: Es gibt keine letzte Sicherheit gegen Lebensrisiken. Insofern ist die Balance zwischen den Erfordernissen der Sicherheit und den Notwendigkeiten der bürgerlichen Freiheiten immer wieder neu auszutarieren.

TAUWETTER

...franziskanische Zeitschrift für Gerechtigkeit,
Frieden und Bewahrung der Schöpfung

2002

1 Afghanistan – das unbekannte Land am Hindukusch
2 Afghanistan –Mehr als 2 Jahrzehnte Krieg
3 Israel und Palästina – ein Land und zwei Gerechtigkeiten
4 Ehrfurcht vor der Schöpfung

2003

1 Krieg – Niederlage der menschheit
2 Internationaler rat des franziskanerordens
für gerechtigkeit, Frieden und bewahrung der Schöpfung
3 Mit Eigensinn und Gottesgespür:
Klara von Assisi zum 750. Todestag
4 Wasser als Lebensgut

2004

4 Der Sudan zwischen Machtkampf und Völkermord
3 Gewaltfrei
2 Zwei Klassen Medizin
1 Menschenwürdig sterben

2005

4 Europäische Identität
3 Sozialstaat Deutschland
2 Der Herr gebe Dir den Frieden – Eine neue Welt ist möglich
1 Pax Americana

2006

4 Interkulturelles Zusammenleben – Muslime und Christen in Deutschland
3 20 Jahre Friedensgebet von Assisi
2 Ostafrika: Die Wunde im Fleisch
1 Rote Karte für den Menschenhandel

2007

4 Elisabeth – eine leidenschaftliche Frau
3 Kolumbien: Die Schatten des Todes
2 Die Sache des Friedens
1 Weltsozialforum Nairobi 2007

2008

1 Bedroht – verfolgt – vertrieben: Flüchtlingsschicksale in Ostafrika
2 Geld: Gott-Götze-Gerechtigkeit
3 Franziskaner im Dialog mit dem Islam
4 Der Afghanistan – Konflikt

2009

1 Anstösse zur menschlichkeit
2 Krise aus Dummheit und Gier
3 Schöpfung im herzen der sendung

Bestellung alter Hefte (vgl. www.tauwetter-online.de)

Redaktion Tauwetter, Immermannstrasse 20,
Postfach 240139, 40090 Düsseldorf
redtauwetter@aol.com