Vertrauen in der Informationsgesellschaft

*Buchbeitrag von Jörg Tauss. In: Informationelles Vertrauen für die Informationsgesellschaft. Klumpp, Dieter/Kubicek, Herbert/Roßnagel, Alexander (Hrsg.). S. 63-70..**

* *mit freundlicher Genehmigung der Alcatel-Lucent Stiftung*

Bertolt Brechts Satz „Vertrauen wird dadurch erschöpft, dass es in Anspruch genommen wird" scheint Maxime moderner Sicherheitspolitik in der Informationsgesellschaft zu werden. Immer weniger (ver-)traut der Staat seinen Bürgerinnen und Bürgern, immer mehr wird der Rechtsstaat zum Präventionsstaat, in der zunächst auch der Unschuldige seine Unschuld beweisen muss. Wer nichts zu verbergen hat, könne doch transparent sein. Wer nicht transparent ist, macht sich verdächtig. Nur der Verdächtige lässt Verbindungsdaten nicht speichern, seine Festplatten nicht durchsuchen.

Online-Durchsuchung, Vorratsdatenspeicherung, Online-Abgleich von biometrischen Merkmalen in Ausweisdokumenten und Videoüberwachung sind Stichworte für die These, dass die für innere Sicherheit zuständigen Behörden und ihre Politiker die Bürgerinnen und Bürgern immer mehr überwachen wollen und ihnen zugleich immer weniger Vertrauen entgegen zu bringen bereit sind.

Wenig verwunderlich also, dass so manche bereits am Nachruf für den Schutz der personenbezogenen Daten schreiben. Doch die Wahrung des Rechtes auf informationelle Selbstbestimmung bleibt ein zentrales Ziel der politischen und rechtlichen Gestaltung der Wissens- und Informationsgesellschaft, wie dies auch das Bundesverfassungsgericht dankenswerter weise immer wieder bestätigt hat. Das ist, nachdem vor 30 Jahren das Bundesdatenschutzgesetz in Kraft trat, angesichts der immensen technologischen Herausforderungen einer weltweit vernetzten Gesellschaft und angesichts der neuen Gefährdungen auch unabdingbar. Nachdem man in den vergangen Jahren - von der Debatte über die Weitergabe von Flugdaten bis hin zur aktuell diskutierten Vorratsdatenspeicherung - sich dessen ungeachtet kaum des Eindrucks erwehren konnte, Rechtsstaat, Datenschutz und das Recht auf informationelle Selbstbestimmung stünden immer mehr hinter tatsächlichen und vermeintlichen Sicherheitsinteressen zurück, muss die fehlende Abwägung Bürgerrechte versus diverser Sicherheitsgesetze endlich wieder auf die politische Agenda. Was noch immer aussteht, ist eine umfassende und ehrliche Evaluation der Anti-Terrorgesetze. Die Innenpolitik scheut sich davor und beantwortet die parlamentarische Forderung nach dieser Evaluation mit der Selbstevaluation durch die betroffenen Behörden. Vertrauen in die Wirksamkeit eigener Gesetze sieht anders aus. Warum scheuen sich die Verantwortlichen, die in den letzten Jahren geschaffenen neuen Eingriffsbefugnisse für die Sicherheitsbehörden hinsichtlich ihrer Verhältnismäßigkeit, Wirksamkeit und Effizienz tatsächlich nach transparenten Kriterien durch unabhängige Wissenschaftler evaluieren zu lassen?

Noch vor dieser Evaluation werden unter dem Deckmantel Terrorismusbekämpfung immer neue Gesetze vorbereitet. Gegenwärtig wird in Deutschland und in den europäischen Ländern die Umsetzung der umstrittenen Richtlinie zur Vorratsdatenspeicherung beraten. Der Gesetzentwurf der Bundesregierung zur Neuordnung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen im Strafverfahren liegt auf dem Tisch. Angesichts der Eingriffstiefe in die Grundrechte

der europäischen Bürgerinnen und Bürger und angesichts der Reichweite - betroffen sind 480 Millionen Menschen in Europa, davon 80 Millionen in Deutschland - stellen sich die Fragen der Angemessenheit und Verhältnismäßigkeit in besonderem Maße, und die Politik ist in der Pflicht, hinreichend zu antworten. Hier gilt es, rechtsstaatliche Grundsätze zur Erhebung und Verarbeitung dieser Daten, klare Löschungspflichten sowie Beschränkungen des Zugangs auf richterliche Anordnung und lediglich zur Aufklärung schwerer Straftaten zu formulieren. Daneben gilt es vor allem, den Berufsgeheimnissen, etwa von Seelsorgern, Anwälten, Journalisten und Abgeordneten, wirksam Geltung zu verleihen.

Um jedem falschen Eindruck entgegen zu wirken: Politik hat ihre Verantwortung für eine wirksame Kriminalitätsbekämpfung wahrzunehmen. Sie hat aber auch ihre Verpflichtung für Bürgerrechte ernst zu nehmen. Doch die Vorgaben der EU-Regelungen gingen und gehen zu weit. Deshalb ist es sinnvoll, dass sich der Deutsche Bundestag in einem Antrag „Speicherung mit Augenmaß - Effektive Strafverfolgung und Grundrechtswahrung" maximal für eine Minimalumsetzung der Richtlinie ausgesprochen hat.

Dennoch ist und bleibt es auch bei einer solchen Minimalumsetzung unbestritten, dass die Einführung gesetzlicher Speicherungspflichten für Telekommunikationsverkehrsdaten in die Grundrechte sowohl der Nutzer als auch der Anbieter von Telekommunikationsdiensten eingreift; konkret betroffen hiervon sind das Fernmeldegeheimnis nach Artikel 10 Abs. 1 des Grundgesetzes (GG) und die Freiheit der Berufsausübung nach Artikel 12 Abs. 1 GG. Die Abfrage der gespeicherten Daten kann zudem weitere Grundrechte berühren, etwa die Presse- und Rundfunkfreiheit nach Artikel 5 Abs. 1 Satz 2 GG.

Betroffen sein können zudem Zeugnisverweigerungsrechte bestimmter Berufsgruppen, beispielsweise von Anwälten und Seelsorgern - Berufsgruppen also, die besonders auf Vertrauen angewiesen sind, um ihre Arbeit leisten zu können. Das gilt auch für berufsmäßige Journalistinnen und Journalisten, die auf Informationen durch Dritte und deren Vertrauen angewiesen sind. Die Grundrechte und auch die Zeugnisverweigerungsrechte sind in einem freiheitlichen demokratischen Gemeinwesen von besonders großer Bedeutung. Eingriffe in diese Grundrechte, von denen zahlreiche Personen betroffen werden, die in keiner Beziehung zu einem konkreten Tatvorwurf stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, sind deshalb besonders schwerwiegend und bedürfen einer besonderen Rechtfertigung. Das gilt erst recht für das Vorhaben einer solch weit reichenden verdachtsunabhängigen Speicherung von Kommunikationsdaten auf Vorrat.

Der vom Bundeskabinett beschlossene Gesetzentwurf und die Forderung aus dem Bundesrat sind viel zu weitgehend und müssten im parlamentarischen Verfahren grundlegend korrigiert und verbessert werden -sie sind weder verhältnismäßig noch angemessen.

Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen greifen besonders intensiv in die Grundrechte der Bürgerinnen und Bürger ein. Daher müssen für ihre Zulässigkeit strenge Voraussetzungen gelten, und auch der Rechtsschutz muss wirksam ausgestaltet sein. Angesichts des nun vorliegenden Gesetzentwurfes bleiben aber mit Blick auf den Grundrechtsschutz erhebliche Zweifel und massive - auch verfassungsrechtliche - Bedenken bestehen. Das gilt beispielsweise,

wie ausgeführt, für die vorgesehene Neuordnung der Zeugnisverweigerungsrechte und die damit einhergehende Relativierung der Zeugnisverweigerungsrechte für Journalisten und Medienvertreter. Gleiches gilt hinsichtlich der Umsetzung der Vorgaben der Richtlinie zur Vorratsdatenspeicherung. Zwar ist es richtig, dass sich der Gesetzentwurf eng an die Vorgaben hält, die der Deutsche Bundestag beschlossen hat; entsprechend dieser Vorgaben soll die Speicherungsfrist auf sechs Monate begrenzt werden, Daten, die über den Inhalt einer Kommunikation Aufschluss geben, dürfen nicht gespeichert werden. Der zuständige Bundesratsausschuss forderte nun aber bereits eine Verdoppelung der Speicherdauer und eine nochmalige Erweiterung der Daten.

So bleiben nach wie vor massive Bedenken hinsichtlich der Notwendigkeit und Verhältnismäßigkeit einer flächendeckenden Speicherung von Telekommunikationsdaten auf Vorrat wie auch bezüglich der gewählten Rechtsgrundlage. Leider war die Forderung nicht durchsetzbar, der Deutsche Bundestag solle die Verabschiedung des Gesetzes daher so lange aussetzen, bis die Frage der Rechtmäßigkeit vom Europäischen Gerichtshof abschließend geklärt ist. Darüber hinaus hat der Deutsche Bundestag in seinem Beschluss zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung auch klargestellt, dass bei der Anwendung der Richtlinie insbesondere auch die Berufsgeheimnisse gewahrt bleiben müssen. Daher müssen die Vorgaben zur Vorratsdatenspeicherung auch hier im Zusammenhang mit der Neuordnung der Zeugnisverweigerungsrechte mit der Bundesregierung weiter diskutiert und im parlamentarischen Verfahren verbessert werden.

Denn insgesamt begegnet der Gesetzentwurf der Bundesregierung zur Neuordnung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Vorgaben der Richtlinie zur Vorratsdatenspeicherung massiven grundsätzlichen und verfassungsrechtlichen Bedenken, die die Politik auch in Hinblick auf mögliche neue Klagen vor dem Bundesverfassungsgericht nicht gleichgültig lassen können. Viele sind aufgeschreckt, und das ist zu begrüßen. Denn ein wirksamer Datenschutz muss, so hat es Professor Spiros Simitis ausgedrückt, als politische Unruhe aufgefasst werden.

Diese aktuelle Diskussion macht allerdings auch deutlich, dass immer wieder um die Balance zwischen Freiheit und Sicherheit gerungen werden muss - und zwar sowohl bezüglich der bürgerlichen Freiheiten wie auch der Medienfreiheiten - und dass diese Balance zwischen Freiheit und Sicherheit immer wieder auch infrage gestellt wird und neu zu justieren ist. Wir stehen zwischenzeitlich an einem Wendepunkt von einer freien Gesellschaft zumindest in die Richtung einer unfreien Gesellschaft - mit mehr Staat aber weniger Rechtsstaat.

Notwendig ist in einer demokratisch verfassten Gesellschaft auch in einer neuen Gefährdungssituation durch organisierte Kriminalität und Terrorismus jedoch eine verfassungskonforme Abwägung zwischen den notwendigen Mitteln der Terrorismusbekämpfung und der Strafverfolgung auf der einen Seite und dem Schutz der Grundrechte, etwa dem Recht auf informationelle Selbstbestimmung aber auch anderen Grundrechten wie etwa den Medienfreiheiten, auf der anderen Seite.

Datenschutz ist als Grundrechtsschutz eine unverzichtbare Funktionsbedingung für jegliches demokratisches Gemeinwesen. Ein solcher Grundrechtsschutz ist aber mir dann gewährleistet, wenn die Erhebung, Speicherung und Nutzung von personenbe-

zogenen Daten grundsätzlich der freien Selbstbestimmung unterliegen. Das gilt in ganz besonderem Maße dann, wenn beinahe alle Lebensbereiche durch neue Informations- und Kommunikationstechnologien durchdrungen sind und sensible Daten und Informationen aus allen gesellschaftlichen Bereichen in zunehmendem Maße in weltweite Informations- und Kommunikationsnetzwerke eingespeist und übermittelt werden. Dass dies für die Gesellschaft und die Wirtschaft auch Vorteile mit sich bringt, ist unbestritten. Allerdings bieten die Möglichkeiten heimlicher Datenerhebung oder -manipulation sowie die Integration unterschiedlicher Datenbestände zur Analyse umfassender Persönlichkeitsprofile auch erhebliches Gefährdungspotenzial.

An dieser Stelle kann stellvertretend für solche Gefährdungspotenziale durchaus die viel diskutierte RFID-Technologie mit ihren Chancen, aber eben auch mit ihren negativen Aspekten und Gefahren benannt werden. Der Bürger muss umfassend über den Einsatz, Verwendungszweck und die Inhalte von RFID-Tags informiert werden. Als Betroffener muss man die Möglichkeit haben, die RFID-Tags dauerhaft zu deaktivieren respektive die darauf enthaltenden Daten endgültig zu löschen. Eine heimliche Erstellung personenbezogener Verhaltens, Nutzungs- oder gar Bewegungsprofile darf es nicht geben. Die Sinnhaftigkeit der Verbindung neuer Ausweisdokumente mit der RFID-Technik ist an keiner Stelle vernünftig belegt.

Gerade das Beispiel RFID zeigt in aller Deutlichkeit, dass eine autonome Handlungs- und Kommunikationsfähigkeit der Bürgerinnen und Bürger - als Voraussetzung für die gesellschaftliche Akzeptanz und Entwicklung der zivilen Informationsgesellschaft - gefährdet sein kann. Das gilt es zu verhindern, da sich fehlendes Vertrauen und fehlende Akzeptanz seitens der Nutzer auch negativ auf die wirtschaftlichen Entwicklungschancen entsprechender Angebote auswirken dürften. Basis für Akzeptanz ist das Vertrauen der Anwender in die Technologien der Informationsgesellschaft. Und Datenschutz ist - mittlerweile auch weltweit anerkannt - einer der zentralen Akzeptanzfaktoren dafür.

Dennoch: auch wenn das deutsche Datenschutzrecht international eine führende Stellung einnimmt, es ist nur noch bedingt wirksam. Neue Formen personenbezogener Daten und deren Verarbeitung sind bisher nur ungenügend aufgenommen, die Gefahren und Chancen neuer Techniken der Datenverarbeitung bisher nur unzureichend berücksichtigt. Darüber hinaus sind zahlreiche Formulierungen zum Teil widersprüchlich oder unübersichtlich. Das wurde auch in Anhörungen zur Modernisierung des Datenschutzes durch Fachexperten immer wieder deutlich gemacht. Im Deutschen Bundestag besteht deshalb innerhalb aller (!) Fraktionen zumindest in allgemeiner Form Einigkeit darin, Reformen hinsichtlich eines modernen und innovativen, leicht verständlichen und übersichtlichen Datenschutzrechtes zugig voranzutreiben. Das ist angesichts neuer technologischer Entwicklungen mit ständig wachsenden Datenbeständen und einer zunehmenden Vernetzung auch dringend erforderlich. Der zunehmenden Konvergenz der Technik muss sinnvollerweise eine Konvergenz des Datenschutzrechtes folgen, ohne dabei das bestehende Schutzniveau abzusenken und noch vorhandenes Vertrauen zu gefährden.

Ein wirkungsvoller Datenschutz ist natürlich nie ein klar definierter und abgeschlossener Bereich. Das Datenschutzrecht ist ein überaus dynamischer, sich im permanenten Wandel befindlicher Prozess, so dass bestehende Normen immer wieder aufs Neue aktuellen Entwicklungen und Erkenntnissen angepasst werden müssen. Das bedeutet keine Überregulierung. Im Gegenteil: Erst ein modernes Datenschutzrecht

führt zu unbürokratischen und effizienten Lösungen und ist so ein wichtiges Instrument zum Bürokratieabbau. Mehr noch: ein modernes und effizientes Datenschutzrecht ist vielmehr auch ein wirtschaftlicher Standortvorteil, insbesondere dann, wenn das bestehende Datenschutzrecht um neue Datenschutzinstrumente ergänzt wird. Ein solches wichtiges Instrument ist das Datenschutzauditgesetz wie in § 9a des BDSG vorgesehen und wie zum wiederholten Mal auch vom BfDI gefordert. Die Vorteile und vertrauensbildenden Komponenten eines solchen Gesetzes liegen auf der Hand. Da gilt sowohl für den Verbraucher, als auch für die Wirtschaft:

Der Verbraucher erhält durch ein Audit erstmals die Möglichkeit, Produkte und Dienstleistungen hinsichtlich ihrer Datenschutzkonformität zu überprüfen bzw. zu vergleichen. Das führt, davon bin ich überzeugt, u.a. zu der angesprochenen und überaus notwendigen Stärkung der Akzeptanz des Datenschutzes.

Für die Wirtschaft bedeutet die Möglichkeit, eigene Produkte und Dienstleistungen durch eine unabhängige, evtl. öffentliche Stelle auditieren zu lassen, einen nachhaltigen Wettbewerbsvorteil gegenüber Mitkonkurrenten und kann gleichzeitig die Selbstverantwortung im Bereich des Datenschutzes und der Datensicherheit stärken - die Firma Microsoft hat uns das im Februar eindrucksvoll gezeigt, als man zwei Produkte durch das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein auditieren ließ. Auch andere Stimmen aus Wirtschaft und Industrie und insbesondere aus den entsprechenden Interessenverbänden zeigen, dass ein solches Datenschutzaudit mehr und mehr gewünscht wird.

Dem Vertrauen zu einem solchen Auditgesetz müssen zwei fundamentale Prinzipien zugrunde liegen. Es muss auf dem Prinzip der Freiwilligkeit beruhen und dabei unbürokratisch ausgestaltet sein. Einem Unternehmen muss es frei stehen, ob es sich einem solchen Datenschutzaudit unterzieht oder nicht. Würden wir die Auditierung gesetzlich zu einer Verpflichtung machen, wäre die beabsichtigte Wirkung konterkariert und ein Mehr an Bürokratie wäre geschaffen. Das wäre nicht zielführend. Ziel muss eine win-win-Situation für alle Beteiligten sein. Wie ein solches Gesetz konkret ausgestaltet wird, werden die Gespräche und Verhandlungen mit unserem Koalitionspartner und dem Bundesministerium des Inneren in dieser Legislaturperiode zeigen.

Ein weiteres wichtiges Thema in der politischen Debatte sind biometrische Verfahren. Auch wenn der Hype dieser Diskussion hinter einige der bisher erwähnten Themen zurückgefallen ist, so rücken doch, und nicht zuletzt aufgrund gestiegener Sicherheitsanforderungen und des Wunsches nach absolut täuschungs- oder fälschungssicherer Identifikation bzw. Verifikation, die biometrisch erfassbaren Merkmale von Personen immer mehr in den Blickpunkt. Dabei berühren diese Verfahren die unterschiedlichsten und insbesondere für den Bürger weitest reichenden Bereiche.

Hierbei geht es weniger um die - natürlich dennoch interessante - Frage der (überflüssigen) Kosten einer Nutzung von biometrischen Merkmalen in Ausweisdokumenten, sondern vielmehr um die grundsätzliche Zuverlässigkeit sowie die Angreifbarkeit solcher Systeme. Ich bezweifle, dass der Einsatz von Biometrie-Pässen wirklich ein Mehr an Sicherheit bringt und bringen wird. Daran haben auch die gebetsmühlenartig vorgebrachten Hinweise und Forderungen zweier Bundesinnenminister nichts geändert.

Ein digitales Foto und Fingerabdrücke im Pass verraten nichts über mögliche kriminelle oder terroristische Absichten des Passinhabers. Vielmehr gibt es Hinweise, dass ein solcher ePass schnell selbst zum Sicherheitsrisiko werden kann: bei einer zehnjährigen Gültigkeit von Reisepässen kann doch heute niemand seriös ausschließen, dass die biometrischen Daten nicht doch irgendwann unbemerkt gelesen, kopiert oder verändert werden können - spätestens, wenn sie durch den Reisenden in einem „Schurkenstaat" schon während eines Hotelaufenthalts tagelang in fremde Hände zu übergeben sind. Dieser Aspekt wurde bisher in der Debatte sträflich vernachlässigt.

Datenschutz ist also letztlich nicht nur Grundrechtsschutz. Dem Datenschutz kommt auch eine grundlegend neue Bedeutung als Wettbewerbsund Standortvorteil und bei der Verhinderung neuer Kriminalitätsformen (Stichwort „Phishing") zu. Wir müssen diesen Vorteil gerade auch im Hinblick auf den europäischen und internationalen Kontext stärker nutzen. Je länger aber die notwendige und umfassende Modernisierung des Datenschutzes auf sich warten lässt, desto größer ist im Anschluss der gesetzgeberische Aufwand und desto geringer das Vertrauen in staatliches Handeln beim Schutz personenbezogener Daten. Dieses Vertrauen bei den Bürgerinnen und Bürgern ist für die Verwirklichung einer modernen Wissens- und Informationsgesellschaft unabdingbar. Im Brecht'schen Sinne darf dieses Vertrauen durch die Bürgerinnen und Bürger in Anspruch genommen werden.