Gläserner Mensch, kontrollierter Bürger, berechenbarer Kunde?
Sind wir auf dem Weg in die Totalüberwachung durch Staat und Wirtschaft?

Datenschutzpolitische Herausforderungen und Forderungen

Von **Hartmut Lubomierski**, Hamburgischer Datenschutzbeauftragter
(Stand: Mai 2005)

Jeder Mensch kommuniziert, bewegt sich im öffentlichen Raum, konsumiert, hinterlässt Spuren. Was ist heute das besondere daran?
Noch nie zuvor wurden die Verhaltensweisen des Menschen so extrem technisch unterstützt und konnten technisch so perfekt und eindeutig abgebildet und unbegrenzt aufgezeichnet und abgerufen werden wie heute.
Unser Kommunikationsverhalten erfolgt ganz überwiegend elektronisch vermittelt über Telefon, E-Mail, Internet, Handy. Bereits jetzt werden alle diese Verbindungsdaten lückenlos gespeichert und sie sollen noch länger gespeichert werden. Stichwort: Vorratsdatenspeicherung für ein Jahr oder sogar bis zu drei Jahren.
Unser Bewegungsverhalten im öffentlichen Raum ist weitgehend nachvollziehbar. Stichwort: Videoüberwachung im öffentlichen Raum, Maut, Ortung des Handys, Automatische KFZ-Kennzeichenerfassung.
Spuren, die wir hinterlassen, sind heute eindeutig zu identifizieren. Stichwort: Genetischer Fingerabdruck.

E-Mail: mailbox@datenschutz.hamburg.de
Klosterwall 6 - D-20095 Hamburg - Tel.: 040 - 4 28 54 - 40 40 - Fax: 040 - 4 28 54 – 40 00

Jeder Mensch ist einmalig. Das galt zwar schon immer, aber noch nie war diese Einmaligkeit so eindeutig und fälschungssicher abbildbar wie heute. Stichwort: Biometrie, DNA-Identifikationsmuster.
Jeder Mensch zeigt ein Konsumverhalten, ob im Tante-Emma-Laden oder beim Otto-Versand. Aber wir kaufen immer öfter per Kunden- und Kredit-Karte, bestellen im Internet. Unser Konsumverhalten wird elektronisch erfasst und ausgewertet.
Jeder Mensch hat eine bestimmte genetische Disposition. Es werden immer mehr Tests entwickelt, um Aussagen über Lebenserwartung, Eigenschaften, Leistungsfähigkeiten sowie Veranlagungen zu Krankheiten zu ermöglichen.

Nimmt man all diese Daten über eine Person zusammen, also alle Daten über Kommunikationsverhalten, Bewegungsprofil, Konsumverhalten, genetische Disposition, so haben wir einen Befund, auf den die Metapher „gläserner Mensch“ voll zutrifft.

Dennoch scheint dieser Befund heute beim „Normalbürger“ keine Ängste vor einem „Überwachungsstaat“ auszulösen. Aus der Horrorvision einer totalen staatlichen Überwachung durch Technik ist die Erwartung geworden, durch den Einsatz von Technik und Datenerfassung werde sowohl unsere individuelle als auch die gesamtgesellschaftliche Sicherheit erhöht und unser Kommunikations- und Informationsbedürfnis besser und bequemer befriedigt.

Die Möglichkeit des Staates wie der Wirtschaft, sich automatisiert Informationen zu beschaffen und diese zu verarbeiten und auszuwerten, um „Profile“ von Menschen zu erstellen (Persönlichkeitsprofil, Kundenprofil, Wählerprofil, Täterprofil) scheint die Bürger nicht zu schocken.

Warum schreien wir über diesen Befund nicht kollektiv auf?
1983, vor mehr als 20 Jahren, haben die Menschen aufgeschrieen, weil sie einen Fragebogen ausfüllen sollten zur Volkszählung, deren Daten anschließend anonymisiert wurden und die lediglich dem Staat als Planungsgrundlage dienen sollten. Die Daten, die damals erhoben wurden, waren harmlos gegenüber denjenigen, die heute angegeben werden müssen, um „Arbeitslosengeld II“ oder einen Kredit nach „Basel II“ zu beantragen, und die heute dauerhaft personenbezogen gespeichert und abgeglichen werden.

Das Bundesverfassungsgericht sagte bereits 1983: Personenbezogene Daten können zu einem weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung hinreichend kontrollieren kann.

Damals kreierte das Bundesverfassungsgericht das Grundrecht auf informationelle Selbstbestimmung und formulierte den Grundsatz: Jeder Einzelne hat die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Und das Verfassungsgericht stellte fest: Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.

Wer weiß heute, wer was wann und bei welcher Gelegenheit über ihn weiß. Wissen wir, was wir bereits an persönlichen Daten wem preisgegeben haben und was mit diesen Daten geschieht?

1983, ein Jahr vor Orwells 1984, war die Angst vor einem Überwachungsstaat größer als heute. Wir haben die paradoxe Situation, dass zu einem Zeitpunkt, als sich die Risiken einer massenhaften und schnellen automatisierten Verarbeitung personenbezogener Daten gerade erst abzeichneten, der Datenschutz im Mittelpunkt des öffentlichen Interesses stand. Heute aber, da sich diese Risiken zu realen Gefahren verdichtet haben, also der früher nur als Schlagwort beschworene „gläserne Mensch“ Gestalt annimmt, scheint die Sensibilität für die Bedeutung des Datenschutzes weitgehend abhanden gekommen zu sein.

Was sind die Gründe? Entscheidend ist wohl: Wir sehen heute – zumindest in Deutschland - keine Institution, weder den Staat noch in der Wirtschaft, die eine totale Überwachung des Menschen vorzunehmen sich anschickt. Eine „Stasi“-Angst existiert im vereinten Deutschland nicht.

Der Topos „Informationsgesellschaft“ wird positiv empfunden.

Die Allgegenwart von Informationstechnik, die alltägliche Gewöhnung an Informations- und Kommunikationstechnik, an den Computer lässt Warnungen vor Missbräuchen als Ausdruck von Technikfeindlichkeit und Rückständigkeit erscheinen.

Die gesellschaftliche und politische Komplexität ist so gestiegen, dass sich der Bürger ohne technische, datenverarbeitende Unterstützung überfordert fühlt.

Ohne technische Vermittlung scheint eine adäquate Teilnahme an der arbeitsteiligen Gesellschaft aber auch gar nicht mehr möglich zu sein. Wir sehen uns dazu verurteilt, uns der Technik zu bedienen und uns auf Technik zu verlassen.

Die Miniaturisierung der Informations- und Kommunikationstechnik und ihre ständige Verbilligung lässt uns diese Technik als Erleichterung und Verbesserung der Lebens- und Arbeitsbedingungen wahrnehmen und die dadurch eröffneten Missbrauchsmöglichkeiten vernachlässigen.

Die politischen Herausforderungen, die Bekämpfung des internationalen Terrorismus, Konsequenzen der Globalisierung, der Umbau der Sozialsysteme, Privatisierung und Verwaltungsmodernisierung, all dies erzeugt einen Handlungsdruck und Regelungsstress, angesichts dessen Datenschutz vielfach als effektivitätshemmender Stör- und Kostenfaktor betrachtet wird, der sinnvolle Lösungen be- oder verhindert.

Die Notwendigkeit einer wirksamen unabhängigen Kontrolle dieser Eigendynamik staatlichen und wirtschaftlichen Handelns zur Sicherung des Persönlichkeitsrechts und der Privatsphäre wird nicht hinreichend erkannt.
Dabei werden die Begehrlichkeiten sowohl von Seiten des Staates als auch der Wirtschaft nach einer Erfassung, Sammlung und Nutzung personenbezogener Daten immer stärker.

Für den Bereich der Verbrechensbekämpfung fordert die Polizei „das volle Programm“.

Immer weitergehende Instrumentarien für Vorfeldermittlungen werden eingefordert, um unabhängig von der Eingriffsschwelle des klassischen Polizeirechts, also vom Vorliegen einer konkreten Gefahr oder eines Anfangsverdachts, tätig werden zu können:

- Präventive Telekommunikationsüberwachung, obwohl die repressive TKÜ bereits jetzt bei Schwerstkriminalität weit ins Vorfeld konkreter Rechtsverletzungen hineinreicht,
- Verdachtsunabhängige Personenkontrollen an jedem Ort in der Stadt,
- Videoüberwachung im öffentlichen Raum.

Damit bezieht die Polizei ganz überwiegend völlig unbeteiligte und gesetzestreue Bürger in ihre Beobachtung ein. Die Polizei erhält wegen der Heimlichkeit dieser Vorfeldtätigkeit Instrumente, die bisher nur dem Verfassungsschutz zugestanden wurden. Mit dieser Art der Verdachtsschöpfung wird die Unschuldsvermutung aufgehoben. Der beobachtungsfreie, der undokumentierte Raum wird für den Bürger immer enger und letztlich auf den „absoluten Kernbereich privater Lebensgestaltung“ reduziert. Hinzu kommt der Wunsch der Strafverfolgungsbehörden nach

- Vorratsdatenspeicherung aller Telekommunikationsverbindungen, heute in der Regel bis zu 3 Monaten, künftig bis zu einem Jahr, am liebsten bis zu 3 Jahren.
- DNA-Analyse, heute nur bei schweren Straftaten, qualifizierter Negativprognose und unter Richtervorbehalt, künftig auch bei Bagatellkriminalität und einfacher Negativprognose ohne Richtervorbehalt.

Dabei ist zugestanden, dass die DNA-Analyse zur Identifikation des Täters die Revolution, der Quantensprung in der Kriminalistik ist. Also will die Polizei dieses Instrument auch uneingeschränkt anwenden. Jeder Täter ist für sie ein potentieller Wiederholungstäter.

Die Polizei sagt: Neue Verbrechensformen wie Terrorismus und organisierte Kriminalität erfordern eingriffstiefere Instrumente, um den Tätern nicht nur hinterherzulaufen.
Wer hier den verfassungsgemäßen Nachweis der Erforderlichkeit und der Verhältnismäßigkeit der Eingriffe einfordert, setzt sich dem Vorwurf des Täterschutzes aus.

An welche personenbezogenen Daten will die Wirtschaft heran?
Die Wirtschaft will vor dem Hintergrund sinkender Zahlungsmoral, eines hohen Vollstreckungsschutzes etwa für Mieter und Schuldner, angesichts hoher Arbeitslosigkeit und immer unsicherer werdender Einkommensverhältnisse den Kunden personalisieren und bewerten, durchschauen und bewerben. So wird der Kunde z.B. in seiner Kreditwürdigkeit sowie seiner Zahlungsfähigkeit und –willigkeit kategorisiert, mit einem Scorewert belegt. Heute fällt kaum noch eine kommerzielle Entscheidung ohne Scoring- oder Rating-Verfahren. Der Kunde soll auch in seinem Verbraucherverhalten erfasst und für gezielte Werbung erschlossen werden. Um dies durchzusetzen, wird Personalisierung immer stärker zwingende Zugangsvoraussetzung für die Teilnahme am Konsum. Dies führt zu einem Verlust der Möglichkeit der Anonymität für den Bürger, für den Kunden.

Aber empfindet es der Fußballfan als etwas Negatives, wenn er Karten zur Weltmeisterschaft nur noch personalisiert kaufen kann, dafür sogar seine Personalausweisnummer angeben muss und sich verpflichtet fühlt, sich mit einer Nutzung seiner Daten für Werbezwecke einverstanden zu erklären? Oder überwiegen für ihn die Vorteile der Online-Buchung gegenüber einem langen Anstehen nach Karten und einem versprochenen Ausschluss des Schwarzmarktes.

Die durch immer kostengünstigere Genanalyse erzielbaren Aussagen über die genetische Disposition eines Menschen lassen die Begehrlichkeit von Arbeitgebern, Versicherern und sonstigen Interessenten steigen, diese Daten zur Risikoabschätzung zu erlangen.

Gibt es Anonymität im Internet? Wurde das Internet am Anfang als die große Freiheit, als der virtuelle weltweite Abenteuerspielplatz erlebt, in den anonym eingetaucht werden konnte, so haben alle schnell lernen müssen, dass Missbrauch, Betrug, Hacker, Spam, Passwort-Fishing die Illusion der Anonymität des Internets zerschlug. Zwar besteht die Forderung, dass man sich auch im Internet, d.h. im virtuellen Leben, so anonym bewegen können müsse, wie man es im realen Leben könne. Nur stimmt bereits diese Prämisse gar nicht mehr, denn auch im realen Leben können wir uns wegen der Technikabhängigkeit und permanenten elektronischen Erfassung kaum noch anonym bewegen.

Wie stark ist das Grundrecht auf informationelle Selbstbestimmung gegenüber diesen Begehrlichkeiten?

Staatlicher Bereich:
Gesetzliche Einschränkungen des Rechts auf informationelle Selbstbestimmung sind weitgehend zulässig, da die Anerkennung des Rechts auf informationelle Selbstbestimmung durch einen Gesetzesvorbehalt „erkauft“ wurde.

Der Gesetzesvorbehalt hat nicht eingriffshemmend gewirkt. Vielmehr hat der Gesetzgeber in Bund und Ländern von der Einschränkungsmöglichkeit des Rechts auf informationelle Selbstbestimmung durch Gesetz massiv Gebrauch gemacht, wobei trotz eines hohen Detaillierungsgrades der Regelungen letztlich Abwägungsklauseln zur Anwendung kommen. Die Gesetzgeber haben dabei mehrfach den Grundsatz der Verhältnismäßigkeit verletzt und die verfassungsrechtlich einzuhaltende Grenze der Erforderlichkeit der Eingriffe überschritten und mussten von den jeweiligen Verfassungsgerichten in ihre Grenzen verwiesen werden.

Bereich der Wirtschaft:
Die ständig steigenden Gefährdungen der informationellen Selbstbestimmung durch die Wirtschaft sind nur schwer mit gesetzgeberischen Maßnahmen zu bekämpfen, da sich das Recht auf informationelle Selbstbestimmung in seiner Abwehrwirkung in erster Linie gegen den Staat richtet. Das Bundesdatenschutzgesetz ist insoweit ein „Papiertiger“.
Die Wirtschaft nutzt auf der Grundlage des Prinzips der Vertragsfreiheit ihre Angebotsmacht dazu aus, den Kunden über Anreizsysteme, Kundenbindungsprogramme sowie abverlangte

Einwilligungserklärungen zu personalisieren und zur Preisgabe seiner persönlichen Daten zu bewegen. Stichworte: Preisausschreiben, Gewinnspiele, Bonus-Cards, Lifestyle-Umfragen.
Die – meist pauschale – Einwilligung des Kunden in z.B. eine „Bearbeitung seiner Daten zu Marketingzwecken“, auf die sich die Marketingstrategen und Callcenter bei Telefonwerbung berufen, erfüllt dabei wegen fehlender Bestimmtheit sehr oft nicht die gesetzlichen Anforderungen an eine wirksame Einwilligung.

Welche rechtspolitischen Fragestellungen ergeben sich daraus?

Sehen wir uns – ausgelöst durch den 11.9.2001 – auch in Deutschland einer staatlichen „Überproduktion“ von Sicherheit ausgesetzt, die weit über den Bereich der Terrorismusbekämpfung hinausgreift? Ist der 11.9. die Einstiegsdroge für Überwachungsphantasien?

Nehmen wir wahr, dass der Bereich, in dem sich der Bürger unbeobachtet und unerfasst bewegen kann, immer enger wird, dass der Bürger auch durch gesetzestreues Verhalten einer Überwachung nicht mehr ausweichen kann?

Fühlen wir uns dadurch in unserem Recht auf freie Entfaltung unserer Persönlichkeit beeinträchtigt oder empfinden wir dies als Preis für mehr Sicherheit? Welche „Sicherheit“ ist genug? Welche Risiken müssen/wollen wir in Kauf nehmen?

Nehmen wir den Verlust von Anonymität überhaupt wahr?

Akzeptieren wir angesichts der technisch basierten Informationsgesellschaft, dass Privatheit, d.h. Unbeobachtetheit und Bewegungsfreiheit, letztlich nur noch durch Technikabstinenz erlangt werden kann?

Fühlen wir uns durch den Verlust der Anonymität in unserer Entscheidungsfreiheit gefährdet oder empfinden wir Personalisierung als Entscheidungshilfe und Serviceleistung?

Sind wir angesichts des bevorstehenden Einsatzes der RFID-Technologie zur Warenkennzeichnung und Kaufverhaltenserfassung für eine gesetzliche Verpflichtung der Wirtschaft, alternativ auch anonymisierte Formen des Konsums anzubieten z.B. White Cards, Guthabenkonten etc.?

Nehmen wir die starke Zunahme von Datenströmen gerade auch im nicht-öffentlichen Bereich, die zu einer immer engeren Verknüpfung aller Daten führt, wahr und erkennen wir, dass es damit technisch möglich wird, durch Profilbildung das Verhalten eines bestimmten Menschen ohne dessen Wissen und Wollen abzubilden und ihn für Dritte berechenbar zu machen?

Sind wir gewillt, gesetzliche Regelungen zur Beschränkung der Profilbildung und des Scoring-Verfahrens sowie zur Begrenzung zentraler Auskunftssysteme zu schaffen und damit zur Stärkung des Rechts auf informationelle Selbstbestimmung des Bürgers beizutragen?

Halten wir es für erforderlich, Arbeitgebern, Versicherern etc. zu untersagen, Daten über die genetische Disposition des Menschen zur Risikoabschätzung zu verwenden?

Effektiver Datenschutz setzt einen verlässlichen rechtlichen Rahmen voraus, der den Umfang und die Grenzen zulässiger Datenverarbeitung klar umreißt und die Rechte und Pflichten aller Beteiligten eindeutig festlegt. Infolge der rasanten technischen Entwicklung und neuer Sicherheitsherausforderungen droht jedoch die Gefahr, dass der Datenschutz ins Hintertreffen gerät.

Die Dynamik der Informations- und Kommunikationstechnik, die fortschreitende Digitalisierung und Miniaturisierung sowie eine gleichzeitige Produktverbilligung bewirkt zwar einerseits eine Erleichterung und Verbesserung der Lebens- und Arbeitsbedingungen, ermöglicht aber andererseits neue Formen des Missbrauchs und der Gefährdung des informationellen Selbstbestimmungsrechts des Einzelnen.

Der Gesetzgeber muss diese Gefahren für den Datenschutz erkennen und gewillt sein, Datenschutz seinem Verfassungsrang entsprechend auch gegenüber neuen gesellschaftlichen Herausforderungen und neuen technischen Entwicklungen und Gefährdungen durchzusetzen und problemadäquate Normierungen zum Schutz des Persönlichkeitsrechts und der Privatsphäre zu schaffen.