Transparenz der Verantwortung in Behörden

12/2005

Von Dr. Philipp Sonntag / Büro Berlin der PI Patent Interconsulting GmbH und Mitglied der c-base Berlin

www.philipp-sonntag.de www.c-base.org/crew/sonntag/ und www.patent-interconsulting.com/

Beitrag auf dem 22C3 Chaos Communication Congress in Berlin, am 29. 12. 2005 um 12 Uhr

Inhalt

Wir brauchen eine neue, gesellschaftlich breit überzeugende Lösung für das Problem mit dem Datenschutz. Derzeit geht die Aushöhlung der Persönlichkeitsrechte durch schrittweise Einschränkung des Datenschutzes weiter, einseitig mit Hinweisen auf abzuwehrende Gefahren. Die Abwägung zwischen Erfordernissen wegen Gefahren einerseits und Privatsphäre andererseits sollte in allen Institutionen der Demokratie strukturell verankert sein. Ein Beitrag hierzu wäre, dem „gläsernen Bürger“ eine „gläserne Verwaltung“ zur Seite zu stellen. Erst bei Transparenz der Verantwortung kann eine demokratische Kontrolle greifen.

Es hilft wenig, den gesellschaftlichen Nutzen von Datenzugriffen generell zu leugnen. Beispielsweise wäre für den Katastrophenschutz ein weitgehender Zugriff auf eine breite Palette von Daten praktisch hilfreich. Diese Aussage gilt bis in die persönlichen Daten des Einzelnen hinein, wenn für ihn – z. B. nach einem Unfall, einem Terror-Anschlag oder einer Katastrophe – durch eine reichhaltige Gesundheitskarte medizinische Daten präzise und rasch verfügbar wären. Dieselbe oder eine ähnliche Karte könnte dem Besitzer rasche Abfertigung bei Kontrollen am Flughafen garantieren.

1) Laufende Verschärfung der Kontrollen

Die Verschärfung wird penetranter. Hauptgrund: Bedrohungen durch Terroristen wachsen mit Qualität und Quantität von Waffentechnik und –handel. Die Fülle der amerikanischen Biowaffenforschung und die Verfügbarkeit von Biolabortechnik machen Geheimhaltung unmöglich. Radioaktivität ist ebenso wenig kontrollierbar wie die Kombination von immer präziseren Waffen, vor dem Hintergrund von kommerziell breitem Waffenhandel und Gewaltbereitschaft von Behörden wie dem CIA[1].

Dies ermöglicht den Bau von leichten, mobilen und weitreichend zielsicheren Raketen, preisgünstig und in wachsender Qualität. Aktuell wurde versucht, Bodenluftraketen in die USA zu schmuggeln, welche für Angriffe auf Passagierflugzeuge gebaut sind[2]. Inzwischen hängt es mit von der Politik der „Schurkenstaaten“ ab, inwieweit jede Stadt weltweit zur Geisel der Terroristen wird, denn die Abwehr von Massenvernichtungswaffen wird mehr als das hundertfache des Angriffs kosten.

Die Risiken im Zusammenhang mit dem menschlichen Faktor sind schon lange bekannt[3]. Auch eine noch so krasse Einschränkung der Demokratie mit „technisch perfekten Kontrollen“, schließlich in Richtung „jeder gegen jeden“ wird das Problem nicht lösen. Eine Chance bietet eine transparente, mit begründetem Vertrauen in sich gefestigte Gesellschaft.

2) Wachsendes Misstrauen zwischen Staat und Bürgern

Das Misstrauen wächst mit den Zugriffsoptionen des Staates.

Es entspricht einer natürlichen Tendenz jeglicher Bürokratie und Verwaltung, sich Zugriff zu verschaffen. Resultat ist ein aktuell wachsendes Misstrauen zwischen Staat und Bürgern. Um dieses aufzulösen muss Transparenz an der richtigen Stelle etabliert werden. Der Bürger bekommt zu hören: „Wer nichts zu verbergen hat, der hält seine Daten nicht zurück.“ Aber genau den Staatsdienern, die mit diesem Argument kommen, misstraut der Bürger aus schlechter Erfahrung, weil eben gerade einige dieser plakativ Angepassten dazu neigen, sich intolerant gegenüber unangepassten Minderheiten zu verhalten.

Der Bürger fürchtet, dass öfters als in der Presse zu lesen, Daten für einen Zweck erhoben und dann für einen anderen missbraucht werden, sei es gegen vielfältige Minderheiten, für Indiskretionen, bei Bewerbungen usw.

3) VORSCHLAG: Transparenz der Verantwortung in Behörden

Hierfür gibt es eine juristisch klare, dem Stand der Technik entsprechende und politisch gut begründbare Lösung:

---

[1] CIA MANUAL – A STUDY OF ASSASSINATION. In: die Datenschleuder, Heft 074, 2001, S. 17 - 24

[2] Härpfer, Susanne: Wehrhafter Adler – obwohl es in den USA die Raketenabwehr für Flugzeuge gibt, begint die EU erst mit der Entwicklung – zur Freude der Industrie. In: Tagesspiegel, 21. 11. 2005

[3] Sonntag, Philipp: Verhinderung und Linderung atomarer Katastrophen. Osang, 1981, S. 100 ff

Transparenz der Verantwortung in Behörden:

- **Es dürfen Daten <u>erhoben</u> werden, für die es eine vernünftige, einigermaßen plausible Begründung und eine gesetzliche Regelung gibt – das ist für praktische Zwecke wie z.B. Katastrophenschutz zumeist gut argumentierbar**
- **Ebenso dürfen die Daten für begründete Zwecke <u>weitergegeben</u>, <u>verarbeitet</u> und <u>verwendet</u> werden**
- **Neu: Bei jeder Erhebung, Weitergabe, Verarbeitung und Verwendung muss bei jedem Datensatz zweifelsfrei mit <u>notiert</u> werden: Wofür? Warum (kurze sachliche Begründung)? Wer (praktische Durchführung ebenso wie entscheidende Verantwortung)? Wo? Wann? Aufbewahrung?**

Das heißt nicht, dass man möglichst viele Daten erfassen soll. Der genetische Fingerabdruck wird sehr selten bei Straftaten gebraucht[4]. Der Unfug, Vaterschaft genetisch nachzuforschen, hat in vielen Familien Unheil angerichtet. Für sinnvolle Daten muss Transparenz technisch hergestellt und demokratisch abgestimmt werden.

4) Transparenz mit Gütesiegel

Der Umgang mit Daten des Bürgers in den zugehörigen Verwaltungen soll mit passender Hard-, Soft- und Braínware zertifiziert werden, am besten mit Gütesiegel aktiv und passiv gesichert. Die Verwendung von nicht zertifizierten Daten muss möglichst wirkungsvoll durch Software verhindert werden, die Umgehung dieser Software strafbar sein.

Ziel ist, dass es keinen Datensatz, nicht mal ein einzelnes Datum geben darf, bei dem nicht der ganze Weg von der ersten Aufzeichnung über alle Kopien, Verarbeitungen, Verwendungen etc. bis hin zur letzten Nutzung mit notiert worden ist.

Dies ist für moderne Datentechnik überhaupt kein Problem. Die Strafen für eine Verletzung der Regeln müssen eindeutig begründet (klare Verletzung von Vorschriften) und ausreichend sein. Datenschützer müssen mehr Zugriff als bisher haben und jede Verletzung muss in einer der Sache angemessenen Art und Weise, zumindest in anonymisierter Form veröffentlich werden.

5) Transparenz der Verantwortung

Ein Gütesiegel bewirkt, dass jeder Staatsdiener in einer seiner Aufgabe optimal entsprechenden Form <u>abwägen</u> wird, ob und wenn ja wie er die kritischen Daten nutzt. Es kann je nach Situation ebenso ein Übergriff sein, sie zu nutzen wie ein Versäumnis sie nicht zu nutzen. Dabei sollen die Strafen oder sonstige Nachteile bei Fehlern in aller Regel gering oder Null sein. Nur bei ersichtlich

[4] Burkhard Hirsch, Tagesspiegel 5. Nov. 2005, S. 5

willkürlichen Entscheidungen und bei klaren Verletzungen gültiger Vorschriften sollte es Konsequenzen geben, und nur vor solchen Verletzungen hat der Bürger Angst. Das Gütesiegel ist gut mit dem Konzept einer „maschinenlesbaren Regierung“ vereinbar, wie es Wau Holland, Gründungsmitglied des CCC, sie im CCC vorgeschlagen hatte.

6) Behörden und Terroristen je mit besten Daten

Behörden und Katastrophenschützer einerseits und Terroristen andererseits sind in einer je mit besten Daten geführten Auseinandersetzung um die Infrastruktur und ihre demokratische Kontrolle. Transparente Verantwortung würde strukturelle Demokratie etablieren. Stattdessen werden bisher die Behörden durch Datenschutz stark behindert – während zugleich der Datenschutz unzureichend ist und laufend durch neue Techniken und Vorschriften weiter eingeschränkt wird. Eine „Gläserne Verwaltung“ (Kurzbezeichnung für Transparenz der Verantwortung in Behörden, teils auch in entsprechenden Dienstleistungsfirmen etc.) löst diese Probleme grundlegend und schafft sich wesentlich höhere Effektivität und Effizienz.

7) Einhaltung der Datenschutzgesetze wäre nur mit Transparenz demokratisch wirksam

Im Grunde ermöglicht erst die gläserne (Verantwortung der) Verwaltung eine korrekte Erfüllung bestehender Gesetze. So verlangt das Bundesdatenschutzgesetz[5] gerade die Bereitstellung derjenigen Daten, welcher erst bei der gläsernen Verwaltung richtigerkennbar und verfügbar würden:

> BDSG § 19: Auskunft an den Betroffenen
>
> (1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über
>
> 1. Die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und
>
> 2. den Zweck der Speicherung.
>
> In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden .....

Transparenz der Verwaltung würde eine wertvolle Option eröffnen: Derzeit soll man als Bürger möglichst genau angeben, was man woraus wissen will. Mit Hilfe von elektronischen Daten, Koordination der Ämter und Suchfunktionen würde zum ersten Mal gläsern, ob und wo überhaupt eigene Daten vorhanden sind: Das wäre ein enormer Informationsgewinn nicht mehr nur gegen, sondern nun auch für den Bürger.

Hilfreich, jedoch leider nicht bei personenbezogenen Daten, ist das IFG[6].

Leider ist die Demokratie von krankhaftem Misstrauen infiziert. Das zeigt der peinliche Umgang mit den Bundesbeauftragten für den Datenschutz[7]:

---

[5] Bundesdatenschutzgesetz (BDSG) vom 20. September 1990, zuletzt geändert durch Gesetz vom 17. Dez. 1997, § 19

[6] IFG – Gesetz zur Förderung der Informationsfreiheit im Land Berlin, vom 15. Okt. 1999 und: Berliner Beauftragter für Datenschutz und Akteneinsicht: Informationszugangsrecht, S. 7

[7] ebd. § 19 Absatz (6)

> (6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

Natürlich darf der Betroffene, wenn er zugleich ein Verdächtigter bei begründeter Gefahr für den Staat ist, nicht über Erkenntnisse der Behörde informiert werden, solange die Gefahr begründet ist. Peinlich für die Demokratie ist aber, dass man dem Bundesbeauftragten für den Datenschutz Daten verweigert und ihm offenbar nicht zutraut, mit der Weitergabe an den Betroffenen verantwortlich im Sinne des Staates umzugehen. Zu aller mindest müsste eine zeitlich verzögerte, vollständige Auskunft an ihn und durch ihn gewährleistet sein.

8) Interaktive Verwaltung – Stand der Technik und Usancen bei „Moderner Staat 2005“ [8]

Aktuell angedacht und vorbereitet und teils praktiziert wird die interaktive Verwaltung, über elektronische Medien, mit Bürgerkarte, Internet, Biometrie, elektronischer Signatur (gemäß Signaturgesetz) etc. Dabei bringen multifunktionale Chipkarten „erhebliche datenschutzrechtliche Probleme mit sich“ [9], und „Grundvoraussetzung für die Zulässigkeit multifunktionaler Bürgerkarten ist die Abschottung der einzelnen Funktionsbereiche voneinander. Nur wenn dies technisch sichergestellt werden kann, ist die Hinzunahme weiterer Funktionen hinnehmbar“. Ein umständlicher Weg.

Es ist daher wünschenswert, dass dieser aktuell sowieso zu leistende Aufwand an Hard- und Software die Erfordernisse einer gläsernen Verwaltung baldmöglichst einbezieht. Ähnlich haben sich die Informationsbeauftragten geäußert: „Deutschland muss für mehr Verwaltungstransparenz sorgen“ [10].

Auf der 9. Fachmesse und Kongress „Moderner Staat“ am 29. und 30. November 2005 in Berlin wurde eine Fülle kommerzieller Software zu E-Government angeboten, für eine Einbeziehung der Bürger und Unternehmen in das Verwaltungshandeln über das Internet und andere Medien. Dabei wurde deutlich, dass bereits teilweise Ansätze zu einer transparenten Verwaltung realisiert wurden und klare Absichten in diese Richtung gehen, wenn auch überwiegend aus vagen Hoffnungen auf Bürokratieabbau und Verringerung der Kosten.

Ein Schritt in Richtung der gläsernen Verantwortung ist das deutsche Signaturgesetz. Eine nur durch gezielte Software aufzuhebende Spannung besteht

---

[8] www.moderner- staat.de

[9] Konferenz der Datenschutzbeauftragen des Bundes und der Länder: Vom Bürgerbüro zum Internet. Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung; 2000, S. 33 poststelle@lfd.niedersachsen.de

[10] zitiert nach: Berliner Beauftragter für Datenschutz und Akteneinsicht: Dokumente zum Datenschutz, 2001; S. 73

zwischen den Voraussetzungen einer gläsernen Verantwortung einerseits und den Kosten sowie den Ansätzen zu bürgernahen, einfachen Lösungen, etwa der aktuellen Realisierung eines Formulars, welches der Bürger mit dem Adobe Reader (!) ausfüllen und speichern sowie dann die Datei an die Verwaltung senden kann.

Transparenz schafft das Signaturgesetz für einen Kreis von Zugangsberechtigten, in aller Regel rein intern je für eine Behörde, je mit einer Insellösung, und zwar in direkter individueller Umsetzung mittels unterschiedlicher Produkte aus den Angeboten der Softwarehäuser (wie Bol, Oracle, SAP, SER, Siemens etc).

Ansätze in Richtung einer gläsernen Verantwortung der Behörden sind beispielsweise die Betonung der Nachvollziehbarkeit, Rekonstruierbarkeit, Revisions- und Manipulationssicherheit von Aktenvorgängen in Behörden[11], ebenso die Betonung der Rechtssicherheit der digitalen Identität von Menschen und Objekten in der elektronischen Welt, vor allem speziell für Hochsicherheitsbereiche „für citizen, business und government“[12], ebenso die Betonung von „safety First“ für personenbezogene Daten, mit „Berechtigungsebenen“ bei denen der jeweilige Benutzer nur auf solche Funktionen zugreifen „darf“ (= können soll), die seiner Aufgabe innerhalb der Organisation entsprechen, wofür es „Anwenderprotokolle“ und „Prüfprotokolle“ gibt[13]. Bei der aktuell kommerziell angebotenen Software mehrerer Firmen ist es möglich, Zugangskriterien für Nutzer zu etablieren und deren Aktionen für später rekonstruierbar mit dem jeweiligen Datensatz zu verbinden – was fehlt ist der noch demokratisch zu regelnde Zugriff von außen.

Treibende Kraft sind vor allem praktische Vorteile[14] (hier in verkürzter Darstellung):

- Integration und Standardisierung von Funktionen, Reduzierung von Aufwand an Funktionen, Zeit, Kosten
- Antragstellungen durch den Bürger jederzeit und von zu Hause aus, jederzeit interaktiv gesteuerter Zugriff auf Formulare, automatische hinweise auf unvollständige oder fehlerhafte eigene Eingaben
- Automatisierte Lenkung, Automatisierung und Zugriffsfähigkeit der Dokumente

Die „Gesellschaft für Effizienz in Staat und und Veraltung e.V.[15] „kämpft für“ die potenziellen Vorteile wie Stärkung der Privatinitiative und Eigenverantwortlichkeit sowie Vereinfachung und Beschleunigung der Verwaltungsabläufe und „kämpft gegen“ Einengung der Freiräume des Bürgers und insbesondere gegen

---

[11] SER: Integriertes Government Content Management für den modernen Staat / PRODEA (PRocess Oriented Document related Enterprise Application), S. 29

[12] SMC: Stark wie ein Baum – SMC Kryptographie, S. 1 und SMC-Trust® (Flyer)

[13] ORACLE: Die menschliche Komponente – Oracle Human Resources Management System, S. 10

[14] Strakeljahn, Uwe (IT-Leiter der Stadt Melle): eGovernment aus kommunaler Sicht. Beitrag auf dem „Best Practice Forum“ bei Fachmesse und Kongress „Moderner Staat 2005“

[15] www.gfe-deutschland.de

„anonymes Staatshandeln“ (!) sowie „Ungewollte Folge- und Nebenwirkungen von Gesetzen und Gerichtsentscheidungen“.

Ein weiteres durchgreifende Gesetz ist das Dritte Verwaltungsverfahrens-änderungsgesetz. Seine Regelungen stellen das elektronische Dokument mit qualifizierter elektronischer Signatur dem traditionellen Schriftsatz (Unterschrift mit blauem Kugelschreiber / Tinte) gleich. Die Folge sind einer Reihe von (De-) Regulierungsanforderungen und –optionen[16].

Relativ weniger problematisch sind Vorgänge, welche nicht mit persönlichen Daten der Bürger zu tun haben, sondern mit der Beteiligung der Bürger an Verwaltungsentscheidungen. Ein Beispiel ist die Anwendung eines Bürokratieabbaugesetzes in einer Modellregion[17]. Auf einer DIN A4 Seite erhält der betroffene Bürger Aussagen zur jeweiligen Projektbezeichnung („Bereich“), Problemstellung, Lösungsvorschlag, Gesetzesgrundlage, zu den zu erwartenden Auswirkungen und zur Zuständigkeit in der Verwaltung. Organisation und Finanzierung dieser mediengestützten Bürgernähe sind verbesserungsfähig und werden kontrovers diskutiert, so z.B. in den Zeitschriften „move – moderne verwaltung“[18] und „kommune21“[19]

Ziel ist eine einheitliche Sicherheitsinfrastruktur, wofür bereits Standards definiert wurden wie SASCIA (Signature Alliance Signature Card Interoperable API) für die Schnittstelle zwischen Kartenleser und Signaturkarten, das geht in Richtung einer umfassenden Chipkarte für den Bürger, mit der er an den standardisierten Schnittstellen alle für ihn relevanten Informationen erhalten könnte[20].

Die Einbeziehung der gläsernen Verwaltung wäre zunächst ein zusätzlicher Aufwand, sie kann jedoch für die kommerziellen Ziele positive Aspekte einbringen wie eine Verstärkung von Bürokratie- Abbau, Sicherheit und Akzeptanz.

9) Datenschutz und - benutz der EU

Die Richtlinie 95/46/EG will aus wirtschaftlichen und konservativen Gründen die Hindernisse für den freien Datenverkehr aus dem Weg räumen, „ohne den Schutz von personenbezogenen Daten zu beeinträchtigen“ [21], das betrifft „Verarbeitungen“ wie das Erheben, Speichern und Weitergeben von Daten. Die Bestimmungen klingen wie die weit verbreitete Verniedlichung von dahinter verborgenen Problemen. Wenn man sie wörtlich nimmt, sollten gute Chancen bestehen, die gläserne Verwaltung politisch durchzusetzen, gestützt auf Formulierungen wie etwa (ebda S. 8 ff, S. 12):

---

[16] Ernst, Tobias: Modernisierung der Wirtschaftsverwaltung durch elektronische Kommunikation. Carl Heymanns Verlag, 2005, 268 S.

[17] Modellregion für Bürokratieabbau – OstwestfalenLippe (OWL); Initiative „Witschaftsnahe Ver3altung“, Zwischenbericht 2004

[18] move – moderne verwaltung, insbesondere aktuell in den Heften 2 und 3/2005; siehe auch www.move- online.de

[19] kommune21 – E-Government, Internet und Informationstechnik, insbesondere Heft 12/2005; siehe auch www.kommune21.de

[20] Stahl, Ernst und Markus Breitschaft: Gute Karten. In: kommune21, 12/2005, S. 18 - 19

[21] Datenschutz in der Europäischen Union. Amt für amtliche Veröffentlichungen der EG, Luxemburg, S.5

- Sie haben das Recht, über alle Arten der Datenverarbeitung informiert zu werden, die Sie betreffen ... die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung und alle weiteren Informationen wie z.B. die Empfänger der Daten ...
- Personenbezogene Daten dürfen nur verarbeitet werden, wenn der Betroffene aus freien Stücken zugestimmt hat

All das wird zur Farce, wenn die Nachvollziehbarkeit menschlichen Verhaltens technisch abrufbar wird, ohne persönliche Einwilligung und ohne gesetzliche Grundlage. Zunehmend „unterhalten“ sich, verstärkt durch „pervasive computing“ und kostensparendes Delegieren an „die Technik“, Datensysteme bei Behörden und besonders Industrie miteinander, ohne dass ein Mensch im Einzelnen zuschaut oder gar verantwortlich kontrolliert. Es geschehen Schritte in Richtung gläserner Bürger, die selbst mit gläserner Verwaltung bedenklich wären[22]:

> Die Europäischen Justizminister und die Europäische Kommission möchten die Telefon- und Internetverbindungsdaten aller 450 Millionen Europäer aufzeichnen..... Vorratsdatenspeicherung ist eine Maßnahme, welche die Überwachungsbefugnisse in bislang nicht gekanntem Maße ausweitet....

10) Nur wer im Glashaus sitzt, wirft nicht mit Steinen

Befürworter ebenso wie Gegner einer starken Überwachung des Bürgers könnten mit einer Gläsernen Verwaltung besser leben:

- Befürworter: Technokratische Terrorismus-Bekämpfer fordern möglichst weitgehende Überwachung der Bürger – und fast jeder Bürger gehört einigen als dubios betrachtbaren Minderheiten an. Eine gläserne Verwaltung ist für diese Befürworter zwar ungewohnt, aber wenn sie selbst nichts zu verbergen haben, dann sollte eine Transparenz der Verantwortung für sie attraktiv sein.
- Gegner: Wer die zu weitgehende Überwachung der Bürger fürchtet, wird ein Instrument begrüßen, das im, Ungang mit der Datenfülle eine verantwortungsbewusste, abwägende statt hortende Verwaltung erzeugt.
- Und unentschlossen Abwägende? Wer sich zwischen mehr und weniger Überwachung nicht entscheiden kann, braucht einen neuen Ansatz: Die feinfühlig demokratische Abwägung wird mit in die Verwaltung gelegt und genau dafür lassen sich klare Regeln präzisieren.

11) Praxisgegenstände und Aufgaben der Realisierung

[22] www.dataretentionisnosolution.com

Die Einschränkungen der Grundrechte seit 1994[23] bezeichnen zugleich die **Bereiche**, für die ich die gläserne Verantwortung der Verwaltung als besonders wichtig betrachte:

- Das Verbrechungsbekämpfungsgesetz erweitere Befugnisse der Geheimdienste und erleichterte ihre Zusammenarbeit mit der Polizei
- Die Telekommunikationsgesetze (TKG und TKÜV) verpflichtete Kommunikationsdienstleister, den Zugriff der Geheimdienste zu erleichtern
- Mit dem „Großen Lauschangriff“ wurde der Grundgesetzartikel 13, Unverletzlichkeit der Wohnung, geändert. Mit aktuell verfügbaren und zukünftigen Techniken wird unweigerlich die demokratiefeindliche Wirksamkeit über optische und akustische Überwachung hinaus erweitert werden.
- Sicherheitspakete, insbesondere zum Ausländerrecht und zu Kontenabfragungen, auch für Sozial- und Finanzamt, werden viel Erbitterung bis hin zu Gewaltbereitschaft verursachen
- Handys können als Peilsender verwendet werden. Nicht zuletzt die psychischen Schäden können gravierend sein, wenn man immer weniger Anhaltspunkte hat, um zwischen Verfolgung und Verfolgungswahn zu unterscheiden
- Pervasive Computing mit Verfahren wie RFID, Biometrie und Ubiquitous Computing (in Kleidung eingewobene Computer, mit Sensoren und Funk) geben über jeden Ort, jeden Gegenstand und jedes Lebewesen eine Fülle von Überwachungsdaten preis. Bei integriert systemischer Auswertung resultieren Verhaltensprofile, die von tendenziösen Fragebogen und Kriterien zu vorprogrammierten Verdächtigungen und Schuldzuweisungen führen. Die „Kontextsensitivität“[24] der dezentralen und teilselbstständigen Mini-Computer führt zu einer Eigendynamik der Bewertung von Situationen und der Steuerung von Aktionen in der Gesellschaft, gezielt ohne menschliche Kontrolle.
- Der gefährlichste sich abzeichnende Schritt sind Implantate mit Emotionsüberwachung und vorprogrammierter Psycho-Pharmakavergabe, jeweils wenn bestimmte Gehirnareale Aktivität melden. Das wird ohne gesellschaftliche Gegensteuerung innerhalb der Psychiatrie beginnen und sich über Gefängnisse und Altersheime hinweg weiter ausweiten.

Dies alles kann – ohne gläserne Verantwortung der Verwaltung – zu einer Eskalation der Überwachung und Gängelung führen.

Eingriffe: Derzeit speichern die Telefongesellschaften Verbindungsdaten ihrer Kunden als Grundlage der Rechnungen und zu individuellen Auskünften an

---

[23] Reuter, Markus und Johann.M. Hoffmann: Mit Sicherheit ein guter Bürger. In: Schwarzlicht 2/2005, S. 13

[24] Lorenz Hilty Siegfried Behrendt, Mathias Binswanger, Arend Bruinink, Lorenz Erdmann, Jürg Fröhlich, Andreas Köhler, Niels Kuster, Claudia Som, Felix Würtenberger: Das Vorsorgeprinzip in der Informationsgesellschaft - Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt, Seite 8
TA 46/2003; Studie des Zentrums für Technologiefolgen-Abschätzung, www.ta-swiss.ch und Institut für Zukunftsstudien und Technologiebewertung (IZT), Berlin, www.izt.de

den Kunden. Strafverfolgungsbehörden können zugreifen. Die Bundesregierung will Unternehmen verpflichten, alle Telefon- , SMS-, E-mail- und Internetdaten ihrer Kunden mindestens zwölf Monate lang zu speichern. Gespeichert werden soll, wer mit wem kommuniziert und wer welche Internetseite besucht, nicht aber der Inhalt der Kommunikation oder der Internetseiten[25]. All dies wäre bei gläserner Verwaltung demokratisch verträglich.

Gezielt erreichbare Vorteile: Umgekehrt kann ein Bürger seine eigene Situation durch Bereithaltung seiner persönlichen Daten vereinfachen, wenn dies mit technischen Standards eingerichtet worden ist[26]: Kreditkarten sind weitaus sicherer als Kennkarten bzw. Führerscheine. Es sollte freiwillig möglich sein, eine mit vielen, auch biometrischen und gesundheitlichen Daten bestückte IT-Kennkarte zu haben, mit der man z.B. viel einfacher und schneller in einen überwachten Flughafen gelangt, weil die Daten mit dort schon gespeicherten abgeglichen werden können.

Gewöhnung an Vor- und Nachteile einer Gläsernen Verwaltung: In Schweden macht schon seit dem Jahr 1766 das inzwischen im Grundgesetz verankerte „Öffentlichkeitsprinzip“ eine wache Demokratie möglich[27]: „Danach sind alle in einer Behörde vorhandenen Akten und Dokumente – auch elektronisch gespeicherte – für die Allgemeinheit zugänglich. Offenheit ist die Grundregel, Geheimhaltung die Ausnahme. Wenn Daten nicht herausgegeben werden, muss dies begründet werden. Dem Antragsteller steht der Klageweg offen. Meistens geben die Gerichte dem Einspruch statt. Durch das Öffentlichkeitsprinzip sind auch Protokolle von Polizeiverhören, Fotos, die für Pässe eingereicht werden, oder Dienstabrechnungen der Minister für jeden einsehbar.“

12) Folgeschäden bleiben gewollt unbekannt

Der Bürger will wissen: Welche Folgen haben staatliche Aktionen für ihn? Etwa: Die eigene Wohnung würde bei einer (knappen) Überflutung der Deiche 1 m tief im Wasser stehen. Der nächster Zufluchtsort wäre XY, mit Lagezeichnung.

Dies würde übliche, bisher weitgehend ungewohnte Technikfolgeabschätzungen zu staatlichen Projekten voraussetzen. Verwaltungen und Politiker haben ein feines Gespür dafür, die Folgen Ihrer Handlungen zu vertuschen, indem solche Folgeabschätzungen systematisch verweigert, verhindert, ignoriert, jedenfalls äußerst selten finanziert werden. Das krasseste Beispiel ist die Schließung des OTA (Office of Technology Assessment in Washington, genau deshalb, weil es jahrelang hervorragende Arbeit geleistet hatte und somit die Power von Lobbyismus in Bereichen wie Sicherheit, Ökologie, Wirtschaft eingeschränkt hatte.

Diese Vermeidung von Studien zu Folgeschäden widerspricht dem Prinzip einer gläsernen Verantwortung in Behörden. Schäden werden verdeckt. Dinge, die wir befürchten, geschehen laufend und bleiben unbemerkt, ein Beispiel: Die für den Mensch größte, unmittelbarste und schädlichste Umweltverschmutzung ist die Massenvergabe von psychiatrischen Beruhigungsmitteln,

[25] Tagesspiegel 15. 3. 2005, S. 2
[26] Ellison, Larry: A Techie’s Solution. In: Newsweek, Oct. 2001, S. 68
[27] Lemkemeyer, Sven: In Schweden sind die Akten gläsern – Das Öffentlichkeitsprinzip erschwert die Korruption“, in: Tagesspiegel, 26. 07. 2002

wie es insbesondere an Heimbewohnern geschieht. Die technische Tendenz geht in Richtung von Sensorik wie zur Messung des Blutzuckerspiegels und der vorprogrammierten Abgabe von Insulin aus einem Implantat innerhalb des Körpers. Dies wird seit über 15 Jahren präzisiert. Im Zuge der Kostenersparnis und schematisierten Verantwortungslosigkeit durch „Kontrolle“ besteht die Gefahr dieses System für die Verabreichung von Psychopharmaka bei Erregung des Patienten zu automatisieren. Auch wer wund liegt, würde dann so „kostensparend beruhigt“. Es ist eine Frage des Bewusstseins: Mit interdisziplinärer Transparenz könnten endlich Übergriffe wie die Massenvergabe von psychiatrischen Medikamenten ähnlich verfolgt und geahndet werden, wie derzeit die Vergabe kleinster Mengen von bestimmten Aufputschmitteln etc. beim Sport.

13) Emotionale Verarbeitung

Der gläserne Bürger ist ein Analphabit: Es hat nur geringe Kenntnisse vom Umgang mit Computern, Telekommunikation, Software, Überwachungstechniken und den ihn betreffende Gesetzen. Behörden entscheiden nicht „in dubio pro reo“, sondern „in irritatione pro institutione“.

Vieles ist heute bis ins Intime hinein deutlich weniger geschützt als vor einem Jahrzehnt und wird teils genüsslich dargeboten. Sogar breite Videoüberwachung wäre emotional verkraftbar, sobald die gläserne Weiterverarbeitung sichergestellt ist. Der Betroffene will es wissen, so würde Vertrauen aufgebaut, Überwachung effektiv. Erst dann könnte Überwachung die Terrorakte teils verhindern, teils die Verfolgung von Terroristen verbessern. Auch die Abwehr von unerwünschten Aktionen, etwa von Stalkern, von automatisiert- penetranten Werbeaktionen usw. könnte bei hoher Transparenz besser gewährleistet werden.

14) Aktuelle Aufgabe: Die technische, juristische und praktische Machbarkeit der gläsernen Verwaltung im Detail darlegen und Ihre Auswirkungen demokratisch steuern

Die gläserne Verwaltung ist kein Automatismus. Erster Schritt wäre eine interdisziplinäre Studie, welche die Machbarkeit herausarbeitet und ihre laufende Präzisierung ermöglicht, indem sie die demokratischen Konsequenzen ebenso beim Ansatz wie bei den Auswirkungen evaluativ etabliert. Ein interdisziplinäres Verbund- Projekt zur Ausarbeitung der Studie würde vor allem diese Aspekte einbeziehen:

- Die technische Machbarkeit, bei gesellschaftlicher Feinabstimmungen und demokratischer Steuerung
- Die laufende differenzierende Evaluation, Kriterien zur Hard- und Software für die Präzisierung und Stärkung der gläsernen Verantwortung
- Die integrative Impact- Analyse für demokratische Prozesse und Akzeptanz.