



What the fuck
is informationelle Selbstbestimmung?!

Inhalt

- 4 Vorwort
- 6 Stop 1984: Warum Datenschutz?
- 9 Stop 1984 in aller Kürze
- 11 Der gläserne Schüler
- 13 Videoüberwachung
Die Realität im Lichte des Datenschutzrechts
und der Restvernunft
- 20 Nein zur elektronischen Gesundheitskarte!
- 25 Komitee für Grundrechte und Demokratie
- 27 RFID-Chips
- 31 Persönlichkeitsrechte ade –
die „Aufenthaltskarte für Ausländer“
- 37 Alltag Überwachung
- 48 Online-Festplattendurchsuchung
- 49 Rasterfahndung
- 54 Freiheit oder Sicherheit?
- 60 Arbeitnehmerdatenschutz
- 65 Forum InformatikerInnen für Frieden und
gesellschaftliche Verantwortung e.V. (FifF)
- 66 Anonym im Netz – eine kleine Einführung
- 69 Wer die Kontrolle hat, dem gehört die Zukunft!
- 74 Die Deutsche Vereinigung für Datenschutz

Vorwort

„ Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. 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 unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Informationen dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte

(Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. “

Diese Worte, anstelle eines langen Vorwortes, stammen aus dem Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983. Fast 25 Jahre später scheint das Recht auf informationelle Selbstbestimmung keine Bedeutung mehr zu haben: Vorratsdatenspeicherung, Anti-Terror-Datei, Videoüberwachung, RFID-Chips – immer mehr Daten werden gesammelt, immer mehr neue Kontroll- und Überwachungsmöglichkeiten entstehen.. Mit dem Argument eines erhöhten Sicherheitsbedürfnisses des Staates werden datenschutzrechtliche Bedenken überstimmt. Kritische Stimmen gibt es wenige, Protest regt sich kaum.

Zum zweiten Mal gibt der Allgemeine Studierenden Ausschuss (AStA) der Fachhochschule Münster/Steinfurt eine Broschüre zum Thema Datenschutz heraus. Die erste Broschüre erschien im Sommersemester 2006 mit dem Schwerpunkt Videoüberwachung und wurde von einer Veranstaltungsreihe begleitet. Dieser Schwerpunkt war nicht zufällig gewählt. Die

Hochschulverwaltung der FH plant schon seit 2004 die Überwachung der Rechner-Pools und der Hochschulbibliotheken mit Kameras. Dass die NutzerInnen der Pools bisher noch unbeobachtet an den Computern arbeiten können und weder sie, noch die Bildschirmhalte für Wochen gespeichert werden, ist dem erfolgreichen Intervenieren der Landesdatenschutzbeauftragten und dem AStA zu verdanken. Einen ausführlichen Artikel zu diesem Thema und die Broschüre findet ihr unter folgendem Link:

<http://www.astafh.de/wp-content/uploads/2006/12/videoueberwachung.pdf>

Wir bedanken uns bei allen Autorinnen und Autoren für ihre Artikel, dem AStA der Uni Münster, den ReferentInnen des Referats für Politische Bildung/Demokratische Rechte: Eva Plaschke und Tim Ackermann, der Kunstakademie Münster, der Fachschaft Geschichte (Uni Münster), der Fachschaft Soziologie (Uni Münster), der Fachschaft Oecotrophologie (FH Münster) für ihre Unterstützung und bei Lena Schall und Johannes Munding für die grafische Umsetzung.

Euer FH - AStA



Stop 1984: Warum Datenschutz?

Warum Datenschutz und Privatsphäre für jede/n Bürgerin und Bürger wichtig sind und wodurch diese grundlegenden Rechte bedroht sind, ist ein Thema, dessen Aspekte sich nicht ohne Weiteres trennen lassen: Eines greift fast direkt ins andere über.

Zunächst einmal: Für Datenschutz und Privatsphäre einzutreten bedeutet nicht, zum vielfach von Kritikern propagierten „Paranoiker“ zu werden.

Aluhüte sind sowohl nutzlos als auch unmodisch - und Datenschutz beginnt ohnehin schon viel früher und im alltäglichen Leben jedes Einzelnen.

An unseren Daten sind zunächst zwei wesentliche Interessengruppen interessiert: Auf der einen Seite die Regierung bzw. deren Organe von Sicherheit und Ordnung, auf der anderen Seite die private Wirtschaft. (Weitere Interessengruppen sind denkbar, lassen sich für die Zwecke dieses Artikels jedoch der einen oder anderen Gruppe beordnen.)

Die Regierung benötigt unsere Daten für Zwecke der Verwaltung,

der inneren Sicherheit sowie für die Statistik. Private Wirtschaftsunternehmen sind eher an der Erstellung von Konsumentenprofilen, der Kundenbindung und der Steuerung des Konsumverhaltens interessiert. In gewissen Bereichen spielen auch bei der privaten Wirtschaft Sicherheit (z.B. bei der Verhinderung von Ladendiebstählen), Verwaltung (z.B. Kundenadresssätze) und Statistik (z.B. Lokalisierung von „Ladenhütern“) eine Rolle.

Einige zentrale Fragen für die Beurteilung einer Datenerfassung könnten lauten:

- Wer will meine Daten haben?
- Welche Daten sollen erfasst werden?
- Wie bzw. wo werden diese Daten gespeichert?
- Welche Zugriffsberechtigten wird es geben?
- Wie lange werden meine Daten gespeichert?
- Wodurch wird Mißbrauch verhindert?
- Was kann ein Unberechtigter schlimmstenfalls mit diesen Daten anfangen?

Die Liste läßt sich natürlich fortsetzen - dies würde jedoch den Rahmen des Artikels sprengen.

Bei einfachen Beispielen läßt sich die Notwendigkeit von Datenschutz noch leicht erkennen: Das Paßwort für die Online-Spieleseite muß im Regelfall nicht so streng geheim gehalten werden wie die PIN-Nummer für die EC-Karte:

Kann im ersten Fall schlimmstenfalls ein Fremder in meinem Namen neue Highscores erspielen, bedeutet Datenmißbrauch im zweiten Fall möglicherweise hohe finanzielle Verluste.

Bei komplexeren Fragestellungen wie der Erfassung biometrischer oder gentechnischer Daten auf Ausweisen, der Video- und Audioüberwachung öffentlicher Plätze inklusive „Mustererkennung“ von Bewegungen oder Sprache oder den Kundenkartensystemen großer Handelsketten ist die tatsächliche oder denkbare Gefahr des Mißbrauchs nicht ganz so offensichtlich. Viele Risiken werden auch erst erkennbar, nachdem die Daten längst erfaßt worden sind und der „Inhaber“ jede Kontrolle über deren Verbreitung und Verwendung verloren bzw. abgegeben hat.

Beispiel Gendaten: Gegenwärtig werden beim so genannten „genetischen Fingerabdruck“ zum Zwecke der erkennungsdienstlichen Behandlung keine verwertbaren Genomdaten erfasst. Doch bereits jetzt gibt es Überlegungen der Versicherungen, mittels Genuntersuchungen beispielsweise das Risiko von Erbkrankheiten auszumachen, um die Versicherungsprämien gegebenenfalls entsprechend anzupassen. Dazu wird aber die Erfassung vollständiger Gendatensätze erforderlich sein. Vor wenigen Jahren konnten nur grobe Erkenntnisse daraus gezogen werden, doch die Technik schreitet stetig voran. Welcher Versicherte kann mit Sicherheit ausschließen, dass zehn Jahre nach der Erstuntersuchung der immer noch vorliegende Gendatensatz erneut untersucht wird, um dann beispielsweise bestimmte Sexualpräferenzen oder eine Affinität für riskante Lebensweisen festzustellen? Oder wer könnte sicher ausschließen, dass

diese Daten nicht einfach falsch interpretiert werden?

Ähnliches gilt für Daten wie z.B. „Welche Internetseiten hat XY aufgerufen?“, „Wen hat XY angerufen bzw. von wem wurde XY angerufen?“, „Wo hat sich XY zum Zeitpunkt A aufgehalten?“ oder „Welche Einkäufe hat XY getätigt?“. All dies sind Dinge, deren Verwendungszweck von „belanglos“ über „lästig“ bis „bedrohlich“ reichen können - auch ohne dass jemand „etwas zu verbergen“ hat. (Wer wirklich etwas verbergen will, wird im Übrigen immer Mittel und Wege dazu finden).

Wenn diese Daten noch dazu über einen längeren Zeitraum gespeichert werden, kann man gegebenenfalls noch Monate oder gar Jahre später nachvollziehen, was ein Einzelner getan hat - möglicherweise genauer, als der Betroffene selbst sich jemals erinnern könnte.

So wurden z.B. eine Vielzahl von Personen durch die Polizei Bad Segeberg vorgeladen. Der Grund: Laut Auswertung ihrer Handy-Einbuchungsprotokolle waren die Betroffenen zum Zeitpunkt einer Brandstiftung in der Nähe des Tatortes.

Ähnlich besorgniserregend ist die immer weiter um sich greifende Kameraüberwachung, z. T. mit Tonaufzeichnung. Niemand der Beobachteten weiß mit Sicherheit, was mit den Bild- und Tondaten geschieht, auf welche Kriterien das gewonnene Datenmaterial untersucht wird und wer Zugriff auf die gewonnenen oder vermuteten Erkenntnisse hat.

Stop1984 in aller Kürze

Allein diese kleinen Beispiele zeigen schon, dass der informationellen Selbstbestimmung in Deutschland, besonders im Zeichen der (vorgeblichen) Sicherheitserhöhung und Terrorismusbekämpfung ein immer geringerer Stellenwert eingeräumt wird. Es sollte aber jedem Einzelnen bewusst sein, dass das Preisgeben von Daten und Informationen stets die Gefahr des Missbrauchs birgt, das für sich genommen belanglose Datensätze miteinander verknüpft werden können (und werden!), und dass diese verknüpften Informationen erhebliche Folgen haben können: Vom „gläsernen Konsumenten“ bis hin zu falschen Verdächtigungen seitens der Sicherheitsorgane.

Oberstes Gebot beim täglichen, persönlichen Datenschutz sollte also sein:
Stets so wenig Daten wie möglich überlegt preisgeben. (z.B. auf Kunden-Rabattkarten verzichten, wenn dafür umfassende persönliche Daten preisgegeben werden müssen und das Konsumverhalten durchleuchtet werden soll.)

Die im Mai 2001 entstandene NGO (Nicht-Regierungs-Organisation) STOP1984 befaßt sich mit dem Schutz von Bürgerrechten bzw. der Aufklärung, in welcher Weise diese bedroht sind. Ein Schwerpunkt liegt auf dem Recht auf informationelle Selbstbestimmung sowie dem Recht auf Privatsphäre. Darüber hinaus befassen wir uns mit vielen verwandten Themen, von tagesaktuellen Geschehnissen auf lokaler Ebene bis hin zur Zensur in China.

Der Name unserer Gruppe stammt von dem 1948 von George Orwell verfassten Roman „1984“, in dem ein Staat die Überwachung und Meinungsmanipulation bis zur Perfektion verbessert hat: Selbst die Gedanken werden kontrolliert. Das Individuum schwindet vor dem „Großen Bruder“, dem übermächtigen und unsichtbaren Kontrollapparat, immer mehr dahin. Begriffe wie Selbstentfaltung, Meinungsfreiheit und Individualität sind bedeutungslos geworden. War diese Namensgebung zu Beginn noch überspitzt zu verstehen,

zeigen die Bestrebungen nach „möglichst totaler Sicherheit“ seit den Terroranschlägen des 11. September 2001, dass die Wirklichkeit mitunter die Fiktion schneller einholt, als einem recht sein kann.

Wir wollen verhindern, dass mit „Totschlagargumenten“ wie ‚Wer nichts zu verbergen hat, muß auch nichts befürchten‘ eine Basis auf politischer und sozialer Ebene geschaffen wird, auf der Überwachung und Kontrolle des Individuums sich immer weiter ausbreiten kann und schließlich (z.B. bei einem politischen Paradigmenwechsel oder einer Verschiebung der Mehrheitsverhältnisse auf Bundes- oder EU-Ebene) in der Errichtung eines totalitär anmutenden Staates münden könnte.

STOP1984 verfolgt keine klare politische Linie. Im Gegenteil setzen wir uns dafür ein, dass jede demokratisch legitimierte Partei bzw. jede legale Interessengruppe frei am politischen Entscheidungsprozess teilnehmen können soll. Auch unangenehmen Ansichten muß auf gesellschaftlicher Ebene begegnet werden können, statt durch simples Wegsehen oder gar technische Filtermaßnahmen die Illusion zu erwecken, es gäbe diese Ansichten gar nicht. Unsere Ansicht ist: Man kann nur gegen etwas sein, wenn man es betrachten, untersuchen und diskutieren kann. Mit dieser radikalen Einstellung zur Meinungsfreiheit werden wir gelegentlich auch scharf angegriffen - aber der Konsens innerhalb unserer Gruppierung ist: Meinungsfreiheit ist für alle da. Oder, um Voltaire zu zitieren: „Ich finde Ihre

Der gläserne Schüler

Meinung widerlich und kann keinem Ihrer Worte zustimmen, aber ich werde alles daran setzen, damit Sie sie sagen können.“ Denn beginnt man erst damit, eine Gruppe auszugrenzen, weil man ihre Ansichten nicht gutheißen kann, ist der Gedanke naheliegend, diesen Weg weiterzugehen...

Das bedeutet aber zugleich, dass STOP1984 sich mit keiner der politischen Gruppierungen oder Richtungen identifiziert oder gemein macht. STOP1984 ist bestrebt, politisch so neutral wie nur möglich zu bleiben.

Das spiegelt sich in gewissem Maße auch in der Organisationsstruktur von STOP1984 wider: Wir sind eine offene Gruppe von Leuten, bei der sich jede/r Interessierte einbringen kann, und zwar mit so viel Zeitaufwand und mit den Fähigkeiten, die jemand mitbringt. Einige von uns suchen im Internet nach Neuigkeiten, die in unseren beliebten täglichen Nachrichtenverteiler (DailyNews) einfließen, andere kümmern sich um die Technik der Webseite <https://www.stop1984.com> bzw. um den Server, auf dem diese Webseite und unsere themenbezogenen Mailinglisten laufen.

Bei aktuellen Anlässen wird auf den jeweiligen Mailinglisten dann jemand gesucht, der beispielsweise einen Flyer zu einer Demo erstellt oder sich um das Übersetzen eines Textes kümmert. Diese Struktur ist aber keine Einbahnstraße: In gleicher Weise kann jemand, der eine Aktion vor dem örtlichen Supermarkt plant oder eine Internet-

Radiosendung vorbereiten will, auf den Listen gezielt nach Unterstützern mit Rat und Tat suchen.

Bei einer solchen Organisation bleibt es nicht aus, dass die Ansichten einzelner Mitstreiter mitunter stark voneinander abweichen - doch wir alle verfolgen ein erklärtes Ziel:

Wir wollen ein Bewußtsein für den Datenschutz schaffen.

Wir wollen den Menschen den Wert ihrer eigenen Privatsphäre, den Wert ihrer eigenen Daten und die Gefahren des Datenmißbrauchs bewußt machen. Wir wollen die möglichen politischen, sozialen und persönlichen Folgen einer zunehmenden Überwachung und die Gefahr des politischen Desinteresses verdeutlichen.

Dieses Ziel ist nur durch engagierte und interessierte Bürgerinnen und Bürger zu erreichen. Daher ist STOP1984 bestrebt, mit Aufklärung, Berichterstattung und Aktionen Interesse und Bewusstsein zu fördern und den Einzelnen zum Nachdenken anzuregen.

Schüler-IDs sollen die gesamte Bildungskarriere nachvollziehbar machen — das war 2006 einen BigBrotherAward wert.

Die Schülerin/der Schüler soll „gläsern“ werden sagen die Datenschützer, die Kultusministerkonferenz (KMK) nennt das die „Umstellung der Schulstatistik auf Individualdaten mit bundeseinheitlichem Kerndatensatz“. Was ist darunter zu verstehen?

Es begann mit PISA

Die Kultusministerkonferenz –also die Konferenz der KultusministerInnen der Länder- erklärte bereits im Jahr 2000, sie wolle die Voraussetzungen für eine umfangreichere und länderübergreifende Datenerhebung schaffen. Wir erinnern uns: 2000 war das Jahr der PISA-Studie. Deshalb wurde dieser Vorstoß auch damit begründet, eine bessere Datengrundlage für eine bessere Bildungsvermittlung schaffen zu wollen. Eine Schulstatistik, die u.a. auch dem Bundesamt für Statistik zukam, existierte damals bereits. Sie verzeichnete jedoch nur anonymisierte Gruppenerhebungen. Im

Mai 2003 stimmte die Konferenz der 16 Schulamtschefs der Länder einer Umstellung auf individualisierte Datenerhebung einstimmig, mit Enthaltung von Sachsen, zu. Festgelegt wurde dabei der „Kerndatensatz“, der in ein „nationales Bildungsregister“ eingespeist werden sollte. Bereits im Schuljahr 2003/04 erfolgte die Umstellung in Schleswig-Holstein, 2005 und 2006 kamen fast alle weiteren Länder hinzu, die Ausnahme bildet das weiterhin skeptische Sachsen. 2006 gewann die KMK damit den BigBrotherAward der Datenschutzorganisation foebud im Bereich „Verwaltung und Behörden“ für herausragende Mängel im Datenschutz.

Die Datensammlung

Die Verabschiedung des Kerndatensatzes, betrifft nicht nur SchülerInnen. Er enthält ebenso Daten zu der Berichtsschule, den Kursen der Schule, den Schulabgängern und Absolventen, den Lehrkräften und weiteren optionalen Merkmalen. Die einzelnen Datensätze sind dabei untereinander verknüpfbar. Aber bleiben wir bei den Schülerinnen und Schülern.

Für die bedeutet die Datensammlung konkret: jeder Schülerin/jedem Schüler wird eine Identifizierungsnummer zugeordnet (das ist die sogenannte Schüler-ID), die für die gesamte Schullaufbahn gleich bleibt. Anhand dieser ID werden nun diverse persönliche Daten erhoben und in ein „nationales Bildungsregister“ eingespeist. Die Daten umfassen Geschlecht, Geburtsdatum und Konfession,

Einschulung, Schulwechsel und Sitzenbleiben, sowie den besuchten Unterricht und die Teilnahme an bestimmten Fördermaßnahmen, zudem die Herkunft und bei nicht-deutschen SchülerInnen die zu Hause gesprochene Sprache.

Mit dem obigen Datensatz lässt sich nun also feststellen, „dass etwa in Afghanistan geborene männliche Schüler in Hamburg häufiger als in Bayern Latein als dritte Fremdsprache haben.“ Was man daraus wohl für Schlüsse für die Bildungspolitik ziehen könnte? Natürlich gar keine. Interessant sind die Daten dagegen für andere: allen voran die Arbeitgeber und die Banken. Auch wenn diese bisher keinen Zugang zu den Daten haben sollen – der Ruf danach wird sicherlich laut und die Möglichkeit besteht. Immerhin gibt es bereits Überlegungen aus den Kultusverwaltungen eine zentralen Zugriff der KMK zu schaffen und nicht nur anonymisierte, sondern auch Daten „in individueller Form für den Verwaltungsvollzug zu nutzen“. Was das genau sein soll, weiß allerdings kein Mensch.

Zuletzt

Offiziell sind die SchülerInnenendaten zwar vertraulich zu behandeln. Aber die entsprechenden Datenschutzbestimmungen sind kaum vorhanden. Zugriffs-, Berechtigungs- und Anonymisierungskonzepte fehlen ebenso wie Bestimmungen zum Schutz der Datenübertragung. Mal ganz abgesehen von einer klaren Zweckbestimmung der Datensammlung. Es bleibt also dabei: zuerst wird gesammelt, dann kann man ja weiter sehen.

Annelie Kaufmann

Videoüberwachung

Die Realität im Lichte des Datenschutzrechts und der Restvernunft

Heutzutage kann man wohl durch kaum eine deutsche Stadt mehr gehen, ohne früher oder später, bemerkt oder unbemerkt in das Blickfeld einer Kamera zu geraten. Ob in Fußballstadien, Einkaufspassagen, auf Autobahnen, an Universitäten, Bahnhöfen, oder anderen öffentlichen Plätzen: Die Überwachung durch Videokameras ist auf dem Vormarsch. Seit dem 11. September 2001 steht die Legitimität der Einschränkung von Freiheit zu Gunsten der Sicherheit verstärkt auf dem Prüfstand. Unterschiedliche Interessengruppen leisten ihren Beitrag in der öffentlichen Debatte um die Verschärfung von Sicherheitsgesetzen und die damit einhergehende Lockerung der demokratischen Rechte. Und während noch diskutiert wird (oder während das Fußball-WM-Fieber tobt...) werden die einen oder anderen Gesetzesvorlagen (sogenannte „Sicherheitspakete“), die schon lange in den Schubladen geschlummert haben, verabschiedet.

Die Tangente des Datenschutzrechts

Bei durch Videoüberwachungen gewonnenen Bildern handelt es sich um so genannte personenbezogene Daten, jedenfalls solange eine Person darauf identifizierbar und nicht nur grob schemenhaft zu erkennen ist. Mit den Möglichkeiten der Digitaltechnik ist das meistens der Fall und damit beantwortet, weshalb die Videoüberwachung datenschutzrechtliche Belange tangiert.

Die „W-Fragen“: Was ist relevant?

Zunächst interessiert die Frage, wer überhaupt Videoüberwachungskameras aufhängt und an welchen Orten. Dabei ist einmal zu unterscheiden zwischen öffentlichen und privaten Betreibern. Diese Unterscheidung bezieht sich auf deren rechtliche Stellung: bei privaten handelt es sich beispielsweise um Privatpersonen, Vereine oder Firmen, bei öffentlichen um städtische oder kommunale Einrichtungen, Universitäten, etc. Relevant ist diese Unterscheidung für die Frage, an wen man sich zu wenden hat, sollte man nähere Informationen wünschen oder gegen die Kameras vorgehen wollen.

Wesentlich wichtiger für datenschutzrechtliche Bedenken ist allerdings der Ort, an dem die Videokameras aufgehängt werden: auch hier wird zwischen öffentlichem und privatem Raum unterschieden. Gemeint ist die öffentliche Zugänglichkeit der betreffenden Orte, die sowohl im Freien als auch in Gebäuden liegen können. Dem gegenüber steht die begrenzte Zugänglichkeit, die nur einem be-

stimmten Personenkreis den Zutritt gewährt. Aus dieser Unterscheidung ergeben sich verschiedene rechtliche Maßstäbe: Die Überwachung öffentlicher Räume ist an strengere Vorgaben gebunden, die Anforderungen an die Verhältnismäßigkeit der Maßnahme stellt und den Betroffenen Rechte gewährt, um sich gegen diese Maßnahme zur Wehr zu setzen.

Öffentliche Orte, die Videoüberwacht werden, gibt es viele, nehmen wir das Beispiel Frankfurt am Main: So sind im Hauptbahnhof knapp 150 und am Flughafen mehrere hundert Kameras installiert, auf dem Messegelände sind Dutzende im Einsatz und auch die „Konstablerwache“, offener Platz und S- und U-Bahn Station an der belebten Einkaufsstraße „Zeil“ wird seit zwei Jahren videoüberwacht. Dort geht die Reichweite der Kameras übrigens weit über das ursprünglich definierte Ziel, die Konstablerwache, hinaus: Die Kameras erfassen auch umliegende Balkone und Fenster.

Des Weiteren ist von Interesse, auf welche Art die Videoüberwachung organisiert ist. Zur Gewährleistung des Datenschutzes ist zunächst vonnöten, dass die Betreiber einer Videoüberwachungsanlage ein Verzeichnis anlegen, in dem unter anderem der Zweck und die Rechtsgrundlage der Überwachungsmaßnahme bestimmt werden.

Vor In-Betriebnahme ist dann eine „Vorabkontrolle“ vorgeschrieben, die regelmäßig durch den behördlichen Datenschutzbeauftragten erfolgt.

Das Beispiel der Universität Münster zeigt deutlich, wie unbedarft die Betreiber in datenschutzrechtlichen Fragen sein können oder wie dreist sie versuchen, sich möglichst wenig Aufwand zu machen: So gab es zu dem Zeitpunkt, zu dem Studierende die Videokameras bemerkten, lediglich ein so unvollständiges Verzeichnis, dass die

Landesdatenschutzbeauftragte aufgrund des Informationsmangels nicht einmal eine Kontrolle durchführen konnte. Dies zeigt deutlich wie wichtig es ist, dass BürgerInnen

aufmerksam sind und nachhaken, wenn sie eine Videokamera sehen.

Rechtlich ist weiterhin von Belang, ob eine bloße Beobachtung durch optisch-elektronische Anlagen stattfindet, etwa durch eine Person, die die Vorgänge vor der Kamera über einen Monitor verfolgt, oder ob eine weitere Verarbeitung der so gewonnenen personenbezogenen Daten geschieht in Form von Speichern, Verändern, Übermitteln, Sperren und Löschen. Erlaubt sind diese Verarbeitungen grundsätzlich nur zu demselben Zweck, zu dem die Daten erhoben werden dürfen, was als Zweckbindung bezeichnet wird. Aber natürlich gibt es auch hier Ausnahme. Die Verarbeitung durch Speicherung ist jedenfalls bei Weitem keine Seltenheit.

Ein Beispiel für die Speicherung und Planung der zweckungebundenen Weitergabe von Daten ist das deutsche Mautsystem. Bisher nur zur Abrechnung der LKW-Maut benutzte Daten sollen zukünftig der Strafverfolgung zur Verfügung stehen. Im Dienste der Inneren Sicherheit wird das Verhalten der einzelnen Menschen an den maßgeblichen Netzknoten der Verkehrsinfrastruktur überwacht und nachvollzogen. Besonders nach spektakulären Fällen, wie der Festnahme eines unter Mordverdacht stehenden LKW-Fahrers, stoßen solche Eingriffe auf wenig Widerspruch.

Für die von der Videoüberwachung Betroffenen ist wichtig, dass mit ihren Daten kein Missbrauch betrieben werden kann. Dazu gehören die Wahrung des Datengeheimnisses, die Verhinderung unbefugten Zugriffs, die sichere Übermittlung aber auch die Verfügbarkeit der Daten, also deren Schutz vor Verlust oder Zerstörung, so dass sie jederzeit die Möglichkeit haben, auf diese zuzugreifen.

Damit man aber überhaupt die Chance hat, sich mit diesen Maßnahmen auseinanderzusetzen, muss die Videoüberwachung erkennbar sein, was durch eine Beschilderung der videoüberwachten Bereiche geschehen kann. Dann erst ist es den Betroffenen möglich, ihre Rechte auf Auskunft, Einsicht, Löschung, Anrufung des/der Landesbeauftragten für Datenschutz und gerichtlichen Schutz geltend zu machen.

Auch dieses Erfordernis wird nicht immer erfüllt. Wiederum das Beispiel der Universität Münster: Hier fehlten Hinweise völlig und auf die mehrfach mit Nachdruck vorgebrachte Aufforderung wurden Schilder aufgehängt, die man ihrerseits suchen muss.

Greifbare Zukunft: Was Kameras noch alles können

Einen kleinen Vorgeschmack darauf, wie Videoüberwachung schon jetzt erprobt wird und in naher Zukunft funktionieren könnte, bietet die Möglichkeit der biometrischen Gesichtserkennung. Am Mainzer Hauptbahnhof testet das Bundeskriminalamt mit 200 Freiwilligen in einem viermonatigen Pilotprojekt, ob sich Gesichter in Menschenmassen eindeutig per Überwachungskamera identifizieren lassen. Mit dieser so genannten Foto-Fahndung sollen zukünftig Straftäter oder Verdächtige automatisch entdeckt werden können, indem die Aufnahmen mit einer Foto-Datei abgeglichen werden. Auch anlässlich der Fußballweltmeisterschaft 2006 montierte die Polizei Kamerasysteme, die mit einer Software zur Gesichtserkennung ausgestattet sind, in der Umgebung von Stadien, an öffentlichen Plätzen und an Verkehrsknotenpunkten, um die Gesichter von Passantinnen und Passanten automatisch mit den Datenbeständen der Polizei abzugleichen.

Die letzte „W-Frage“: Allgemein übliche Begründungen und deren Kritikwürdigkeit

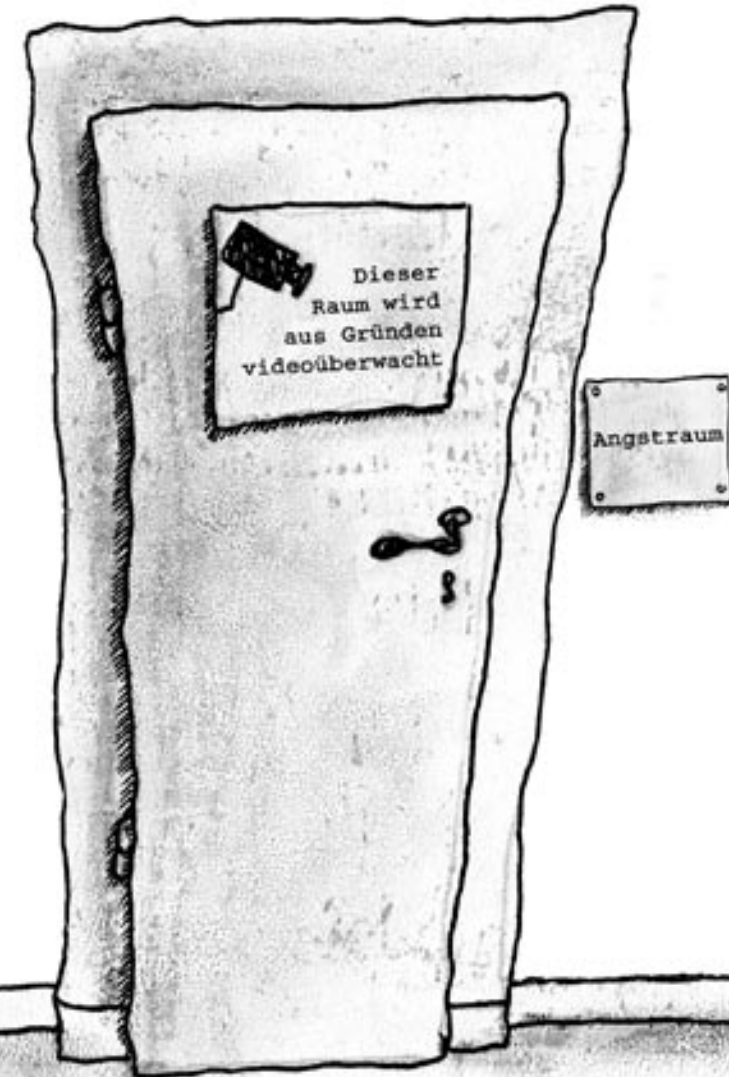
Grundsätzlich gilt zunächst, dass der Zweck der Videoüberwachung dem Schutz von Personen oder Sachen dienen muss, wobei zumindest eine abstrakte Gefahr vorliegen muss, dass Sachen beschädigt oder gestohlen werden könnten, oder dass Personen verletzt werden. Zusätzlich kommt eine Überwachung durch Videokameras nur in Betracht, insofern es keine Möglichkeit gibt, die Gefahren durch weniger grundrechtsbeeinträchtigende Maßnahmen zu verhindern, beispielsweise durch eine ständige Anwesenheit von Sicherheitspersonal. Und abschließend kann selbstverständlich eine Abwägung mit dem schutzwürdigen Interesse der Betroffenen nicht unterbleiben.

In der Regel gibt es zwei „Erfolge“, die mit der Videoüberwachung erreicht werden sollen: erstens die Abschreckung potentieller Straftäter, zweitens die Erhöhung des subjektiven Sicherheitsgefühls und damit der Abbau sogenannter „Angsträume“.

Ersterem ist entgegenzuhalten, dass sich potentielle Straftäter durch Videoüberwachung nicht von ihren Vorhaben abhalten lassen. Erfahrungen aus Staaten mit exzessivem Einsatz von Kameras

(USA, Großbritannien) berichten von einer Verlagerung von Kriminalitätsschwerpunkten in nicht überwachte Gebiete. So finden Hauseinbrüche nicht mehr von der videoüberwachten Straßenseite aus statt, sondern durch den Garten. Drogenszenen ziehen um an die nächste Straßenecke. Überwachung von einzelnen Gebieten führt also lediglich zu Verdrängung von Straftaten in andere Bereiche. Dies kann aber keinesfalls ein Argument sein, eine totale Überwachung einzuführen, sondern steht zunächst nur für die Tatsache, dass Videoüberwachung nicht hält, was sie verspricht. Hierbei wäre allerdings anzumerken, dass die Verdrängung nicht selten sogar ein gewünschter Effekt ist, um prestigeträchtige Viertel wieder salonfähig zu machen. Der soziale Abstieg anderer Viertel wird dabei mit einkalkuliert. Häufig wird die Videoüberwachung für stadtkosmetische Maßnahmen gegen drohende Ordnungswidrigkeiten von Obdachlosen, Junkies oder Punkern eingesetzt. Dafür sind die Instrumente des Polizeirechts jedoch nicht geschaffen.

Die zweite Begründung ignoriert, dass es sich bei dem angeblichen Erfolg eben tatsächlich nur um ein subjektives Gefühl handelt. Objektive Sicherheit wird nur vorgetäuscht, Kameras greifen bei einer Straftat nicht ein. Im videoüberwachten Raum besteht sogar die Gefahr, dass BürgerInnen



wegen der vorgetäuschten Sicherheit durch die Anwesenheit einer Kamera davon absehen, in einer Notsituation zu helfen. Spätere Identifizierung mag der Strafverfolgung und Verbesserung der Aufklärungsquote dienlich sein, Verbrechenopfern wird so nicht geholfen.

Die politische Fragwürdigkeit von Videoüberwachung

Beide Argumente werden für gewöhnlich mit der These unterfüttert, dass der „brave Bürger“ nichts zu verbergen habe, sich also von der permanenten Überwachung nicht gestört fühlen könne. Mit der Einführung der Videoüberwachung öffentlicher Räume werden BürgerInnen allerdings dazu gezwungen, die Rechtmäßigkeit des eigenen Verhaltens in Frage zu stellen und sich darüber Gedanken zu machen, ob ihr Verhalten sie verdächtig macht oder ihre Unschuld beweist. Die grundsätzlich geltende Unschuldsvermutung seitens des Rechtsstaats wird de facto außer Kraft gesetzt. Zusätzlich wissen die Betroffenen in der Regel nicht, wie mir ihren Bildern weiter verfahren wird. Anstelle der versprochenen Sicherheit entsteht also ein Höchstmaß an Unsicherheit. Jemand der nichts zu verbergen hat, sollte auch nicht überwacht werden.

Hinzu kommt, dass die Betroffenen im Falle einer Übertragung der Bilder an einen Monitor, der beobachtet wird, stark der Willkür des Beobachtenden ausgeliefert sind. Zu einem überdurchschnittlichen

hohen Prozentsatz werden dabei Menschen mit dunkler Hautfarbe, Angehörige von Minderheiten und auch jüngere Frauen beobachtet. Die Menschen vor der Kamera sind Voyeurismus und Vorurteilen der Beobachtenden hilflos ausgeliefert.

Bei Videoüberwachung handelt es sich zudem um einen Eingriff in das Grundrecht des Einzelnen auf Informationelle Selbstbestimmung, stellte das Bundesverfassungsgericht 1983 im „Volkszählungsurteil“ fest. Zu den Auswirkungen einer jederzeit möglichen Aufzeichnung individuellen Verhaltens äußerte es sich folgendermaßen: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und Informationen dauerhaft gespeichert, verwendet und weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung der Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl.“ (BVerfGE, NJW 1984, 422)

Abschließend...

... bleibt zu sagen, dass die Probleme, die hinter der Videoüberwachung stehen, sozialer Natur sind. Für deren Lösungen werden Konzepte benötigt, die sich um die Ursachen kümmern; der Versuch,

mit Videoüberwachung auf diese Probleme zu antworten, stellt sich in ein fragwürdiges Verhältnis zu den demokratischen Prinzipien des Grundgesetzes. Öffentliche Räume dienen der demokratischen Kommunikation und dem gemeinsamen Miteinander. Jeder kann prinzipiell verlangen dort von systematischer Überwachung in Ruhe gelassen zu werden. Videokameras sind dagegen Ausdruck von Misstrauen und eine Machtdemonstration. Egal, welche Argumente man für den Einsatz von Videoüberwachungskameras vorbringen mag, datenschutzrechtlich bedenklich und politisch inakzeptabel ist er allemal.

Eva Plaschke



Quellen:
www.foebud.org
web.uni-muenster.de/ASTA/index.php
www.heise.de
www.dergrossebruder.org
www.gruene-frankfurt.de
www.jungle-world.com
www.datenschutz.hessen.de

Nein zur elektronischen Gesundheitskarte!

Wer alles unter Kontrolle haben will, weiß nie genug. Der Hunger nach Daten wird in allen Bereichen immer größer, nicht zuletzt weil diese immer schneller und umfassender ausgewertet werden können. Im Bereich der „Inneren Sicherheit“ kennen wir dies allemal. Um die Speicherung von Telefonverbindungsdaten und von DNA-Daten, um die Nutzung der LKW-Mautdaten und den Aufbau von Verdachtsdateien wird der Streit geführt. Auch die medizinischen Daten aller Bürger und Bürgerinnen können jedoch von höchstem Interesse sein. Die Zeiten von Volkszählungsboykott und öffentlichen Auseinandersetzungen um den Schutz privater Daten scheinen leider einem anderen Jahrhundert zu entstammen.

Das Gesundheitsmodernisierungsgesetz von 2003 sieht die Einführung einer neuen - elektronischen - Gesundheitskarte vor. Zum 1.1.2006 sollte dies bereits geschehen sein. Da aber, nicht zuletzt unter Drängen des Bundesgesundheitsministeriums, eine umfassende technische Lösung

gefunden werden sollte, die jeden Datenhunger potentiell stillen können soll, geriet dieses Projekt in Verzug. Sowohl divergierende Interessen der beteiligten Organisationen als auch technische Probleme sind die Ursachen für die Verzögerung. Die Gematik - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH - wurde im Januar 2005 von den 15 Spitzenorganisationen des deutschen Gesundheitswesens gegründet. Ein Industriekonsortium (blThealth) unter Leitung der IBM Deutschland besorgt die wissenschaftliche und technische Begleitung. Die Informatikindustrie kann so – unterstützt von der Bundesregierung – ohne Risiken und auf Kosten der Beitragszahlenden eine neue Technologie entwickeln, die sie an die gesetzliche Krankenversicherung verkaufen und dann weltweit exportieren kann.

Die eGK soll zwei Teile enthalten - einen Pflichtteil und einen freiwilligen Teil. An der Schnittstelle liegt die elektronische Übermittlung der Rezeptdaten, die verpflichtend ist. Ob diese Daten darüber hinaus zentral gespeichert und ausgewertet werden, ist eine der zu stellenden Fragen. Ansonsten enthält der verpflichtende Teil die Daten, die auch bisher auf der Krankenkassenkarte gespeichert sind. Ein Lichtbild kommt hinzu und erweitert die Karte um die Kontrolle ermöglichende Ausweisfunktion. Eine lebenslang gültige Versicherungsnummer bildet die neue Grundlage.

Der freiwillige Teil der eGK soll die Speicherungen von Gesundheitsdaten ermöglichen. Notfalldaten,

Arzneimitteldokumentation, Arztbrief und Patientenakte könnten gespeichert werden. Dies soll nicht auf einem eingebauten Speicher erfolgen, sondern die Karte soll mittels eines Prozessors den Zugriff auf ein Computernetzwerk ermöglichen. Dort sind die Daten zentral gespeichert und können von überall eingesehen werden. Sie sind zwar verschlüsselt und pseudonymisiert, können aber auf die einzelnen PatientInnen rückbezogen werden. Zugänglich werden die Daten, wenn ein Patient gemeinsam mit einem Arzt oder einem Angehörigen der Heilberufe mittels ihres jeweiligen Ausweises den Zugang zu den persönlichen Daten öffnen.

Gesundheitsdaten verraten eine Menge über einen Menschen, über ererbte Anlagen, über Risiken und Empfindlichkeiten, über die Lebensführung. Es sind höchst sensible Daten, die Möglichkeiten der Diskriminierung und Segregation eröffnen, deren Kenntnis und Nutzung einer Verletzung personaler Integrität Tür und Tor öffnen können. Sie ermöglichen eine Stigmatisierung durch Diagnosen, die lebenslang gespeichert bleiben.

„Vergessener“ Datenschutz

Im Gesetz sind einige datenschutzrechtliche Hürden aufgebaut. Einem Placebo gleich tun sie so, als ob Datenschutz in diesem Bereich auf Dauer möglich wäre. So müssen die PatientInnen einer Speicherung ihrer Daten „freiwillig“ zustimmen. Sie entscheiden, ob und was gespeichert wird.

Sie sind die „Herren“ ihrer Daten. Wie soll dieses große Versprechen jedoch in der Praxis eingelöst werden? Woher sollen die selbstbestimmenden BürgerInnen, die als leidende und Rat suchende PatientInnen zum Arzt kommen, Kenntnis über Aussagefähigkeit und Nutzen der Daten haben? Welcher Arzt kann und wird sich die Zeit nehmen, darüber intensiv zu beraten? Was sollten die Kriterien solcher Aufklärung sein? Vor allem aber: Welchen Nutzen hätten die Daten, wenn sie nicht vollständig, sondern interessiert ausgewählt wären und kein Arzt sich darauf verlassen könnte. Entweder bewährt sich also die Freiwilligkeit der Datenspeicherung dahingehend, dass alle zustimmen, oder die Freiwilligkeit muss abgeschafft werden.

Gesetzliche Vorgaben lassen sich schnell ändern, wenn dies im behaupteten allgemeinen Interesse ist. Der Umgang mit dem LKW-Mautgesetz zeigt dies aktuell. Das Gesetz schließt explizit eine anderweitige Verwertung der erhobenen Daten aus. Als die Möglichkeit, mit Hilfe dieser Daten unter Umständen Verbrechen aufklären zu können, propagiert wurde, stand das Gesetz schnell zur Disposition. Wie so oft wurde angeblich aus dem Datenschutz ein Täterschutz.

Zu stellen ist auch die Frage, wo die Gesundheitsdaten gespeichert werden und unter welcher Aufsicht dies geschehen soll. Sie unterliegen dem Arztgeheimnis. Wie kann dies gewährleistet werden, wenn Daten auf vernetzten Servern außerhalb



von Arztpraxen gespeichert werden? Wenn dieses Netz möglicherweise gar privat betrieben wird? Wie sollte dies kontrolliert werden? Dies leitet über zu Fragen nach den Möglichkeiten der Gewährleistung von Datensicherheit.

Denn zu den vielen Fragen nach einem legalen Missbrauch der Daten kommen Fragen nach dem illegalen Gebrauch hinzu. Dies fängt bei der Frage an, ob eine solche Datenmenge überhaupt technisch zu schützen ist. Der Chaos Computer Club bezweifelt dies und beweist immer wieder das Gegenteil.

Eigenverantwortung der Patienten?

Das „Akzeptanzmanagement“, mit dem die Einführung der eGK verbunden ist, verspricht Großartiges. Mehr Wirtschaftlichkeit, mehr Effizienz, Verringerung von Missbrauchspotentialen, Erhöhung der Eigenverantwortung der Patienten, mehr Leistungstransparenz.

Ein Gutachten der Unternehmensberater Booz, Allen, Hamilton rechnet jedoch - statt mit 1,4 Milliarden wie das Bundesgesundheitsministerium - mit 3,9, eventuell auch 7 Milliarden Kosten. Erst nach 10 Jahren würden sich möglicherweise Kosten und Nutzen die Waage halten. Allerdings ist davon auszugehen, dass in den Arztpraxen und Apotheken statt Einsparungen mehr Zeitaufwendungen anfallen.

Mit Blick auf die PatientInnen, wird die Stärkung ihrer Rechte und ihrer Selbstbestimmungsmöglichkeiten in den Mittelpunkt gerückt. Alle Zeichen zeigen jedoch in eine ganz andere Richtung. Ärzte und Patienten werden verstärkt kontrolliert werden. Die Entwicklung in Richtung Entindividualisierung der Behandlung und in Richtung Standardisierung wird mit Hilfe der eGK schnell voranschreiten. Die Daten sollen dazu genutzt werden, Krankheitsbilder, verkürzt auf ICD-Nummern, und ihre Behandlung EDV-tauglich zu machen. Hierfür muss sich die Sicht einer medizinischen Disziplin durchsetzen und andere Sichtweisen dominieren. Individuelle Unterschiede können in diesem allgemeinen und riesigen Informationssystem nicht - oder nur gegen dieses System - berücksichtigt werden. Die Standardisierung betrifft sowohl die ärztliche Behandlung als auch die Lebensstile.

Eigenverantwortung wird so zum Synonym für Fremdkontrolle, die zugleich Eigenkontrolle wird. Der Bürger wird ermächtigt und zugleich ohnmächtig gemacht. Gesundheit wird zu einem Projekt, in dem jeder selbst verantwortlich mit allen Wahrscheinlichkeiten und Risiken umgehen muss. Der Bürger und die Bürgerin haben den Anforderungen an gesundes Leben zu gehorchen und einen den Normen entsprechenden Umgang mit körperlichen Anlagen zu pflegen. Im Zuge dessen wird das solidarische Gesundheitssystem marktförmig umgestaltet. Krankheit wird erneut mit Begriffen von Schuld, Verfehlung und Verantwortung in Zusam-

menhang gebracht und ist privat zu verantworten. Gesundheitliche Risiken werden nur noch in engen Grenzen solidarisch getragen.

Die zeitlichen Verzögerungen des Projekts eGK geben den Bürgern und Bürgerinnen zumindest die Chance, sich genauer mit den geplanten Veränderungen zu beschäftigen und ihren Protest zum Ausdruck zu bringen. (Siehe Aufruf des Komitee für Grundrechte und Demokratie: „Wir sagen Nein!“)

Elke Steven
(Komitee für Grundrechte und Demokratie)

Literatur:

Das große Gesundheitsversprechen und seine große Täuschung. Informationen an alle Bürgerinnen und Bürger, beruflich weiß oder alltäglich gekleidet, über die elektronische Gesundheitskarte; Hrsg.: Komitee für Grundrechte und Demokratie (Aquinostr. 7 11, 50670 Köln, Tel.: 0221 97269 30; Fax: 31, www.grundrechtekomitee.de, info@grundrechtekomitee.de)

Aufruf: Wir sagen Nein!
(Komitee für Grundrechte und Demokratie)

Komitee für Grundrechte und Demokratie

Das Komitee für Grundrechte und Demokratie konzentriert seine Arbeit vor allem auf die Situation der Grund- und Menschenrechte in der Bundesrepublik Deutschland. Die Schwerpunkte, Themen und Aktionen verändern sich. Aktuelle Fragestellungen werden aufgegriffen und bearbeitet. Einige grundlegende Themen beschäftigen das Komitee immer wieder neu. Schwerpunkte der derzeitigen Arbeit seien stichwortartig herausgegriffen: Strafrecht, Haftbedingungen und Gefangenenhilfe; Friedenspolitik; Demonstrationsrecht/-beobachtungen; Flucht, Migration und Asyl; Soziale Bürger- und Menschenrechte; Verletzungen von Grundrechten im Namen der „Inneren Sicherheit“; Neue Technologien (Humangenetik/Biomedizin, Gesundheitssystem); Prozessbeobachtungen; Fragen einer menschenrechtlich-demokratisch nötigen bundesdeutschen und europäischen Verfassung; „Ferien vom Krieg“ für Kinder und Jugendliche aus dem ehemaligen Jugoslawien, Israel und Palästina. Zu vielen dieser Themen sind Arbeitsgruppen tätig, die Aktionen planen, vorbereiten und ermög-

lichen. Zu aktuellen Fragen werden Stellungnahmen oder Pressemitteilungen herausgegeben. Auf Tagungen und in Publikationen werden Hintergründe und Zusammenhänge grundlegender Probleme analysiert. Alljährlich erscheint das Jahrbuch des Komitees für Grundrechte und Demokratie, in dem die vielen Dimensionen konkreter Gefährdungen von Grund- und Menschenrechten aufgezeigt werden. Dort, wo möglich, nötig und sinnvoll, tritt das Komitee für bedrohte Menschenrechte und gegen undemokratische Maßnahmen in Form strikt gewaltfreien symbolischen Handelns direkt ein.

Die Gefangenenbetreuung umfasst einen umfangreichen Briefwechsel mit Gefangenen und Eingaben zur Verbesserung von Haftbedingungen bei den Behörden, aber auch zahlreiche Gefangenenbesuche. Auf Anfrage erhalten Gefangene Literatur in die Justizvollzugsanstalten geschickt. Ein besonderer Schwerpunkt liegt in der kritischen Auseinandersetzung mit der lebenslangen Freiheitsstrafe und ihren repressiven Auswirkungen auf den so genannten Normalvollzug.

Das Komitee für Grundrechte und Demokratie wurde 1980 gegründet. Die Initiative ging aus von Personen, die am Zustandekommen des Russell-Tribunals über die Situation der Menschenrechte in der Bundesrepublik Deutschland (1978/79) beteiligt waren. Die damals formulierten Ziele sind nach wie vor seine Leitlinie: Couragiertes und menschenrechtlich erforderlichenfalls zivil ungehorsames Engagement für Menschenrechte

aller Menschen und überall.

Im Gründungsmanifest von 1980 heißt es: „Das Komitee begreift als seine Hauptaufgaben, einerseits aktuelle Verletzungen von Menschenrechten kundzutun und sich für diejenigen einzusetzen, deren Rechte verletzt worden sind (z.B. im Kontext so genannter Demonstrationsdelikte, Justizwillkür, Diskriminierung, Berufsverbote, Ausländerfeindlichkeit, Totalverweigerung, Asyl- und Flüchtlingspolitik), andererseits aber auch Verletzungen aufzuspüren, die nicht unmittelbar zutage treten und in den gesellschaftlichen Strukturen und Entwicklungen angelegt sind (struktureller Begriff der Menschenrechte).

Die Gefährdung der Grund- und Menschenrechte hat viele Dimensionen, vom Betrieb bis zur Polizei, vom „Atomstaat“ bis zur Friedensfrage, von der Umweltzerstörung bis zu den Neuen Technologien, von der Meinungsfreiheit bis zum Demonstrationsrecht, von der Arbeitslosigkeit bis zur sozialen Deklassierung, von den zahlreichen Minderheiten bis zur längst nicht verwirklichten Gleichberechtigung der Frau.

Das Komitee hat die Rechtsform eines eingetragenen, gemeinnützigen Vereins. Organisatorisch besteht das Komitee aus einem Mitglieder- und einem Förderkreis zur Unterstützung des Komitees. Vorstand und Arbeitsausschuss beraten regelmäßig über aktuelle Schwerpunktsetzungen. Interessierten senden wir gerne Informationen und die Liste unserer Veröffentlichungen zu.

Komitee für Grundrechte und Demokratie e.V.
 Aquinostr. 7 - 11, 50670 Köln
 Tel.: 0221/9 72 69-30, Fax: 0221/9 72 69-31
 E-Mail: info@grundrechtekomitee.de
 Internet: www.grundrechtekomitee.de
 Spendenkonto: Volksbank Odenwald,
 BLZ 508 635 13, Konto-Nr.: 8 024 618

RFID-Chips

Die so genannten „Schnüffelchips“ sind sehr billig und fast überall einzusetzen. Fast täglich werden neue Anwendungsmöglichkeiten von Wirtschaft und Politik entwickelt. Sie sind unter anderem eine Warenmarkierungstechnologie mit gravierenden gesellschaftlichen Folgen. Werden sie unkritisch genutzt, haben RFID-Chips ein großes Potential zur Gefährdung der Privatsphäre von Konsumenten, zur Verringerung oder bis hin zum Verlust der Käuferanonymität und zur Bedrohung bürgerlicher Freiheiten.

What is it?

RFID ist die Abkürzung für Radio Frequency Identification, also für eine Identifizierung per Funksignal. RFID-Chips bestehen aus einem winzigen Chip, dessen Drähte eine Antenne bilden (Vgl. Bild). Die Chips sind in Gegenstände, Etiketten oder Verpackungen eingebaut und benötigen keine eigene Energiequelle. Ein Lesegerät, auch „Antenne“ genannt, sendet einen Funk-Impuls und der „Schnüffelchip“ sendet eine auf ihm gespeicherte, nur einmal existierende Nummer zurück. Zusätzlich kann ein Chip aber auch

noch weiteren, beliebig beschreibbaren (und damit auch abrufbaren) Speicher enthalten.

Je nach Chip können die darauf gespeicherten Daten auf eine Entfernung von bis zu 10 Metern, und ohne dass die Person die den Chip bei sich hat davon etwas bemerkt, abgerufen werden. Zudem kann das Lesegerät auch mit Satelliten gekoppelt werden...

Where is it used?

Die potenziellen Anwendungsgebiete der „Schnüffelchips“ sind nahezu unbegrenzt. Die Stadion-Tickets bei der WM 2006 waren ebenso mit einem Chip ausgestattet (auf denen personenbezogene Daten der KäuferInnen gespeichert waren) wie auch die neuen Personalausweise (auf dem ein digitales Photo gespeichert ist; ein digitaler Fingerabdruck und weitere biometrische Daten werden folgen). Ebenso ist in der Bahncard100 schon ein RFID-Chip integriert.

Besonders häufig werden die Chips dazu benutzt, Waren eindeutig zu kennzeichnen und damit auch die Möglichkeit zu haben, sie zu verfolgen. Die Metro AG hat Pläne bis 2007 alle ihre 800 Warenhäuser und Vertriebscenter mit RFID auszustatten, womit sich problemlos Bewegungsprofile von Kunden u.ä. erstellen lassen. 2003 führte der Konzern schon RFID-Chips in Kundenkarten ein, was aber nach den Protesten durch die STOPRFID-Kampagne wieder zurückgenommen werden musste.

Auch bei Schließsystemen und Alarmanlagen für Gebäude werden die „Schnüffelchips“ schon lange verwendet. Es wurde sogar schon an der Ausstattung von Euro-Geldscheinen mit den RFID-Chips geforscht. Zwar ist dies noch nicht geschehen, wäre aber wohl technisch kein Problem mehr. Damit würde auch die Anonymität von Bargeld nicht mehr existieren... Natürlich lassen sich auch Uni-Karten und Bibliotheksausweise sowie einzelne Bücher mit RFID ausrüsten oder mensch kann sich den Chip gleich implantieren lassen (ist leider kein schlechter Witz, das gibt es schon!).

Egal ob mensch Auto fährt (Funkschlüssel, Wegfahrsperre), als Waldarbeiter Bäume im Wald einsammelt, einen Skilift benutzt, als EinzelhändlerIn seine Joghurt-Becher drahtlos erfassen will - fast überall werden inzwischen Lösungen mit RFID angeboten. Je billiger die Chips werden, desto mehr werden sie auch benutzt werden und desto mehr Daten werden permanent produziert werden.

What is new?

RFID-Chips stellen eine vollkommen neue Qualität der Überwachungsmöglichkeiten dar. Mit ihnen (vor allem in Verbindung mit der Bezahlung mittels Bank- oder Kundenkarte) wird die Dystopie des „Gläsernen Kunden“ wohl bald keine Zukunftsmusik mehr sein.

Im Unterschied zum klassischen Barcode ist mit den RFID-Chips jeder Gegenstand über seine weltweit einzigartige Seriennummer eindeutig identifizierbar. Somit wäre der Weg jedes Joghurtbechers

bzw. Schuhs einzeln, auch nach dem Kauf, verfolgbar. Wird das Produkt mit einer Kunden- oder Bankkarte bezahlt, kann es auch den jeweiligen KonsumentInnen zugeordnet werden.

RFID-Chips sind per Funk und damit berührungslos, ohne dass die betroffene Person es merken kann, lesbar. Somit kann jeder der über eine entsprechende „Antenne“ verfügt die auf RFID-Chips gespeicherten Daten über eine Person ablesen. Wer was über eine Person weiß, ist damit überhaupt nicht mehr zu kontrollieren.

Die Chips sind so klein und so billig, dass sie nahezu in jedes Produkt eingepflanzt werden können. Dort lassen sie sich nicht mehr entfernen, ohne das Produkt (z.B. den Schuh) zu zerstören. Das bedeutet: Jede Lese-Antenne, an der mensch vorbei kommt, erfasst den Chip aufs Neue (vielleicht im Bus, an der Tankstelle, im nächsten Supermarkt...).

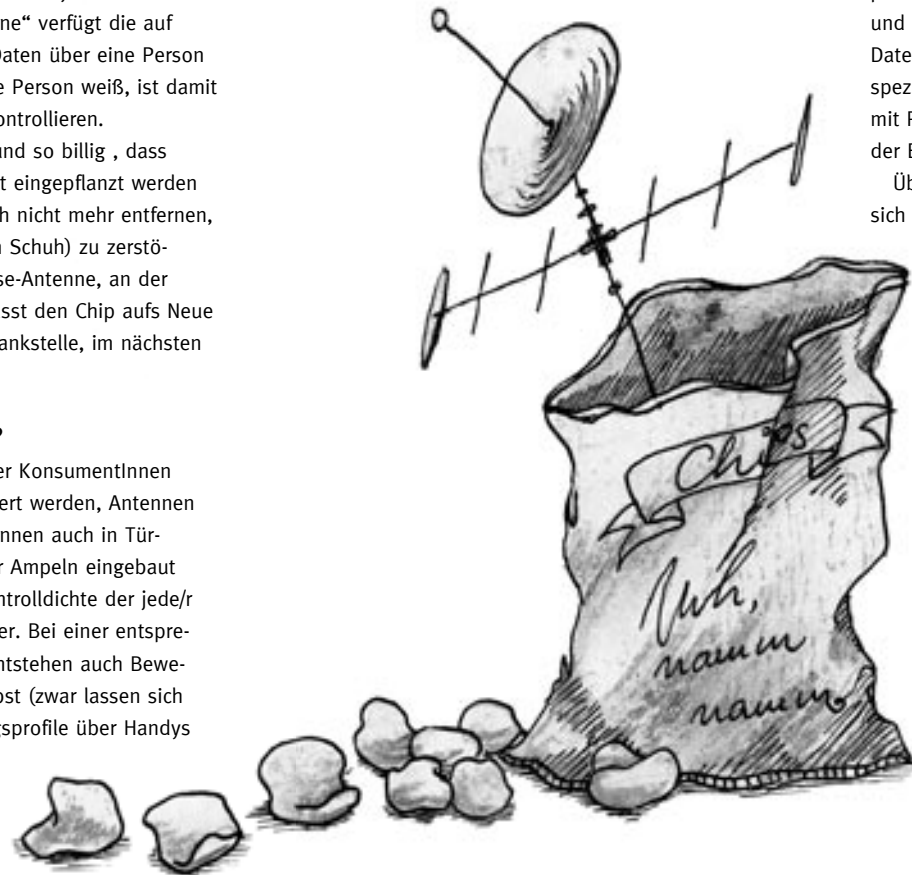
What is the problem?

Das Einkaufsverhalten der KonsumentInnen kann problemlos ausspioniert werden, Antennen zum Auslesen der Chips können auch in Türschwellen, Tanksäulen oder Ampeln eingebaut werden. Somit wird die Kontrolldichte der jede/r ausgesetzt ist deutlich höher. Bei einer entsprechenden Antennendichte entstehen auch Bewegungsprofile quasi von selbst (zwar lassen sich auch jetzt schon Bewegungsprofile über Handys

erstellen, ein Handy kann mensch jedoch zu Hause lassen oder Ausschalten bzw. den Akku raus nehmen). Der einzelne wird sich den „Schnüffelchips“ auch nicht entziehen können, da es Produkte ohne RFID irgendwann einfach nicht mehr geben wird.

Die Nutzung der RFID-Technologie erfordert die Einrichtung riesiger Datenbanken. Im Zuge der permanenten Ausweitung der Speicherkapazitäten und Prozessorleistungen lassen sich massenhafte Datenzusammenführungen vornehmen und damit spezifische Profile erstellen. Werden diese Daten mit Personenidentifikationsdaten verbunden, wird der Einzelne immer „Gläserner“.

Über Personalausweise mit RFID-Chips ließen sich mittels einer neben eine Demonstration



gestellten Antenne innerhalb von Sekunden erfassen, wer an ihr teilnimmt. Sehr praktisch für Polizei und Verfassungsschutz, eine ganz neue Herausforderung für die Wahrnehmung demokratischer Freiheitsrechte (zumindest ohne Repression befürchten zu müssen).

What to do?

Es kann nicht darum gehen eine Technologie komplett verbieten bzw. verhindern zu wollen. Zum einen wäre dies doch sehr unrealistisch, zum anderen gibt es ja durchaus Anwendungsmöglichkeiten, die die informationelle Selbstbestimmung der Einzelnen nicht einschränkt. So mag die Verfolgbarkeit von Waren vom Ort der Produktion bis zum Ort des Verkaufs für den Produzenten durchaus von Vorteil sein und muss, vorausgesetzt die Chips werden vor dem Verkauf wieder entfernt, für die KonsumentInnen keinen Nachteil darstellen. Nur da, wo das Grundrecht auf informationelle Selbstbestimmung beschnitten wird gilt es zu intervenieren.

Die Möglichkeiten individuell gegen die Chips vorzugehen sind leider beschränkt. Sie lassen sich weder immer erkennen noch wirklich zerstören. Es bleibt wohl erstmal nur der Versuch herauszufinden wo denn überall RFID-Chips enthalten sind, wo denn überall Lesegeräte sind und die Beschwerde darüber bei denen die sie verwenden bzw. der Boykott derselben. Im Endeffekt könnte wohl höchstens eine massenhafte Verweigerung der KonsumentInnen die umfassende Verwendung der Chips verhindern.

Für Personalausweis, BahnCard100 u.ä. Gibt es Schutzhüllen, die das Auslesen der Chips verhindern. Diese sind im FoeBuD-Shop erhältlich (Alle Gewinne aus dem Shop fließen wieder in die Arbeit des Vereins). Auch die Entwicklung einer wirksamen Methode oder Technik zur Zerstörung der Chips wäre bei allen Mängeln dieses Weges (z.B. der Schaffung von zwei weiteren KonsumentInnenklassen) ein Fortschritt.

Da diese Möglichkeiten doch sehr beschränkt sind, wären gesetzliche Regelungen wie z.B. eine Kennzeichnungspflicht, umfassende Datenschutzregelungen die die informationelle Selbstbestimmung garantieren u.ä. dringend nötig!

Tim Ackermann
 AStA Uni Münster
 Referat für politische Bildung/demokratische Rechte

Alle Informationen stammen von den StopRFID Seiten des FoeBuD e.V.: www.foebud.org. Dort sind auch umfassende und weiterführende Informationen zu finden.

Persönlichkeitsrechte und die „Aufenthaltskarte für Ausländer“

Unter dem Deckmantel der allseits drohenden Terrorgefahr und spätestens nach den Anschlägen vom 11. September 2001, setzen die Innenminister der Bundesländer nach und nach die langersehnten Sicherheits- und Überwachungsverstärkungen ungeachtet bürgerlicher Freiheitsrechte, rigoros durch. Und selbst nach „Anti-Terrordatei“, „biometrischen Ausweisdaten“ und „Videoüberwachung“, wird weiterhin eine „grundsätzliche sicherheits- und gesellschaftspolitische Neuausrichtung“ (12) gefordert, um weitere Einschränkungen bürgerlicher Freiheiten zu beschliessen.

Mit der „zunehmenden Terrorgefahr“ in Deutschland geraten insbesondere Menschen ins Fahndungsvisier bundesdeutscher „Sicherheits“-fanatikerInnen, die als potentiell terrorverdächtig gelten. So wurden bei der Erfassung von mehr als 5,2 Millionen personenbezogenen Datensätzen im Rahmen der verfassungswidrigen Rasterfahndung nach dem „9/11“ (15), aus allen Daten der Universitäten, Einwohnermeldeämter und Ausländerzentralregister (AZR) rund 32.000

Datensätze in die „BKA-Verbunddatei ‘Schläfer‘“ aufgenommen. Darunter fielen beispielsweise auch alle männliche, ausländische Studierende, die somit als ‘terrorverdächtig’ abgespeichert wurden (16,17).

Vor einigen Wochen stellte Wolfgang Bosbach (CDU) die Forderung nach „strengeren Kontrollen von einreisenden Ausländern“ und warnte vor einer „falschen Toleranz“ (13). BKA-Präsident Jörg Ziercke machte in einem Interview deutlich, dass „in der Vergangenheit nahezu alle Terroranschläge in der westlichen Welt von legal eingewanderten Menschen verübt worden seien“. Schliesslich seien „nur sechs Prozent der untersuchten Terroristen als illegale Einwanderer in das Zielland gekommen“. Ausserdem bestehe „derzeit eine erhöhte Gefahr, dass aus dem Irak Terroristen auch nach Deutschland geschleust werden“, so Ernst Uhrlau vom BND (14).

Im Kontext dieser Aussagen wird schnell deutlich, wer als potentiell terrorverdächtig gilt. Und das nicht nur in Deutschland, denn eine weitgehende, sogenannte „Harmonisierung der europäischen Einwanderungspolitik“ ist das Ziel aller EU-Staaten. Hierbei geht es darum, im Kampf gegen die illegale Einwanderung in die EU, sowie gegen den „internationalen Terrorismus“, alle Kräfte zu vereinen. Dafür hat der Europäische Rat eigens einen EU-Koordinator für Terrorismusbekämpfung geschaffen. Dieser begleitet aktiv u.a. die Zusammenarbeit in Europol und Eurojust und forciert die Umsetzung des „Europäischen Haftbefehls“

(5,6). In dem im November 2004 verabschiedeten sogenannten Haager Programm wurde besonders die praktische Zusammenarbeit im „Rahmen des Gemeinsamen Europäischen Asylsystems“ (7) zur „Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union“ (18) hervorgehoben. Es zielt darauf ab, die Abschottungspolitik der EU mit einer noch restriktiveren Migrations- und Asylpolitik zu kombinieren (18), um eine „konsequente Verhinderung der Einreise und der Zuwanderung von Extremisten“ zu garantieren (25).

Bei dem sogenannten EURODAC-System handelt es sich um eine riesige Datenbank für „den Abgleich von Fingerabdrücken“ (9) von Asylsuchenden in der EU, Finnland und Island, durch die sich zumindest die deutsche Bundesregierung eine „verbesserte Identifizierung“ von Asylsuchenden verspricht (5,8). Doch geht es vielmehr darum, hier lebende Asylsuchende zu überwachen und zu kontrollieren, ihre Mobilität zu beschränken, und ihnen dadurch die Rückreise in ihre Herkunftsländer zu „erleichtern“.

In der EURODAC-Datenbank werden neben den Fingerabdrücken aller betroffener Asylsuchenden in der EU, die älter als 14 Jahre sind eine Vielzahl von persönlichen Daten, wie Herkunft, Alter, Geschlecht, Ort und Zeit der Antragstellung, zentral mit einem Personenkennzeichen versehen und gespeichert (10,11).

Parallel dazu wird u.a. das seit 1990 verwendete Schengener Informationssystem (SIS) als „Sach- und Personenfahndungssystem“ auf das

modernisierte SIS II umgerüstet. Weiterhin nahm die sogenannte „Europäische Grenzschutzagentur (FRONTEX)“ zum Schutz der EU-Aussengrenzen ihre Arbeit auf, und mit Hilfe des „Visa-Informationssystems (VIS)“ sollen ab 2007 „biometrische Daten der Visumantragsteller erfasst (...) und allen Schengen-Partnern zur Verfügung gestellt“ werden (19).

In diesem Zusammenhang plant die deutsche Bundesregierung, derzeit namentlich Wolfgang Schäuble, bereits seit Jahren die Einführung einer sogenannten „Aufenthaltskarte für Ausländer“, „Ausländerkarte“ oder früher „Asylcard“ zeitgleich zu der Einführung des elektronischen Personalausweises im Jahre 2008. Voraussetzung hierfür ist eine „EU-Verordnung zur Einführung von elektronischen Identitätskarten“, die spätestens 2007 verabschiedet werden soll (4,2). Diese „Aufenthaltskarte für Ausländer“ soll nach Vorstellung des Staatssekretärs im Bundesinnenministerium August Hanning, die „üblichen“ biometrischen Feinheiten, wie digitalisierte Fingerabdrücke und ein digitalisiertes Foto, mit einem RFID-Chip kombiniert werden (1,2). Ganz nach niederländischem Vorbild sollen dadurch insbesondere Asylsuchende in Deutschland noch besser überprüf- und kontrollierbarer und vor allem „identifizierbar“ (21) sein. Nach Angaben des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. an der Uni Bremen, sollen u.a. neben den persönlichen Daten, die Religionszugehörigkeit, der Aufenthaltstitel, Angaben zu Sozialleistungen,

Krankheiten, Abschiebehindernisse, Angaben über „Beschränkungen der räumlichen Aufenthaltserlaubnis“ und deren Einhaltung, sowie sämtliche Daten im Zusammenhang zu dem Stand des Asylverfahrens, auf der Chipkarte gespeichert werden (3,20).

Das unabhängige Landezentrum für Datenschutz Schleswig-Holstein rät in einer Stellungnahme zu der Machbarkeitsstudie des Bundesinnenministeriums (BMI) aus „datenschutzrechtlicher Sicht (...) dringend“ von der geplanten Einführung der „Ausländercard“ ab. Kritisiert werden u.a. eine „Entpersönlichung“ und ein „Würdeverstoß“ durch die „umfassende Katalogisierung der Persönlichkeit“ und deren fehlende Transparenz, fehlende Sicherheitssysteme, eine „Erhöhung der Kontrolldichte in allen Lebensbereichen“ sowie die Einführung von Personenkennzeichen und die Nichtvereinbarkeit mit dem Grundgesetz (siehe auch Bundesverfassungsurteil zur Volkszählung von 1983) (22,23).

Die „Ausländercard (...) ermöglicht es, Asylsuchende zu zwingen sich mehrfach am Tag zum Aufenthaltsnachweis an Meldesäulen einzufinden“, so wie es in den Niederlanden bereits „zur Kontrolle einer bis zu vier Mal täglich bestehenden Meldepflicht“ angewandt wird. Bei fehlender Mitwirkungspflicht drohen dann Leistungseinschränkungen und asylverfahrensrelevante Restriktionen (22).

Auch wenn die bundesweite Einführung von Chipkartensystemen mit biometrischen Daten noch Monate dauern wird, haben einige Städte und

Gemeinden bereits ein eigenes System eingeführt. So engagiert sich z.B. die „Friedens“-Stadt Osnabrück seit 1999 für die rigorose Beibehaltung eines Chipkartensystems für Asylsuchende. Die Stadt Ulm hat sich dagegen 2005 für die Einrichtung eines solchen Systems entschieden, während z.B. Berlin-Reinickendorf nach vielen Jahren zum Bargeldsystem zurückgekehrt ist.

Wo die weit unter dem Sozialhilfesatz liegenden Leistungen nach dem Asylbewerberleistungsgesetz bar ausgezahlt wenigstens ein wenig Selbstbestimmung wahren, können die Betroffenen mit den Chipkarten (oder Gutscheinen) nur in ausgewählten Läden (Marktkauf, e-Center, aber nicht etwa ALDI oder LIDL) nur bestimmte Waren, nämlich „Nahrungsmittel, Körperpflegeartikel und Haushaltsgegenstände“ kaufen. Der Kauf traditioneller und günstiger Lebensmittel z.B. vom Wochenmarkt oder dem „kleinen Lebensmittelladen auf der Ecke“ ist nicht möglich. Alkohol und Zigaretten sind nicht erlaubt. Ebenso keine Druckerzeugnisse; vor allem aber können sämtliche Dienstleistungen, angefangen von Bus-Fahrscheinen über Briefmarken, Telefonkosten bis hin zu Kosten für die notwendigen Anwältinnen oder Anwälte nicht bezahlt werden. Ausserdem werden diese Chipkarten einmal im Monat im zuständigen Sozialamt aufgeladen und netterweise mit dem möglicherweise auf der Karte noch befindlichen Guthaben verrechnet.

Eine der derzeit relevanten Vertragspartnerinnen für die Einrichtung, Instandhaltung und Wartung dieser Chipkartensysteme ist die Firma SODEXHO Pass Austria; einem Tochterunternehmen des französischen Cateringgiganten SODEXHO Catering & Services GmbH. Aber auch ACCOR, Infineon, Phillips und Microsoft reiben sich schon die Hände.

Denn schliesslich werden bei einer bundesweiten Einführung einer „Ausländerkarte“ allein (Anm. ungeachtet der Einführung des Personalausweises) einige Millionen Euro Steuergelder fließen. Hinzu kommen noch die Kosten für die Umrüstung und Einrichtung von Lesegeräten etc. in den zuständigen Behörden und Dienststellen sowie hohe Wartungs- und Instandhaltungskosten (26). Somit setze nach Ansicht Hannings, „Deutschland damit industriepolitisch deutliche Zeichen“ (2).

Angesichts der rigorosen Asyl- und Abschtotungspolitik, ist es für Asylsuchende faktisch unmöglich, „legal“ nach Deutschland einzureisen. Daher bedeutet die Einführung dieser Chipkartensysteme insbesondere für die derzeit hier lebenden Menschen ohne deutschen Pass eine radikale Beschneidung ihrer bereits eingeschränkten Persönlichkeits- und Freiheitsrechte.

Abschliessend gilt daher die Forderung eines weitreichenden Verbotes elektronischer Identitätskarten jedweder Art, und die sofortige Abschaffung bestehender Systeme.

Anm.: Passenderweise ist SODEXHO auch aktiv an der Privatisierung von Knästen beteiligt und „versorgt weltweit

Strafvollzugsanstalten mit Dienstleistungen von der Wäscherei bis zur Verwaltung“ (24). Ausserdem versorgt SODEXHO die britischen und US-Kampfverbände in ihren „out-of-area“-Kriegseinsätzen mit der nötigen Feinkost.

Quellen:

(1) Pro Asyl (2006). Die Bundesregierung will eine elektronische Ausländerkarte einführen. Newsletter Nr. 117, Oktober 2006. URL: <http://www.proasyl.de/de/archiv/newsletter-ausgaben/nl-2006/newsletter-nr-117/index.html#c3393>

(2) Spiegel (2006). Innenministerium plant elektronische „Ausländerkarte“. Spiegel online Artikel vom 29. September 2006. URL: <http://www.spiegel.de/politik/deutschland/0,1518,439937,00.html>

(3) TAZ (2006). Aufenthaltkarte für Ausländer. Die tageszeitung, Nr. 8088 vom 30.09./01.10.2006. URL: <http://www.taz.de/pt/2006/09/30/ao137.1/text>

(4) Bundesministerium des Innern (BMI) (2006). Informationstechnik und Innere Sicherheit. Namensbeitrag des Bundesinnenministers Dr. Wolfgang Schäuble in der Fachzeitschrift „Die neue Polizei“, 56. Jahrgang, Heft 2/2006. URL: http://www.bmi.bund.de/cln_012/nn_662984/Internet/Content/Nachrichten/Medienspiegel/2006/10/BM_Schaeuble_Informationstechnik_innere_Sicherheit.html

(5) Auswärtiges Amt (2006). Bekämpfung des Terrorismus und der schweren grenzüberschreitenden Kriminalität. URL: http://www.auswaertiges-amt.de/diplo/de/Europa/Aufgaben/JustizInneres/Kriminalit_C3_A4t.html

(6) Auswärtiges Amt (2006). Asyl und Migration in der EU. URL: <http://www.auswaertiges-amt.de/diplo/de/Europa/Aufgaben/JustizInneres/Asyl.html>

(7) Europäische Kommission – Justiz und Inneres (2006). Europäisches Asylsystem. URL: http://ec.europa.eu/justice_home/fsj/asylum/fsj_asylum_intro_de.htm

(8) European Commission - Justice and Home affairs (2006). EUODAC - a tool for a common EU asylum policy URL: http://ec.europa.eu/justice_home/news/information_dossiers/news_eurodac_index_en.htm

(9) Europäische Kommission – Justiz und Inneres (2006). Glossar. URL: http://ec.europa.eu/justice_home/glossary/glossary_e_de.htm

(10) Europäische Union (2006). „Eurodac“-System. URL: <http://europa.eu/scadplus/leg/de/lvb/l33081.htm>

(11) Der Landesbeauftragte für den Datenschutz in Rheinland-Pfalz (2006). BVerfGE 65, 1 – Volkszählung. URL: http://www.datenschutz.rlp.de/entwicklung/ds_rueckblick/volkszaehlunsurteil.html

(12) Telepolis News(2006). Schäuble: Wir müssen gegen den Terror noch wachsam sein. Artikel vom 26.08.2006. URL: <http://www.heise.de/newsticker/meldung/77304>

(13) Spiegel online (2006). Angst vor Terror : Bosbach will Einreisende stärker kontrollieren lassen. Artikel vom 23.08.2006. URL: <http://service.spiegel.de/digas/servlet/find/ON=spiegel-433141>

(14) Focus (2006). Deutschland rückt nach Ansicht von Sicherheitsexperten immer stärker ins Zielspektrum terroristischer Anschläge. Artikel vom 16.11.2006. URL: http://www.focus.de/politik/deutschland/sicherheit_nid_39424.html

Alltag Überwachung

(15) Wikipedia (2006) Terroranschläge am 11. September 2001 in den USA. URL: http://de.wikipedia.org/wiki/Terroranschlag%3%A4ge_am_11._September_2001_in_den_USA

(16) Heise (2006). Rasterfahndung nach 11. September 2001 verfassungswidrig. Heise online News vom 23.05.2006. URL: <http://www.heise.de/newsticker/meldung/73430>

(17) Breitner, Michael H. (2005). Biometrie in Reisedokumenten – ein Allheilmittel gegen Kriminalität und Terrorismus?! Institut für Wirtschaftsinformatik an der Uni Hannover.

(18) Prinz, Vanessa (2005). Unter österreichischer Präsidentschaft: Tanzania als Vorhof europäischer Asylpolitik? URL: <http://no-racism.net/article/1518>

(19) Auswärtiges Amt (2006). Schutz der EU-Aussengrenzen. URL: <http://www.auswaertigesamt.de/diplo/de/Europa/Aufgaben/JustizInneres/Aussengrenzen.html>

(20) Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. Regionalgruppe Bremen (2000). Asyl-Card. URL: <http://fiff.informatik.uni-bremen.de/asylcard2000.pdf>

(21) Hanning, August (2006). Bundesregierung will elektronische Ausländerkarte einführen. In Heise online News vom 29.09.2006. URL: <http://www.heise.de/newsticker/meldung/78841>

(22) unabhängige Landezentrum für Datenschutz Schleswig-Holstein (1998). Stellungnahme zur Machbarkeitsstudie zur geplanten Einführung einer AsylCard. URL: <http://www.datenschutzzentrum.de/material/themen/divers/asylcard.htm>

(23) Bäuml, H., Gundemann, L., Probst, T. (2001). Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen. URL: <http://www.datenschutzzentrum.de/download/tabga.pdf>

(24) Unternehmensinstitut e.V. (2003). Der Weg aus der staatlichen Schuldenfalle - Konzepte und Beispiele für eine umfassende Privatisierung. Schriftenreihe des UNI Unternehmerinstituts der ASU e.V. □ Band 10. URL: <http://www.asu.de/www/doc/6c23fdb32b57c00398f53e90a3714bd3.pdf>

(25) Bayerische Staatskanzlei (2001). Forde- rungskatalog der Bayerischen Staatsregierung zur Erhöhung der Inneren Sicherheit. Anlage 2 zur Regierungserklärung vom 9. Oktober 2001. URL: http://www.bayern.de/Presse-Info/Regie- rungserklaerungen/RegErklaerung_010910_anl2.html?PHPSESSID=

(26) Bundeszentrale für politische Bildung (BPB) (1998). Deutschland: Einführung der Asylcard wird diskutiert. Migration und Bevölkerung, Ausgabe 07/98. URL: www.migration-info.de

Recherche für einen Dokumentar- film von Roman Mischel und Fiete Stegers

Spätestens als wir die Interview- Passage im Auto auf der nächst- lichen Rückfahrt aus Brüssel noch einmal auf dem Display ablaufen lassen, gratulieren wir uns im Geiste zu dem gelungenen O-Ton. Weil er zeigt, welches Ausmaß das Thema unseres Films hat. Da ist es auch egal, dass wir deswegen eine Abzweigung verpassen.

„Wir haben jetzt die Vorratsda- tenspeicherung, sprich: Ihr Kom- munikationsverhalten wird erfasst“, holt der EU-Parlamentarier Alexan- der Alvaro am Ende bei seiner Ant- wort aus, teilt mit der Handkante energisch eine imaginäre Salami auf seinem Schreibtisch in immer mehr Scheiben: „Wir haben auf nationaler Ebene den großen Lauschangriff. Wir haben die DNA-Analyse und die Rasterfahndung auf Länderebene. Wir haben auf Bundesebene die Maut, die Kontodatenabfrage, wir haben auf kommunaler Ebene die Videoüberwachung von öffentlichen Plätzen, und so fort. Und wenn wir das alles einmal zusammen

nehmen, was theoretisch bereits überwacht sein könnte: Was bleibt da von der Salami eigentlich noch übrig?“ Die Salami, das sind Bürgerrechte und Privatsphäre.

Alvaros Frage trifft genau auf den Ausgangs- punkt unserer Recherche. Welches Gesamtbild setzt sich aus den einzelnen Puzzlestücken zusammen, wie wir sie mal als kleine, mal etwas größere Schnipsel in der Zeitung lesen - von der Verabschiedung der EU-Richtlinie zur Vorratsdaten- speicherung von Telefon- und Internetdaten, dem Vorstoß des Bundesinnenministers zur Auswertung der Lkw-Mautdaten für die Fahndung, bis zur Datensammlung von WM-Beschäftigten und -Besu- chern und Funkchips in Alltagsgegenständen?

„Weil wir uns mit Technologie gut auskennen, kennen wir auch die Gefahren, können sie uns besser vorstellen. Und die Szenarien von Überwa- chung, Kontrolle und Manipulation sind äußerst erschreckend“, sagt Rena Tangens. Die Medienkünst- lerin und ihr Kompagnon Padeluun vom Bielefelder FoeBuD e. V. beschäftigten sich seit Jahren mit Überwachungstechnologien und Bürgerrechten und prangern die Datensammelwut von Staat und Wirt- schaft an. Wer als Journalist in diesem Themenfeld recherchiert, kommt am FoeBuD e. V. nicht vorbei. Von Anfang an ist daher klar, dass Tangens eine wichtige Rolle in unserem Film spielen wird.

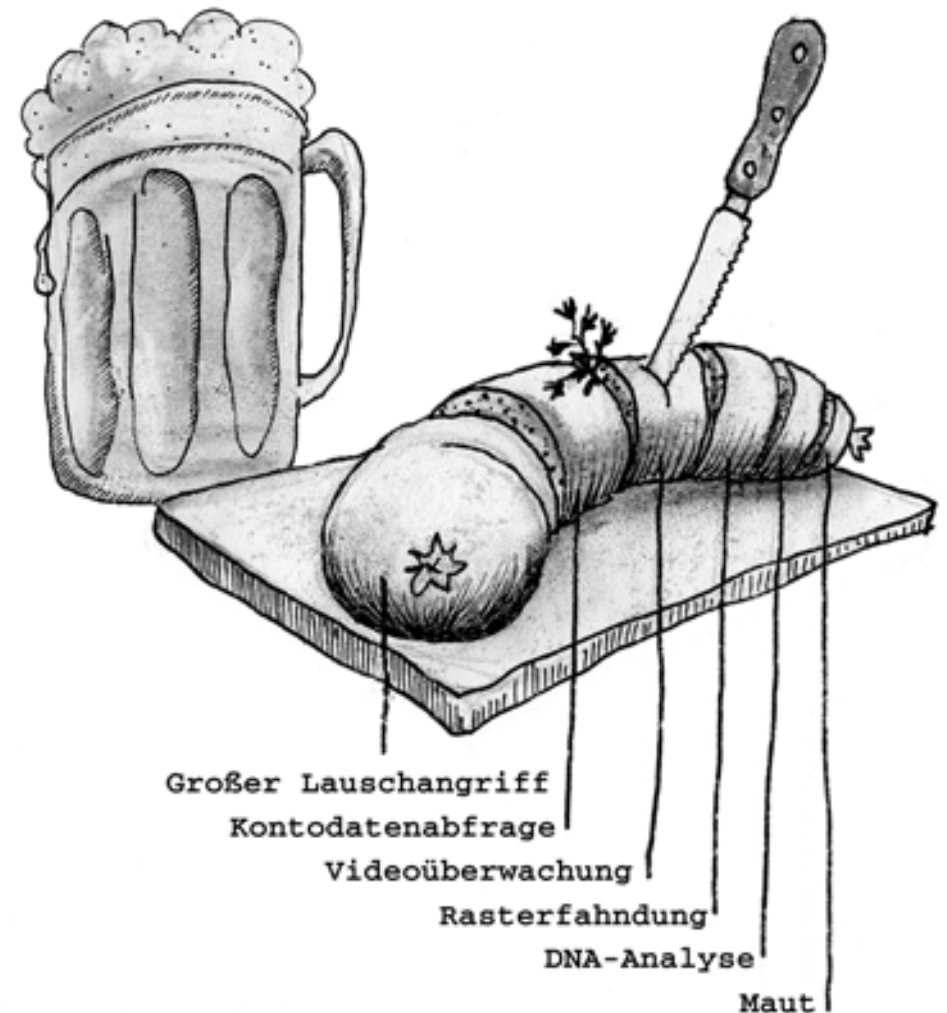
Aber wie lässt sich das schwierige Thema sonst filmisch aufbereiten? Während der Vorrecherchen und der gesamten Produktionsdauer werden wir laufend mit neuen Vorstößen, Entwicklungen und

Aufdeckungen konfrontiert - von der Fahndung mittels Mautdaten bis zur Kontenüberwachung durch die US-Geheimdienste. Reduktion von Komplexität ist gefragt. Wir konzentrieren uns auf drei Aspekte und drei Protagonisten: Alvaro, der im Europaparlament verzweifelt versuchte, die Speicherrichtlinie für Kommunikationsdaten zu entschärfen. Rena Tangens, die die Einführung von RFID-Funkchips seit Jahren kritisch begleitet. Und schließlich Michael Arzt, dessen Initiative in Leipzig ihre Mitbürger über die Folgen von Videoüberwachung aufklären will. „Wir glauben nicht, dass Videoüberwachung das Leben sicherer macht. Ich denke, dass man prinzipiell in dieser Gesellschaft dafür einstehen kann, nicht die ganze Zeit beobachtet zu werden, ohne dass es Verdachtsmomente gegen einen gibt“, erläutert Arzt die Motivation der Gruppe. Arzt, Tangens und Alvaro sind klare Gegner der „Datensammelwut“, wie es Tangens nennt. Dass der Film sich auf sie konzentriert, hat nicht allein dramaturgische Gründe: Wir wollen nicht nur wissen, wo und wie Staat und Wirtschaft immer mehr Informationen über den Einzelnen sammeln, sondern auch, warum dieser schleichende, aber unübersehbare Prozess in der Bevölkerung so wenig Widerspruch auslöst. Sehen die Kritiker nicht, dass den Normalbürgern der versprochene Gewinn an Sicherheit und Bequemlichkeit wichtiger ist als die Befürchtung, ein Stück gläserner zu werden? Und was treibt Arzt, Alvaro und Tangens dann, ihren Kampf weiter zu kämpfen?

Michael Arzt und seine „Leipziger Kamera“ - man könnte meinen, sie hätten schon verloren, bevor sich ihre Gruppe überhaupt 2003 gründete. Ausgerechnet die Stadt der Montagsdemonstrationen und der Stasi-Überwachung ist in Deutschland Vorreiter bei Videoüberwachung im öffentlichen Raum.

„Eine unsere erste Aktionen war ein Kamerastadtplan, der auch im Internet zu sehen ist“, erläutert Michael Arzt. Darauf zu verzeichnet sind alle Kameras in der Leipziger Innenstadt - ein dichtes Netz von den ausgiebig überwachten Einkaufspromenaden im renovierten Hauptbahnhof über Kameras in Geschäften bis zu kaum sichtbaren Klingelkameras, deren Besitzer aber auch einen Teil der Straße im Blick haben. Vor allem aber sind Kameras in Leipzig bereits seit zehn Jahren fester Teil der Polizeistrategie. Die vier Polizeikameras erfassen den Bahnhofsvorplatz, zwei weitere Plätze am Innenstadtring und einen im Szene-Viertel Connewitz, nur ein paar Schritte von einem linken Info-Laden, in dem sich die Kamera-Kritiker treffen. „Kriminalitätsschwerpunkte“, heißt es bei der Polizei. Die Beamten am Monitor haben mehrere hundert Meter Umkreis im Blick. Was sie sehen, wird digital mitgeschnitten, jedoch nach 24 Stunden automatisch gelöscht, wenn sich nichts Verdächtiges ereignet hat.

Für Arzt und seine Mitstreiter ist die staatliche Überwachung jedoch ein grundsätzliches Übel:



Jeder Bürger werde unter einen ständigen Verdacht gestellt. Die Argumente, dass die Kameras Kriminalität verhinderten und zur Aufklärung von Straftaten betrügen, hält Arzt für „Mythen“: „Man glaubt, dass sich jedes Problem durch Videoüberwachung lösen lässt.“

Polizeichef Rolf Müller ist dagegen nach wie vor von der Technik überzeugt. 1996 ließ Müller die erste Kamera aufstellen - vor allem um Autoaufbrüche zu verhindern. „Die Gefahr, dass potenzielle Täter geschnappt werden, hat dazu geführt, dass Delikte an den Kriminalitätsschwerpunkten erheblich zurückgegangen sind. Im letzten Jahr waren es konkret 31 gegenüber über 800 im Jahr 96.“

„Herr Müller sagt, die Kriminalität geht zurück. Dabei wird sie nur verdrängt - an andere Orte und andere Kriminalitätsarten,“ hält Arzt dagegen. Aber die Schattenseiten, vor denen die „Leipziger Kamera“ warnt - sie scheinen kaum jemanden zu interessieren. Vor der Gruppe hatten schon in Leipzig schon andere gegen Müllers Pläne engagiert. Doch die heftigen Proteste der linken Szene hatten nicht lange angehalten, nachdem die Kamera in Connewitz ihren Betrieb aufgenommen hat.

„Ich meine, die Stimmen, die für die Videoüberwachung sprechen, sind in der Mehrzahl“, sagt Polizeichef Müller. „Es gab immer wieder Bitten an uns, sie doch erheblich auszudehnen.“ Das werde

aber auch nicht gemacht, solange kein „Kriminalitätsschwerpunkt“ gegeben sei.

„Ich glaube, es bleibt uns gar keine andere Wahl, als verstärkt zum Mittel der Videoüberwachung zu greifen, denn wir müssen dem Bürger Sicherheit gewährleisten.“ Sagt August Hanning, früher Chef des Bundesnachrichtendienstes und heute Staatssekretär bei Minister Wolfgang Schäuble. Wie für viele ist für ihn die Abwehr und Aufklärung von Terroranschlägen ein Hauptargument für vermehrte Überwachung.

Auch in Deutschland wurde nach dem Schock des 11. Septembers der Ruf nach mehr Sicherheit und mehr Befugnissen für die Polizei laut. Im Eilverfahren peitschte der damalige Innenminister Otto Schily seine Sicherheitspakete durch: Mehr Kompetenzen für das BKA, Einführung biometrischer Pässe, Abschwächung des Bankgeheimnisses um Terrornetzwerken den Geldhahn zuzudrehen, erleichterte Abschiebung verdächtiger Ausländer. Auch andere westliche Staaten reagierten ähnlich. Trotzdem schlagen wieder Terroristen zu - in London, einer der am stärksten videoüberwachten Städte der Welt. „Die Anschläge von London haben noch einmal gezeigt, wie wertvoll Videoüberwachung bei der Aufklärung sein kann“, sagt Hanning. Der Haken an der Sache: Die Bilder helfen den Fahndern erst, nachdem die Bomben explodiert sind.

„Je mehr Bürgerinnen und Bürger mit Zivilcourage ein Land hat, desto weniger Helden wird es einmal brauchen.“
Franca Magnani

des 11. Septembers der Ruf nach mehr Sicherheit und mehr Befugnissen für die Polizei laut. Im Eilverfahren peitschte der damalige Innenmi-

„Man muss mir erst mal zeigen, wann eine Explosion in der U-Bahn durch Videoüberwachung verhindert wurde. Ausnahmeszenarien werden hochstilisiert, um Videoüberwachung durchzusetzen“, kritisiert Arzt. „Den Menschen wird eine Bedrohung suggeriert, und das bringt sie dazu, auch Maßnahmen, die sie selbst betreffen, zu akzeptieren“, meint auch Thilo Weichert, Datenschutzbeauftragter von Schleswig-Holstein.

Dies fällt nicht nur vehementen Kameragegnern auf. Der Sozialwissenschaftler Leon Hempel von der TU Berlin hat die Praxis in London ausführlich untersucht, sich mit Effizienz und sozialen Folgen auseinandergesetzt. Kameras als Schutz vor Terror, Mord und Überfällen - Hempel kennt die Argumentationskette: „Das liegt schlicht und einfach daran, weil Kriminalität ein öffentlichkeitswirksames Thema ist. Und die Spitze des Eisberges ist dann natürlich das Argument der Terrorismusbekämpfung.“

Hempel kennt die Umfragen, nach denen sich Bürger von Videoüberwachung mehr Sicherheit versprechen, hat aber erhebliche methodische Zweifel. Die Fragen seien häufig suggestiv gestellt. Und der Bundesbeauftragte für Datenschutz, Peter Schaar, gibt zu bedenken: „Entscheidend ist nicht das Sicherheitsgefühl, sondern die tatsächliche Sicherheit.“

Von „einer unmittelbaren Bedürfnisbefriedigung der Bevölkerung, ohne tatsächlich wirksam zu sein“, spricht der deutsche EU-Abgeordnete Alvaro in Hinblick auf die so genannte Vorratsdatenspei-

cherung. Weil Telefon-, Handy- und Internetdaten, kann viel über Verdächtige verraten können, vereinbarten die EU-Innenminister schon kurz nach dem 11. September weitreichende Maßnahmen: Nicht die Inhalte, aber die Verbindungsdaten sämtlicher Telefon und Internetverbindungen sollten dauerhaft gespeichert werden - auf Vorrat, falls jemals ermittelt werden sollte.

Zuvor war das in allen EU-Ländern unterschiedlich geregelt. In manchen gab es eine Pflicht zur Speicherung - in Deutschland war dies dagegen ausdrücklich verboten. Offiziell durften die Telekommunikationsunternehmen hierzulande die Daten nur so lange aufbewahren, wie sie diese brauchten, um die Gebühren abzurechnen.

Die Polizei fühlte sich dadurch eingeschränkt: Denn oft seien Daten schon längst gelöscht gewesen, wenn Ermittler darauf zugreifen wollten, argumentiert Konrad Freiberg, der Vorsitzende der Gewerkschaft der Polizei. „Nicht bei allen Straftaten, aber bei mittlerer bis schwerer Kriminalität“ sei die Speicherung nötig“, fordert Freiberg. Weil die Inhalte der Kommunikation nicht gespeichert würden, seien die Bürgerrechte nicht tangiert.

Das sehen Kritiker anders - auch im Europaparlament, das der geplanten Richtlinie des Ministerrats zustimmen musste. Über Handy-Daten könnten möglicherweise Bewegungsprofile erstellt werden. Auch die Speicherung, welche Websites ein Internetnutzer besucht habe, sei ein großer Eingriff in die Privatsphäre.

Das Parlament ernennt Ausschussmitglied Alexander Alvaro zum Berichterstatter in Sachen Vorratsdatenspeicherung. Doch komplett abwenden lässt sich die Speicherung aufgrund des politischen Drucks kaum noch, merken die Abgeordneten bald. Alvaro versucht, die Richtlinie wenigstens zu entschärfen: Welche Daten sollen genau gespeichert werden? Wie lange? Wer trägt die Kosten? So entsteht im Justizausschuss eine abgemilderte Version der Richtlinie.

Am 14. Dezember 2005 soll Alvaro den Kompromissentwurf im Parlament vorstellen, das am Tag darauf entscheiden soll. Doch bereits einige Tage vorher erfährt der Liberale, dass er schon verloren hat. Kurz zuvor hatte der britische Innenminister Charles Clarke als amtierender Vorsitzender des Ministerrats die Chefs der beiden größten Parlamentsfraktionen kurz zuvor noch einmal ins Gebet genommen. Statt den ausgehandelten Kompromiss mit zu tragen, setzten Sozialisten und Konservative daraufhin zahlreiche Änderungswünsche auf die Tagesordnung. „Die eingebrachten Änderungsanträge entsprachen 1:1 der Richtlinie des Rates“, erinnert sich Alvaro: „Letztendlich hat der Rat über die beiden großen Fraktionen damit das, was er auch wollte, durchsetzen können“. Mit bitter klingender Stimme hatte er seinen Namen unter dem Parlamentsbericht zur Richtlinie zurückgezogen, während Clarke und EU-Justizkommissar Franco Frattini in der Pressekonferenz äußerst zufrieden die Fortschritte in der Terrorbekämpfung herausstellen.

Im Frühjahr 2006 segnete der Ministerrat die Richtlinie ab. Bis Ende 2008 müssen die EU-Mitgliedsstaaten nun eigene nationale Gesetze daraus machen. Die Daten für sämtliche Verbindungen müssen nun von den Telekommunikationsunternehmen mindestens dauerhaft gespeichert werden - mindestens sechs Monate, höchstens zwei Jahre - auf Antrag der Staaten allerdings auch noch längere Speicherzeiten.

Die Befürworter der Richtlinie sind zufrieden: „Ich glaube, dass man sagen kann, hier ist Missbrauch ausgeschlossen“, beruhigt GEP-Chef Freiberg. Doch es könnte künftig mehr Menschen gehen wie Peter Strehmel im Juli 2005. Damals fand der freie Journalist der Bad Segeberger Zeitung in Schleswig-Holstein auf einmal einen unerwarteten Schreiben in seinem Briefkasten. Absender: die Kriminalpolizei.

„Habe ich irgendetwas angestellt?“ schoss es Strehmel durch den Kopf. Die Polizei wollte von ihm wissen, wo er in einer ganz bestimmten Nacht einige Wochen zuvor gewesen war. Damals hatte in Bad Segeberger ein Sonderpostenmarkt gebrannt. Die Polizei ermittelte wegen einer Brandserie und hatte Strehmels Handy zusammen mit mehreren hundert anderen Mobiltelefonen im Tatzeitraum in der Nähe des Brandes geortet. Kein Wunder: Weil Strehmel in der Nähe wohnt, hatte ein Kollege aus der Redaktion versucht, ihn zu erreichen und zum Brandort zu schicken. Doch der Lokalreporter hörte sein Handy nicht.

Dennoch war er für die Polizei ein Zeuge, der um „Mithilfe“ gebeten wurde. Die Ermittler wollten genaue Angaben, was er in der Nacht gemacht hatte. Der Zeuge fühlte „Angst und Ärger“: „Das ist so ähnlich wie bei Massengentests. Ich muss reagieren. Wenn nicht reagiere, was passiert dann? Wirklich, man wird dann zu den Verdächtigen gedrängt.“

Für den schleswig-holsteinischen Datenschutzbeauftragten war das, was Strehmel und hunderte andere Handy-Besitzer erlebten, definitiv nicht in Ordnung. Nur zum Aufspüren „von Kontaktpersonen, nicht von Zeugen“

dürften die Ermittler so handeln, sagt Thilo Weichert. Für Landesinnenminister Ralf Stegner haben die Ermittler

dagegen alles richtig gemacht: „Ich will es einmal umdrehen: Wenn die Polizei, das was sie könnte, nicht tut, hat die Bevölkerung dafür wenig Verständnis.“

Man dürfe nicht über das Ziel hinausschießen, nicht die Freiheiten aufgeben, die man verteidigen wolle, ist Stegners grundsätzlicher Standpunkt. Stattdessen redet er gerne von der „Bürgerpolizei“. Und um den Bürger besser zu schützen, bekommt diese in Schleswig-Holstein mehr Rechte - durch eine neues Polizeigesetz, das Stegner „pragmatisch und modern“ nennt. Die Polizei soll verstärkt schon vorbeugend tätig werden, Methoden wie die Schleierfahndung, Telefon- und

Videoüberwachung von öffentlichen Plätzen werden ausgebaut, Beschränkungen bei der Rasterfahndung fallen weg. Und das Gesetz bereitet vor, was Bundesinnenminister Schäuble und viele seiner Länderkollegen einführen möchte: Auf den Autobahnen sollen Kennzeichen für Polizeizwecke erfasst werden. Benutzt werden sollen dafür die Mautanlagen, die bereits den Lkw-Verkehr elektronisch überwachen. In Zukunft könnte auch jeder private PKW erfasst werden, befürchtet der Datenschutzbeauftragte Weichert: „Die Konsequenz wird sein, dass immer mehr Bewegungsprofile zumindest theoretisch möglich sind und dann vielleicht auch irgendwann mal erstellt werden. Das heißt, das anonyme Nutzen des Straßenverkehrs wird künftig nicht mehr möglich sein.“

Aber ist Anonymität im 21. Jahrhundert nicht längst eine anachronistische Vorstellung? Täglich hinterlässt jeder seine Datenspuren. Zum Beispiel völlig unbewusst beim Einkaufen:

Wer interessiert sich für welche Produkte? Wie viel Geld steht dafür zur Verfügung? Das sind Fragen, auf die die großen Konzerne Antworten suchen. Millionen Kunden helfen ihnen dabei, in dem sie an der Kasse ihre Treue- und Bonuskarten herüberreichen. Die Kunden sparen ein paar Cent, die Unternehmen gewinnen wertvolle Konsumdaten. Marktführer ist in Deutschland die Firma Loyalty Partners mit ihren Payback-Karten, die

„Da wird die Freiheit zu einer Gefahr, vor der man in der Sicherheit Zuflucht sucht.“
Burkhard Hirsch

dafür auch immer wieder beim Big-Brother-Award als Negativbeispiel herausgestellt wurde.

„Wenn meine kompletten Einkäufe über ein ganzes Jahr oder viele Jahre gespeichert werden, dann sagt das sehr viel über mich. Lebe ich allein oder in einem Haushalt mit Kindern? Wird aus der Frischeabteilung eingekauft oder nur Chips und Bier? Das ist zum Beispiel für Versicherungen interessant, die möglichst gesunde Kunden haben möchte, die für sie wenig Kosten verursachen“, sagt Award-Organisatorin Rena Tangens. Seit Jahren kämpfen Tangens und der FoeBuD e. V. gegen solche Bonusprogramme, durch die sich Kunden mangels Datenschutz selbst gläsern machen. Potenziert werden die Gefahren nach Meinung des FoeBuD durch RFID-Funkchips, die sich in immer mehr Gegenständen verstecken: „Ein gewaltiges Potenzial für neue Überwachungsmöglichkeiten und Manipulationsmöglichkeiten“, ist Tangens überzeugt.

Die winzigen Chips verstecken sich meist auf der Rückseite eines normalen Warenetiketts. Sie sind ohne Berührung von entsprechenden Scannern auslesbar und über eine weltweite Seriennummern eindeutig identifizierbar: So kann etwa in der Logistik nicht nur der Inhalt einer Warenpalette im Lager automatisch registriert werden, sondern auch, um welche einzelne Palette es sich genau handelt. „Wir rechnen in der Logistik mit einem Einsparungspotenzial bis zu fünfzehn Prozent. Durch die neue Technik sind immer individuellere Waren und Dienstleistungen möglich“, sagt Profes-

sor Michael ten Hompe, Experte des Fraunhofer-Instituts in Dortmund.

Einsparungen bei der Logistik für sich selbst und individuelle Dienstleistungen für die Kunden verspricht auch der Einzelhandelsriese Metro. Der Konzern betreibt in Rheinberg bei Duisburg seinen „Future Store“, ein großes Testlabor für den Einkauf der Zukunft. Kunden mit einer Payback-Karte können hier einen persönlichen Einkaufsberater nutzen. Das Gerät speichert die Einkäufe der Vergangenheit und kann mit diesem Wissen kann individuelle Angebote unterbreiten. Auch RFID spielt im Rheinberger Feldversuch eine Rolle. Erste Produkte sind mit den kleinen Chips ausgestattet - nur zu Logistikzwecken, wie der Metro-Konzern versichert. Doch ein Firmenvideo zeigt für die Zukunft noch andere mögliche Anwendungen: Der Weg der Kundin durch den Future Store wird genau festgehalten. Eine neue Qualität: Künftig kann nicht nur wie bei normalen Bonuskarten erfasst werden, was ein Kunde bereits gekauft hat. Schon dass er ein Produkt auch nur aus der Nähe betrachtet, kann theoretisch über die RFID-Funkwellen erfasst werden. Für Rena Tangens sind eine Vielzahl von automatischen Preisdiskriminierungen denkbar. So könnte dem guten Kunden etwas billiger angeboten, für andere etwas künstlich verteuert werden - im Extremfall, um Abhängigkeiten auszunutzen oder unerwünschte Kundschaft fernzuhalten.

Voraussetzung für solche automatischen individuellen Angebote ist, dass die Kunden über einen

eigenen RFID-Chip zu identifizieren sind, den sie bei sich tragen - zum Beispiel in einer Kundenkarte. Über diesen Aspekt seines „Future Konzerns“ schwieg der Metro-Konzern lieber - bis eine Expertin im Auftrag des FoeBuD eine der Rheinberger Kundenkarten auseinandernahm: Darin verbarg sich ein RFID-Chip. „Und damit sind zehntausend Kunden ein Jahr lang herumgelaufen“, schildert Tangens.

In ein paar Jahren wird wohl jeder Deutsche einen solchen eindeutig zu identifizierenden Funkchip in der Tasche haben: Die neuen, ebenfalls als Folge des 11. Septembers eingeführten Reisepässe



und künftig auch die Personalausweise enthalten nicht nur die Körpermerkmale des Besitzers. Diese werden auch auf einem RFID-Chip gespeichert. Auch die Eintrittskarten bei der Fußball-Weltmeisterschaft waren mit Chips versehen. Die RFID-Befürworter bemühen sich, Bedenken zu entkräften: Die Chips garantieren Fälschungssicherheit und seien nur von den entsprechenden Kontrollgeräten an Grenzen und Stadioneingängen zu lesen. Berührungslos lesbar, das beziehe sich auf einen paar Zentimeter Abstand zwischen Chip und Lesegerät - und bedeute nicht, dass Überwacher orten könnten, ob sich ein Ticketbesitzer im Stadion am Würstchenstand oder auf der Toilette aufhalte.

Solchen Beteuerungen zum Trotz bleiben die Datenschützer skeptisch: „Je stärker die elektronische Vernetzung wird, desto stärker werden auch die Überwachungsmöglichkeiten“, warnt Schaar. Sein Kollege Weichert: „Das große Problem ist, dass Menschen erst aufwachen, wenn sie direkt betroffen sind. Wir müssen vor einer Gefahr warnen, die vielleicht erst in fünf oder zehn Jahren kommt.“

Doch Datenschützer stehen nicht selten als übervorsichtige Bedenkenräger dar. Auf der anderen Seite setzen die Innenpolitiker in Bund und Ländern auf einfache Rezepte. Mit immer neuen Vorschlägen zur Überwachung versuchen sie sich zu überbieten. „Man muss natürlich nüchtern feststellen: Die Länderinnenpolitiker stehen unter dem Druck ihrer Bürger“, konstatiert Staatssekretär Hanning: „Innere Sicherheit ist ein sehr hohes Gut.

Deshalb sind die Länderpolitiker gezwungen, über neue Maßnahmen nachzudenken.“

„Wenn ein Sicherheitsdefizit da ist, dann ist der Ruf nach dem Staat ja immens groß“, meint der schleswig-holsteinische Innenminister Stegner. Prävention ließe sich hingegen schlechter beweisen, aber: „Von manchen Menschen wollen wir, dass sie sich beobachtet fühlen.“

Überwachung in Fußballstadien, öffentlichen Verkehrsmitteln, Flughäfen oder Geldautomaten - darum müsse sich der Staat kümmern, das sei kein Eingriff in die Grundrechte, sagt Stegner, so lange die Verhältnismäßigkeit gewahrt bleibe. „Datenschutz ist ein hohes Gut. Aber Datenschutz darf kein Täterschutz werden“, formuliert Hanning eine Maxime, die man immer wieder hört. Warum schlägt den Politikern dann aber bei ihren Vorstößen regelmäßig das Bundesverfassungsgericht auf die Finger, wie zum Beispiel beim großen Lauschangriff? „Sicherlich mit gutem Grund“, meint Hanning. Aber das Recht auf informationelle Selbstbestimmung, das das Verfassungsgericht in seinem Volkszählungsurteil 1983 aus dem Grundgesetz herausgelesen hat, habe er dort noch nicht gefunden.

Jeder Mensch habe das Recht selbst darüber zu entscheiden, welche persönlichen Daten er von sich preisgibt, urteilten die Richter seinerzeit. Das Prinzip der informationellen Selbstbestimmung leiteten sie aus der Menschenwürde und dem Recht auf persönliche Handlungsfreiheit ab. Wer jedoch nicht weiß, was mit seinen Daten geschieht, was

andere über ihn speichern und weitergeben, kann als Einzelner wie Peter Strehmel böse Überraschungen erleben. Doch während angesichts der Volkszählung sich tausende Bundesbürger weigerten, über ihre privaten Verhältnisse Auskunft zu geben, geben heute viele freiwillig viele privatere Daten preis.

„Wir haben eine andere Situation als bei der Volkszählung, wo man ja gefragt wurde und sich dann aktiv zur Wehr setzen konnte“, sagt Weichert: „Heute ist es ein passives Erleiden und schwieriger, sich dagegen zur Wehr zu setzen.“ „Wenn in einer Straße plötzlich eine Videokamera aufgestellt wird, wird man sie meist weiter benutzen“, meint Michael Arzt. Jeder Bürger vertraue darauf, dass er ja im Endeffekt nichts zu verbergen habe.

Der Bundesdatenschutzbeauftragte fürchtet aber, dass letztlich doch das Eintreten könnte, was die Bundesverfassungsrichter als Schreckensbild an die Wand malten: eine Gefährdung der Demokratie. „Ich kann mir denken, dass diese Überwachungsneigung letztlich dazu führt, dass man bestimmte als kritisch angesehene Verhaltensweisen doch dann sein lässt“, sagt Schaar. „Wenn man tatsächlich nachvollziehen kann, an welchem Ort ich mich millimetergenau aufgehalten habe, ob ich an einer bestimmten Versammlung teilgenommen habe, wenn ich zum Beispiel Beamter bin ...“ Das sei mit dem Grundgesetz nicht vereinbar: „Weil auf diese Weise ein Stück Konformitätsdruck erzeugt wird, und zwar unabhängig von der Frage, ob die

Behörden tatsächlich auf die Daten zugreifen oder nicht.“

„Vom Überwachungsstaat sind wir wirklich weit entfernt“, hält Stegner dagegen. „Wir haben überhaupt nicht das Personal, um so viel auszuwerten. Bewegungsprofile von 80 Millionen Deutschen? Das ist doch eine groteske Vorstellung.“

Doch nicht nur für Rena Tangens ist das Schreckensszenario „dass Daten miteinander verknüpft werden“, durchaus real. Und „dann können wir nicht mehr frei entscheiden, weil wir nicht mehr gefragt, sondern aufgrund von Daten aus unserer Vergangenheit beurteilt werden.“

Bisher haben Kritiker wie Tangens die zunehmende Überwachung unseres Alltags dennoch nicht verhindern können. „Es ist ein Kampf gegen mächtige Gegner, ein Kampf gegen Windmühlen - doch das ist halt so“, sagt Michael Arzt und will nicht aufgeben. Und Tangens ist überzeugt: „Es braucht nur eine kritische Masse von vielleicht zwanzig Prozent der Bevölkerung. Wenn die sagt: ‚Hilfe, ich trage einen Chip bei mir!‘ - und das ist etwas, was Menschen nicht möchten - dann können das auch große Firmen nicht ignorieren.“

Fotos: Mischel/Stegers

Text: Stegers

Ein Trailer des Films ist unter www.onlinejournalismus.de zu sehen.

Online-Festplattendurchsuchungen

Nordrhein-Westfalens Innenminister Ingo Wolf (FDP) stellte im Sommer den Entwurf für das neue Verfassungsschutzgesetz vor. Dieses sieht nun „heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel“ als Aufgaben des Verfassungsschutzes an. Vor allem der letzte Satz hat es in sich. Denn dieser ermöglicht künftig die Online-Durchsuchung von Festplatten in Wohnungen. Und das ohne den Beschluss eines Richters/einer Richterin oder der G10 Kommission (Kommission zur Kontrolle der Eingriffe des Verfassungsschutzes in das Brief-, Post- und Fernmeldegeheimnis). Dieses bedeutet, dass es allein von der Willkür des Verfassungsschutzes abhängt, wessen Festplatte durchsucht wird. Unklar ist noch wie diese Durchsuchungen technisch laufen sollen. Eine Möglichkeit wäre das Einsetzen von Trojanern, die per Mail verschickt werden und welche

die Spionageprogramme dann auf den Rechnern installieren würden. [1] Klar ist jedoch, dass sie laufen sollen, ohne dass die/der Betroffene davon erfährt und sich somit auch nicht dagegen wehren kann. Laut Bundesverfassungsgericht sind solche Eingriffe verfassungswidrig, da die Daten auf dem PC „durch das Recht auf informationelle Selbstbestimmung und gegebenenfalls durch das Recht auf Unverletzlichkeit der Wohnung geschützt“ [2] seien. Denn eine solche Maßnahme käme einer Hausdurchsuchung gleich, welche der/dem Betroffenen bekannt sein müsste, damit er/sie grundsätzlich die Möglichkeit habe, bereits der Durchführung der Maßnahme entgegenzutreten, wenn es an den gesetzlichen Voraussetzungen fehlt, oder aber zumindest die Einhaltung der im Durchsuchungsbeschluss gezogenen Grenzen zu überwachen.

[1] http://www.fr-online.de/in_und_ausland/politik/aktuell/?em_cnt=1033879

[2] <http://www.bundesverfassungsgericht.de/pressmitteilungen/bvgo6-013>

Rasterfahndung

Unmittelbar nach dem 11.09.2001 war es wieder soweit: „Neues aus der Mottenkiste“ titelte die Deutsche Richterzeitung, als sich die Innenminister der Länder entschlossen hatten, ein Instrument der Terrorbekämpfung aus den 70er Jahren wieder einzusetzen: Die Rasterfahndung. Bei der Rasterfahndung werden verschiedene Dateien gegeneinander abgeglichen, weil man vermutet, dass sich in der Schnittmenge Tatverdächtige befinden. So war es etwa bei der Rasterfahndung im Zuge der Terrorismusbekämpfung Ziel, sogenannte „konspirative Wohnungen“, also Wohnungen, die von Mitgliedern der RAF benutzt wurden, zu finden. Da man davon ausging, dass die Mieter bar gezahlt wurde und kein Telefon angemeldet ist, wurden die Daten der bar zahlenden Mieter in Großwohnanlagen mit der Liste der Telefonanschlüsse abgeglichen. Daraus konnte man dann ermitteln, welche Mieter ihre Wohnung bar bezahlten und gleichzeitig über keinen Telefonanschluss verfügten. Das ganze ging soweit, dass auch die Dateien der Zahler von Hundesteuer abgeglichen wurden, weil

man davon ausging, dass Terroristen, wenn sie schon einen Hund halten, jedenfalls für ihn keine Hundesteuer bezahlen. Auf diese Weise wurde der Kreis der „verdächtigen Wohnungen“ immer weiter eingegrenzt und dann der Rest genauer durch die Polizei untersucht.

Nach dem 11.09.2001 suchte man nicht nach Mietern, die ihre Wohnung bar zahlten, sondern es wurden Rasterkriterien aufgrund von Mitgliedern der Täter des 11.09.2001 aus Hamburg ermittelt. Dabei wurden die Daten lediglich von drei Mitgliedern dieser Zelle herangezogen deren Gemeinsamkeiten machten das Raster aus. Danach ergaben sich dann die Rasterkriterien, dass eine Person im Alter von 18 bis 40 Jahre gesucht wurde, die männlich ist, Student oder ehemaliger Student ist, die als Religion dem Islam anhängt, sich legal in Deutschland aufhält und aus einem Staat mit vorwiegend islamischer Bevölkerung stammt. Faktisch wurden damit alle Studierenden mit irgendeinem Bezug zu islamischen Ländern erfasst. Die Daten wurden dann von den Länderpolizeibehörden an das Bundeskriminalamt weitergegeben und dort mit weiteren Dateien abgeglichen. Die eigentliche Rasterfahndung, also der Abgleich der Dateien fand also beim Bundeskriminalamt statt.

Das Bundesverfassungsgericht hatte diese Maßnahme in seinem Beschluss vom 04.04.2006 für rechtswidrig erklärt.

Eine rein juristische Betrachtung eines solchen Vorgangs wäre einigermaßen beschränkt. Die juristische Betrachtung stellt nämlich nur die

Frage, ob die Maßnahme erlaubt ist, „Darf der Staat das?“ also mit den herrschenden Gesetzen übereinstimmt. Nicht gestellt ist die Frage: „Was will der Staat?“. Um diese Frage soll es deshalb zunächst einmal gehen.

Die Rasterfahndung wurde in der Öffentlichkeit weitgehend damit gerechtfertigt, dass es in erster Linie darum gegangen wäre, Mittäter der Anschläge in New York oder Washington aufzuspüren oder aber die weitere Begehung

derartiger Anschläge zu verhindern. Nimmt man sich allerdings die Anträge vor, mit denen die Polizei die Durchführung der Rasterfahndung bei den Gerichten beantragt hat, so fällt auf, dass der Kontext der Rasterfahndung ein viel weitergehender war.

So wurde etwa zur Begrün-

dung der Rasterfahndung in Hessen ausdrücklich ausgeführt, „für den Fall eines Angriffs US-amerikanischer Streitkräfte gegen Ziele in Afghanistan und/oder der anderen Unterstützerstaaten mit hohen Opferzahlen unter der Zivilbevölkerung“ sei „mit einer Vielzahl von Demonstrationen unter großer Beteiligung der in Deutschland lebenden muslimischen Bevölkerung zu rechnen. Daneben sind Gewalttaten durch extremistische islamische Kreise in der Bundesrepublik einzukalkulieren.“, Amtsgericht Wiesbaden, Beschluss vom 25.09.2001, Aktenzeichen 71 Gs 531/01. Die Rasterfahndung

„Das neue Sicherheitsdenken geht von einer absurden Logik aus. Je geringer der Verdacht, umso geringer die Rechte des Bürgers. Das läuft darauf hinaus, dass, wenn es keinen Verdacht gibt, der Bürger sich alles gefallen lassen muss.“

Heribert Prantl

stand also von vorneherein im Zusammenhang mit dem nach dem 11.09.2001 einsetzenden „Krieg gegen den Terrorismus“, den die USA und ihre NATO-Verbündeten weltweit führten. Die für die Anordnung der Rasterfahndung notwendige gegenwärtige Gefahr wurde vom Landgericht Düsseldorf folglich wie folgt begründet: „Dies ergibt sich bereits daraus, dass seitens der Bundesregierung die uneingeschränkte Solidarität – ggf. auch mit

militärischen Mitteln – mit dem Vorgehen der Vereinigten Staaten wiederholt bekundet wurde und dass seitens der hinter den Anschlägen vom 11.09. vermuteten Organisationen spätestens seit der Militärfeldaktion gegen Afghanistan Vergeltungsschläge gegen die an den militärischen Aktionen beteiligten Staaten angekündigt wurden.“, Landgericht Düsseldorf, Beschluss vom 29.10.2001, Aktenzeichen 25 T 873/01.

Bei der Rasterfahndung ging es also nicht nur um eine Methode polizeilicher Arbeit, mit der Rasterfahndung sollte auch die innenpolitische Stabilität Deutschlands in Kriegszeiten sichergestellt werden. So verwundert es nicht wesentlich, dass die Rasterfahndung – obwohl kein Terrorist gefangen wurde – trotzdem als Erfolg gefeiert wurde. Das Bundeskriminalamt etwa führt in seinem Evaluierungsbericht zur Rasterfahndung aus, dass aufgrund der Medienberichterstattung die Raster-

fahndung eine einschüchternde Wirkung auf „das islamistische Potential“ in Deutschland gehabt habe. Zu der von der Polizei Hessen befürchteten „Vielzahl von Demonstrationen unter großer Beteiligung der in Deutschland lebenden muslimischen Bevölkerung“ ist es jedenfalls nicht gekommen. Die Rasterfahndung kann also ebenso wenig von der neuen militärischen Rolle getrennt werden, die Deutschland in der Welt spielt wie dies etwa bei den Verschärfungen im Ausländerrecht der Fall ist.

Die Rasterfahndung ist auch ein Beleg dafür, wie ungeheuer „flexibel“ der Staat auf eine neue Situation reagiert. Der Förderalismus in Deutschland erwies sich als alles andere als „lahm“. Da das Polizeirecht Ländersache ist, war es zunächst notwendig, in allen Bundesländern überhaupt eine Rechtsgrundlage für die Rasterfahndung zu schaffen. Eine solche fehlte in Niedersachsen und in Schleswig-Holstein. In Bremen hatte man sie sogar wenige Monate vor dem 11. September abgeschafft, weil man meinte, dieses Instrumentarium sei überflüssig geworden. Wie stets in Kriegs- und Krisenzeiten dauerte es nur wenige Wochen, bis die parlamentarischen Beratungen – so sie überhaupt stattgefunden haben – abgeschlossen waren und alle Länder entsprechende gesetzliche Regelungen hatten.

Das zweite Dilemma der Rasterfahndung rührte vom Ursprung dieses polizeilichen Instruments her. Ausgelegt war die Rasterfahndung darauf, eine gegenwärtige erhebliche Gefahr abzuwenden. Man stellte sich wie oben dargestellt ja vor, dass eine

konspirative Wohnung von Terroristen gefunden werden sollte, um etwa dort entführte Personen befreien zu können. Für diese Personen bestand selbstverständlich eine gegenwärtige Gefahr für Leib und Leben. Eine gegenwärtige Gefahr ist nämlich dadurch gekennzeichnet, dass der Schaden mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht oder schon teilweise eingetreten ist.

Entsprechend waren die Polizeigesetze beispielsweise in Nordrhein-Westfalen noch auf diese Suche nach entführten Personen ausgerichtet. Ungleich schwieriger war es da, die doch relativ diffuse Gefahrenlage Ende 2001 unter diese gesetzlichen Voraussetzungen zu fassen. Diese Aufgabe ist natürlich für einen ausgebildeten deutschen Juristen ohne Weiteres lösbar. Schließlich gelingt es den deutschen Juristen auch, mit dem Bürgerlichen Gesetzbuch aus dem Jahre 1900 alle Miet- und sonstigen Rechtsprobleme des Zivilrechts zu lösen und dabei dem Zeitgeist des Kaiserreichs ebenso Rechnung zu tragen, wie dem des Nationalsozialismus oder dem Rechtsstaat der Bundesrepublik Deutschland in all seinen Wandlungen von den 50er Jahren bis zu den 90er Jahren.

Die Argumentationsfigur der Richter, die eine gegenwärtige Gefahr in der Regel angenommen hatten, las sich ungefähr so: Je größer der mögliche Schaden, desto geringer sind die Anforderungen, die an einen Nachweis der Gefahr zu stellen sind. Und da es hier immerhin um den ersten Bündnisfall der NATO ging, waren die Gefahren derart unermesslich, dass die Rasterfahndung für zulässig

erklärt wurde. Einzig die Zivilgerichtsbarkeit in Hessen tanzte aus der Reihe und versagte der Rasterfahndung ihren Segen. Das Oberlandesgericht Frankfurt begründete dies mit Worten, die an Deutlichkeit nichts zu wünschen offen ließen. „Mit der Übertragung der Entscheidungskompetenz und Verantwortung auf die Gerichte ist zugleich die Erwartung verbunden, dass sich die zur Entscheidung berufenen Richterinnen und Richter – auch in Krisenzeiten – nicht von eigenen Emotionen oder Emotionen anderer, sondern ausschließlich vom Gesetz leiten lassen (Art. 20 Abs. 3, 92,97 Abs. 1 GG, § 25, 38 DRiG)“. Nach Ansicht des Oberlandesgerichts Frankfurt lag keine konkrete Gefahr für die Begehung von Terroranschlägen vor, jedenfalls war sie von den Polizeibehörden nicht dargelegt worden.

Wie reagiert in dieser Situation die Regierung in Hessen? CDU und FDP ändern das Polizeigesetz und erklären das Oberlandesgericht Frankfurt für unzuständig. Die Rasterfahndung bedurfte in Hessen nicht mehr der vorherigen Anordnung durch die Gerichte. Zuständig für ihre Überprüfung waren nunmehr die Verwaltungsgerichte. Auch das war der Polizei offenbar ein zu großes Risiko: Als ein Studierender in Hessen vor dem Hessischen Verwaltungsgerichtshof die weitere Rasterung seiner Daten verhindern wollte, erklärte das Landeskriminalamt kurzerhand den Verzicht auf die Daten dieses klagenden Studierenden, so dass die Rasterfahndung faktisch nicht mehr rechtlich überprüft wurde.

Insoweit sind die gerichtlichen Auseinandersetzungen um die Rasterfahndung also auch eine Lehrstunde über die Rolle von Justiz und Polizei in Kriegs- und Krisenzeiten geworden.

Zur Entscheidung des Bundesverfassungsgerichts:

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 04.04.2006 der polizeilichen Rasterfahndung nach dem 11.09.2001 dann erhebliche Grenzen aufgezeigt. Das Bundesverfassungsgericht ist der Auffassung, zwar müsse keine gegenwärtige Gefahr für eine Rasterfahndung gegeben sein – also die Situation muss nicht vergleichbar mit der Suche nach einem von Terroristen entführten Industriellen sein -, es reiche allerdings eine konkrete Gefahr aus. Eine solche konkrete Gefahr müsse es dann aber schon sein. Eine Dauer Gefahr, wie sie nach dem 11.09.2001 eigentlich immer vorliege, reiche insoweit nicht aus. Das ergibt sich aus Sicht des Bundesverfassungsgerichts auch daraus, dass es sich bei der Rasterfahndung in Zeiten der modernen Datenverarbeitung um einen erheblichen Grundrechtseingriff handelt. Angesichts der Vielzahl der Daten, die über Personen gespeichert sind, sei dies durch die Banken, sei es durch die Kundenkarten der großen Kaufhäuser, sei es durch die Daten, die bei Bibliotheken etc. vorhanden sind (etwa auch im StudiVZ) sei es ohne Weiteres möglich, ein komplettes Persönlichkeitsbild über einzelne Personen zu bilden. Es mache keinen wesentlichen Unterschied, ob die Daten gleich bei der Polizei gespeichert seien oder

von der Polizei nur jederzeit abrufbar sind. Ebenso wie es der Polizei untersagt sei, sich durch das Sammeln von Daten ein umfassendes Persönlichkeitsbild zu verschaffen, sei eine Übermittlung dieser Daten im Einzelfall an die Polizei nur unter der Voraussetzung zulässig, dass tatsächlich eine konkrete Gefahr für die öffentliche Sicherheit gegeben sei. Das Bundesverfassungsgericht hat damit eine allein einem bloßen Verdacht nachgehenden Rasterfahndung eine Absage erteilt. Gleichzeitig ist das Instrument der Rasterfahndung nicht grundsätzlich in Frage gestellt.

Die Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung reiht sich ein in eine ganze Reihe von Entscheidungen, mit denen das Bundesverfassungsgericht der Neuentwicklung des Rechtsstreits im Zuge des Kriegs gegen den Terrorismus Grenzen aufzeigt. Dies betrifft etwa auch das Luftsicherheitsgesetz, mit dem der Staat ermächtigt worden ist, Passagierflugzeuge abzuschießen. Politische Auseinandersetzungen um Grundrechte in Kriegs- und Krisenzeiten dürfte uns allerdings wohl noch einige Jahre beschäftigen, denn es sieht nicht so aus, als wenn die Kriege und die Krisen weniger würden.

Wilhelm Achelpöehler
Fachanwalt für Verwaltungsrecht

Freiheit oder Sicherheit?

Im Kampf gegen den Terrorismus ist den Sicherheitsbehörden jedes Mittel recht.

Seit dem 11. September 2001 hat sich das politische Klima nicht nur in den USA geändert. Die Politik schürt die Angst vor dem „Internationalen Terrorismus“ und bietet auch die vermeintlich passenden Lösungen: Mehr Kontrollen und mehr Überwachung sollen für mehr Sicherheit sorgen. Der Datenschutz und die Bürgerrechte bleiben auf der Strecke. Datenspeicherungen auf Vorrat, Videoüberwachung aller Orten und Lauschangriffe innerhalb und außerhalb von Wohnungen sollen für mehr Sicherheit sorgen - als ob sich jemals eine Videokamera oder ein Mikrofon zwischen Täter und Opfer geworfen hätte. An zwei Beispielen soll diese beunruhigende Entwicklung verdeutlicht werden.

Vorratsdatenspeicherung – eigentlich verfassungswidrig

Anfang 2006 wurde eine EU-Richtlinie erlassen, nach der Telekommunikationsverkehrsdaten für mindestens sechs Monate von den Telekommunikations- und Internet-

unternehmen gespeichert werden müssen. Dem gingen mehrere Versuche voraus, vergleichbare Regelungen in verschiedenen EU-Staaten auf nationaler Ebene einzuführen. Die ist in den jeweiligen Staaten politisch nicht durchsetzbar gewesen. Nach der EU-Richtlinie muss die Speicherung der Daten selbst dann erfolgen, wenn zum Beispiel wegen einer Flatrate diese Daten für Abrechnungszwecke gar nicht benötigt werden. Durch diese Vorratsdatenspeicherung ist nachvollziehbar, wer wann mit wem per Telefon, Fax, Handy oder E-Mail kommuniziert hat. Bei Handy- und SMS-Nutzung wird darüber hinaus der Standort des Benutzers festgehalten. Auch wer über welchen Provider das Internet wie lange genutzt hat, wird nach der EU-Vorratsdatenspeicherungsrichtlinie für mindestens sechs Monate gespeichert.

Als Begründung müssen der internationale Terrorismus und die organisierte Kriminalität herhalten. Dabei sind diese Kreise in der Lage, durch technische Maßnahmen wie Verschlüsselung und Anonymisierungstechniken oder aber durch den Umstieg auf klassische Kommunikationsmittel, die Vorratsdatenspeicherung zu umgehen. Übrig bleiben die Daten von ganz normalen Bürgern. Es ist davon auszugehen, dass die Vorratsdatenspeicherung keinen einzigen Anschlag „internationaler Terroristen“ verhindert und auch die Aufklärung solcher Anschläge nicht erleichtert.

Ein weiterer Grund für diese Einschätzung ist die riesige Menge an Daten, die durch die Vorratsdatenspeicherung anfällt. Selbst mit modernsten

Computern und Programmen lassen sich diese Datenwüsten nicht auf die Schnelle durchsuchen.

Nicht ohne Nebenwirkungen!

Die mit der Vorratsdatenspeicherung verbundenen Schäden an der Demokratie werden billigend in Kauf genommen.

Alle 450 Millionen EU-Bürgerinnen und -Bürger werden unter Generalverdacht gestellt. Die Vorratsdatenspeicherung greift unverhältnismäßig in die persönliche Privatsphäre ein. Sie beeinträchtigt berufliche Aktivitäten insbesondere in den Bereichen Medizin, Recht und Seelsorge aber auch im Journalismus. Welcher Informant traut sich dann noch, mit Journalisten zu telefonieren, wenn er weiß, dass dies für mindestens sechs Monate nachvollziehbar ist?

Nicht umsonst hat das Bundesverfassungsgericht eine Vorratsdatenspeicherung immer wieder als verfassungswidrig abgelehnt. Bereits im Volkszählungsurteil vom 15.12.1983 führt das Bundesverfassungsgericht aus: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner

Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“ Auch mit Recht auf Achtung des Privat- und Familienlebens aus Art. 8 der Europäischen Menschenrechtskonvention ist eine derartige Vorratsdatenspeicherung nicht zu vereinbaren.

Die Rolle der deutschen PolitikerInnen auf EU-Ebene

Auch deutsche PolitikerInnen brechen auf Europäischer Ebene keine Phalanx für die Bürgerrechte. Wenn die Justizministerin Brigitte Zypries behauptet, dass Deutschland nun die Vorratsdatenspeicherung einführen müsse, da dies ja von der EU vorgeschrieben werde, so stimmt das zwar, aber Zypries verschweigt leider, dass weder sie noch der alte und schon gar nicht der neue Bundesinnen-

-Es kommt einfach darauf an, was man will, man muß sich entscheiden: Alle Menschen überall und miteinander vernetzt, global offene Kommunikationskanäle, Überwachung, usw. – und dann aber noch Privatsphäre erhalten, wie wir sie gewohnt sind – das geht nicht!“
Jeremy Rifkin

minister gegen den entsprechenden EU-Beschluss gestimmt haben. Der Deutsche Bundestag hatte zumindest bis Ende 2005 – also auch in der Zusammensetzung der großen Koalition – standhaft alle Anstrengungen von Bundesregierung und Bundesrat abgewehrt, eine Telekommunikations-Vorratsdatenspeicherung auf nationaler Ebene einzuführen. Erst als auch die deutschen Minister (gegen den ausdrücklichen Beschluss des Deutschen Bundestages) auf EU-Ebene den Weg für die

Vorratsdatenspeicherung freimachen, ist der Deutsche Bundestag – leider nachhaltig – umgefallen. Trotz eingereichter Klagen beim Europäischen Gerichtshof gegen die EU-Vorratsdatenspeicherungsrichtlinie sind weder die Bundesregierung noch der Deutsche Bundestag bereit, eine Entscheidung über die Umsetzung der Vorratsdatenspeicherung in deutsches Recht zu verschieben, bis der Europäische Gerichtshof seine Entscheidung getroffen hat. Und das, obwohl die Klagen gute Aussichten auf Erfolg haben. Leider bedingt eine Nichtigkeitserklärung einer solchen EU-Richtlinie nicht, dass die Gesetze der EU-Staaten, die aufgrund der EU-Richtlinie erlassen wurden, automatisch ungültig würden. Dies könnte zu der absurden Situation führen, dass die Vorratsdatenspeicherung in deutsches Recht umgesetzt wurde, aber die entsprechende EU-Richtlinie nicht mehr in Kraft ist.

Die geplante Umsetzung

Ende November 2006 wurde der Gesetzentwurf zur Umsetzung der Vorratsdatenspeicherung in deutsches Recht an die Verbände zu Stellungnahme gegeben. In der Fassung dieses Referentenentwurfs ist vorgesehen, dass „zur Verfolgung von Straftaten“ die TK-Dienstleister und Internetprovider „die gespeicherten Daten den zuständigen Stellen unverzüglich zu übermitteln“ haben. Wie dies in der Praxis umgesetzt werden soll, ist im Gesetzentwurf nicht geregelt. Schwierig wird es allemal, da hierzu große Mengen auf Vorrat gespeicherter Verkehrsdaten durchsucht werden müssen.

Für die Bereiche Festnetz- und Mobiltelefonie (inkl. SMS) sollen die Regelungen zum 15. September 2007 in Kraft treten.

Antiterrordatei:

„Es wächst zusammen, was nicht zusammen gehört“

Zwar kein nationaler Alleingang, aber doch ein sehr rasches Vorpreschen, ist auch im Bereich der inneren Sicherheit festzustellen. Der ehemalige Innenminister Otto Schily erhielt nicht umsonst den „Lifetime-BigBrotherAward“ für sein „Lebenswerk“. Zu seinem „Schaffen“ gehören nicht nur die so genannten Otto-Kataloge als Reaktion auf den 11. September 2001. Schily propagierte in seiner Funktion als Innenminister auch einen Sicherheitswahn, der mit einem Abbau bürgerlicher Rechte einhergeht. Sein Nachfolger Wolfgang Schäuble steht Schily nicht nach. Ein erneuter – vermutlich aber nur vorläufiger – Höhepunkt ist die geplante Einführung der „Anti-Terror-Datei“.

Am 4. September 2006 hat die Innenministerkonferenz (IMK), bestehend aus dem Bundesinnenminister sowie den 16 Landesinnenministern, beschlossen, eine gemeinsame Anti-Terror-Datei einzurichten. Diese Datei soll von den Polizeien und allen 19 Geheimdiensten des Bundes und der Länder gefüllt und genutzt werden. Am 20. September 2006 wurde der Entwurf des „Gemeinsame-Dateien-Gesetzes“ von der Bundesregierung absegnet.

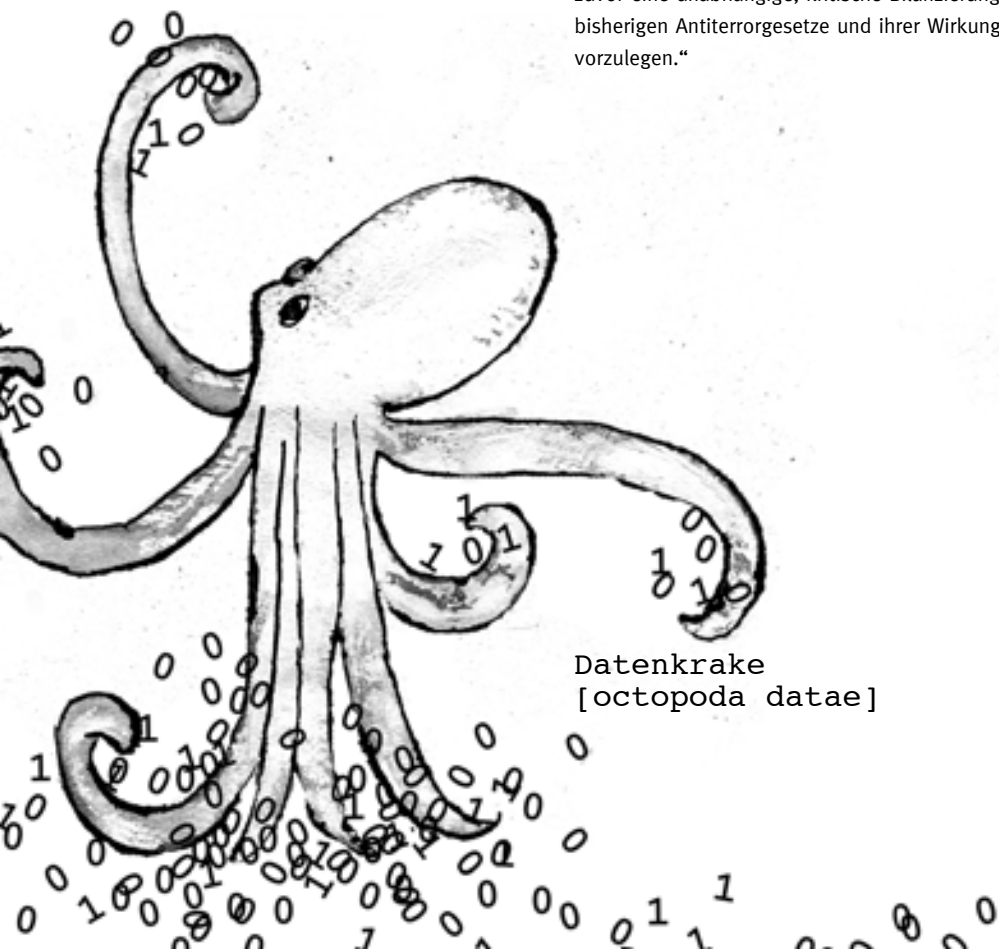
Von der IMK wird die Notwendigkeit der zentralen Anti-Terror-Datei nicht zuletzt mit den Anschlagversuchen auf zwei Regionalzüge im Juli 2006 in Koblenz und Dortmund begründet. Eigentlich sollte den Innenministern bekannt sein, dass die beiden mutmaßlichen Täter vorher weder geheimdienstlich noch polizeilich auffällig geworden waren. Sie wären also in einer solchen Datei überhaupt nicht erfasst worden. Die Innenministerkonferenz spricht hingegen von einer notwendigen „Verbesserung der Zusammenarbeit von Polizeien und Nachrichtendiensten gerade im Hinblick auf den Austausch von Daten über Terroristen“. Dabei sollen in dieser Datei nicht nur rechtskräftig verurteilte Terroristen gespeichert werden. Geplant ist eine Präventivdatei, in der nicht nur Daten von Verdächtigen sondern auch die personenbezogenen Daten mutmaßlicher „Kontaktpersonen“ von Verdächtigen gespeichert werden sollen. Hier besteht die Gefahr, dass auch das soziale Umfeld der bloß Verdächtigen in der Datei vollständig erfasst wird. Dabei sollen „tatsächliche Anhaltspunkte“ ausreichen, um aus einem unbescholtenen Bürger einen Terrorverdächtigen zu machen. Das hat zur Folge, dass dessen Familie, Kinder, Arbeitskollegen, Geschäftspartner, Anwälte, Vermieter, Sportsfreunde etc. systematisch in der Datei erfasst werden.

Mit der Anti-Terror-Datei können alle Polizeien des Bundes und der Länder im vereinfachten Verfahren nicht gesicherte geheimdienstliche

Informationen online nutzen. Umgekehrt bekommen alle Geheimdienste hochsensible polizeiliche Verdachtsdaten.

Eine solche Vernetzung führt zu einer verstärkten Verzahnung von Polizei und Geheimdiensten und bedeutet letzten Endes die Aufhebung des verfassungsmäßigen Gebots der Trennung dieser Arten von Sicherheitsbehörden. Dabei ist das Trennungsgebot eine historisch bedeutsame Konsequenz aus den bitteren Erfahrungen mit der Gestapo in der Nazizeit, die sowohl geheimdienstlich als auch exekutiv vollziehend tätig war. Mit diesem Gebot sollte in der BRD eine unkontrollierbare und damit undemokratische Machtkonzentration der Sicherheitsapparate und eine neue politische Geheimpolizei verhindert werden. Die negativen Erfahrungen mit der Stasi der ehemaligen DDR, die Geheimdienst und -polizei in einem war, untermauern diese ursprüngliche Intention. Für ihren Beschluss zur Antiterrordatei erhielt die Innenministerkonferenz am 20. Oktober in Bielefeld den „BigBrotherAward“ 2006 in der Kategorie Politik. Dr. Rolf Gössner, Rechtsanwalt, Publizist und seit 2003 Präsident der Internationalen Liga für Menschenrechte führt in seiner Laudatio bei der Verleihung dazu aus: „Die Anti-Terror-Datei ist [...] auf dem Hintergrund der seit dem 11.09.2001 erlassenen Antiterror-Gesetze [...] zu sehen, mit denen Aufgaben und Befugnisse von Geheimdiensten und Polizei drastisch ausgeweitet wurden und die die Kontrolldichte in Staat und Gesellschaft beträchtlich erhöht haben. Sie ist auch im Zusammenhang

zu sehen mit dem geplanten ‚Terrorismusbekämpfungsergänzungsgesetz‘, das die Große Koalition jüngst in den Bundestag eingebracht hat und mit dem die befristeten Antiterror-Befugnisse von 2002 nicht nur um weitere fünf Jahre verlängert, sondern auch noch ausgeweitet werden sollen – ohne zuvor eine unabhängige, kritische Bilanzierung der bisherigen Antiterrorgesetze und ihrer Wirkungen vorzulegen.“



Datenkrake
[octopoda datae]

Sicherheitswahn ohne Ende? – „Wer sich nicht wehrt, lebt verkehrt!“

Gegen Sicherheitswahn und für Freiheit und insbesondere gegen die Vorratsdatenspeicherung der Telekommunikationsdaten Verkehrstenden engagiert sich der Arbeitskreis Vorratsdatenspeicherung (www.vorratsdatenspeicherung.de), der bereits vielfältige Aktionen gegen die Vorratsdatenspeicherung unternommen hat. Zuletzt die Demonstration in Bielefeld unter dem Motto „Freiheit statt Angst“. Viele der DemonstrationsteilnehmerInnen nahmen dann auch an der diesjährigen Verleihung der „BigBrotherAwards“ in Bielefeld teil. Diese vom FoeBuD e.V. (www.foebud.de) durchgeführte Veranstaltung weist auf die eklatantesten „Datenkraken“, wie die Datensammler genannt werden, hin.

Zu den ausgezeichneten „Datenkraken“ gehören dieses Jahr u.a. die Society for Worldwide Interbank Financial Telecommunication (SWIFT) und der Landtag von Mecklenburg-Vorpommern. SWIFT kopiert alle Überweisungsdaten auf die Computer des SWIFT-eigenen US-amerikanischen

Operation Center (SWIFT-USA) und ermöglicht somit unter Missachtung des Bankgeheimnisses den US-Behörden den Zugriff auf europäische Banküberweisungsdaten. Der Landtag von Mecklenburg-Vorpommern erhielt den „BigBrotherAward“ für die neuen Befugnissen im dortigen Polizeiaufgabengesetz, die es erlauben öffentliche Plätze, Gebäude, Einrichtungen und Verkehrsmittel nicht nur optisch, sondern auch akustisch zu überwachen: „Flirten, flüstern, tratschen, der Staat hört mit.“ Mit 500 BesucherInnen stieß die Gala anlässlich der Verleihung dieses Jahr auf ein so großes Interesse, wie nie zuvor. Es lohnt sich also für Freiheits- und Bürgerrechte einzutreten.

Von Werner Hülsmann

Zum Autor

Werner Hülsmann ist Vorstandsmitglied des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (Fiff) e.V. – www.fiff.de – und der Deutschen Vereinigung für Datenschutz (DVD) e.V. – www.datenschutzverein.de – sowie als selbständiger Datenschutzberater und externer Datenschutzbeauftragter (Datenschutzconsulting.eu) tätig.

Arbeitnehmerdatenschutz

Was lange währt, wird trotzdem nicht

Immer wieder wurde es von der Politik versprochen und von Datenschützern gefordert: das Arbeitnehmerdatenschutzgesetz.

Obwohl ein Entwurf bereits in einer Schublade der rotgrünen Regierung gelegen haben soll, ist das dringend erforderliche Arbeitnehmerdatenschutzgesetz mit der aktuellen Regierungskoalition wieder in weite Ferne gerückt. Trotz vielfältiger neuer technischer Herausforderungen durch Internet- und E-Mail-Nutzung, durch Einführung von RFIDs im Logistik-Bereich, bleiben die betrieblichen Datenschutzbeauftragten auf die Anwendung sehr allgemeiner Klauseln angewiesen.

Mitarbeiterdatenverarbeitung – nicht nur ein Thema in der Personalverwaltung

Wer Mitarbeiterdatenverarbeitung hört, denkt vermutlich in erster Linie an die Verarbeitung personenbezogener Daten in der Personalabteilung, an die klassische Personaldatenverarbeitung.

Dabei gibt es heute kaum noch Bereiche im Unternehmen, in denen keine mitarbeiterbezogenen Daten

verarbeitet werden. Neben der Personalverwaltung fallen Mitarbeiterdaten insbesondere noch in den folgenden Bereichen an:

- Nutzung von PC und Netzwerken
- Nutzung von Intranet, Internet und E-Mail
- Nutzung der Telefonanlage
- Zutrittskontrolle
- Betriebsdatenerfassung
- Warenwirtschaft
- Buchhaltung
- Schicht- und Projektplanung

Dem Autor wurde von einer Professorin für Datenschutz glaubhaft versichert, dass sie einen derartigen Entwurf tatsächlich in der Schublade eines Referenten der rotgrünen Bundesregierung gesehen habe!

Die rechtlichen Regelungen für diese Bereiche sind eher dürftig. Das Bundesdatenschutzgesetz (BDSG) erlaubt die Verarbeitung personenbezogener Daten nur, wenn

1. wenn und soweit das BDSG selbst dies erlaubt;
2. wenn eine andere Rechtsvorschrift dies vorschreibt oder erlaubt oder
3. wenn der bzw. die Betroffene wirksam eingewilligt hat

Die Einwilligung im Arbeitsverhältnis

Aus zwei Gründen ist die Einwilligung der Betroffenen für Datenverarbeitungen im Arbeitsverhältnis meist ungeeignet:

1. Die Einwilligung ist gemäß § 4a nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht und
2. Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Weder die automatisierte Zeiterfassung noch eine Nutzung der Logdateien der Internetnutzung zur Kontrolle, ob sich die MitarbeiterInnen an die Nutzungsregelungen halten lässt sich auf Grund der Einwilligungen der Betroffenen rechtssicher gestalten. Schließlich will der Arbeitgeber für diese und weitere Zwecke weder von der Einwilligung der MitarbeiterInnen abhängig sein noch für die MitarbeiterInnen, die nicht einwilligen oder ihre Einwilligung zurückziehen, auf eine manuelle Zeiterfassung umstellen.

Erlaubnisse durch andere Rechtsvorschrift

Ein Teil der Verarbeitung der Mitarbeiterdaten im Personalbereich ist durch gesetzliche Regelungen vorgeschrieben. So ist beispielsweise die Verarbeitung der Religionszugehörigkeit vorgeschrieben, wenn sie Durchführung des Kirchensteuerabzugs erforderlich ist. Auch die Verarbeitung oder Nutzung der Daten, deren für die Berechnung der Lohnsteuer und Sozialversicherungsabgaben erforderlich sind, ist zulässig.

Erlaubnisse im BDSG

Für die Verarbeitung personenbezogener Daten der MitarbeiterInnen sind im BDSG im § 28

Absatz 1 noch folgende anwendbare Regelungen enthalten:

„Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt,“

Durch die Ziffer 1 sind die Datenverarbeitungen zulässig, die für die Erfüllung des Arbeitsvertrags oder zur Durchführung des Bewerbungsverfahrens (vertragsähnlichen Vertrauensverhältnis) erforderlich sind. Aber nicht jede Datenverarbeitung im Arbeitsverhältnis fällt unter diese Regelung. So ist es im Allgemeinen zur Erfüllung des Arbeitsverhältnisses nicht erforderlich, dass von dienstlichen Telefonaten Einzelverbindungs-nachweise erstellt werden.

Gleiches gilt für viele weitere Bereiche, in denen personenbezogene Daten der MitarbeiterInnen verarbeitet werden. So reicht die Anwendung der Ziffer 1 nicht aus. Bei der Anwendung der Ziffer 2 ist eine Abwägung zwischen den berechtigten

Interessen der verantwortlichen Stelle, also dem Arbeitgeber und den schutzwürdigen Interessen der Betroffenen, also den Beschäftigten, durchzuführen. Nur wenn kein Grund zu Annahme besteht, dass die schutzwürdigen Interessen der Beschäftigten überwiegen, ist eine Verarbeitung personenbezogener Daten der MitarbeiterInnen auf Basis der Ziffer 2 dieser Regelung zulässig. Bei dieser Abwägung ist der betriebliche Datenschutzbeauftragten häufig auf sich alleine gestellt. Klare gesetzliche Vorgaben fehlen hier, so dass es – auch in der Abhängigkeit von der Fachkunde des betrieblichen Datenschutzbeauftragten, seiner Einstellung und Durchsetzungsfähigkeit – in den Unternehmen zu sehr unterschiedlichen Auslegungen kommt.

Der Betriebs- oder Personalrat und der Arbeitnehmerdatenschutz

Gibt es im Unternehmen oder der Behörde einen Betriebs- oder Personalrat der gemäß Betriebsverfassungsgesetz oder den Personalvertretungsgesetzen gewählt wurde, dann hat der betriebliche Datenschutzbeauftragte in Bezug auf den Arbeitnehmerdatenschutz einen Partner.

Kontrolle des Arbeitnehmerdatenschutzes

Zu den Aufgaben des Betriebs- oder Personalrates gehört es auch, die Einhaltung der Arbeitnehmerschutzgesetze zu überwachen. Das BDSG (bzw. die Landesdatenschutzgesetze für die öffentlichen

Einrichtungen der Länder und Kommunen) gehört nach höchstrichterlicher Rechtsprechung zu diesen Arbeitnehmerschutzgesetzen, soweit es um die Verarbeitung der Mitarbeiterdaten geht. D.h. konkret, dass es zu den Aufgaben des Betriebs- oder Personalrates gehört, die Einhaltung des Arbeitnehmerdatenschutzes zu überwachen. Hier bietet sich eine enge Zusammenarbeit zwischen betrieblichen Datenschutzbeauftragten und Betriebs- bzw. Personalrat an. Zwar sehen manche Arbeitgeber eine solche enge Zusammenarbeit nicht gerne, aber in den Firmen und Behörden, in denen die „vertrauensvolle Zusammenarbeit“ nicht nur eine Gesetzesfloskel ist, sondern sie gelebt wird, kann durch diese Zusammenarbeit eine effizientere Umsetzung des Arbeitnehmerdatenschutzes erreicht werden. So hat der Betriebs- oder Personalrat nicht nur die Aufgabe den Arbeitnehmerdatenschutz zu überwachen sondern im Gegensatz zum betrieblichen Datenschutzbeauftragten auch wirksame arbeitsrechtliche Mittel unzulässige Verarbeitungen personenbezogener Daten der MitarbeiterInnen zu unterbinden.

Arbeitnehmerdatenschutz und Mitbestimmung

In fast allen Bereichen, in denen personenbezogenen Daten der MitarbeiterInnen verarbeitet werden, bestehen für den Betriebs- oder Personalrat Mitbestimmungsrechte. So sind alle Systeme, die eine Leistungs- oder Verhaltenskontrolle ermöglichen ebenso mitbestimmungspflichtig.

Auch „Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer“ sind ebenso mitbestimmungspflichtig wie die Gestaltung von Personalfragebogen und die „Richtlinien über die personelle Auswahl bei Einstellungen, Versetzungen, Umgruppierungen und Kündigungen“. Dort wo der Betriebs- oder Personalrat Mitbestimmungsrechte hat, kann er gestaltend auf den Arbeitnehmerdatenschutz im jeweiligen Unternehmen, in der jeweiligen Behörde einwirken. In dem in einem Betrieb oder einer Behörde eine Betriebs- oder Dienstvereinbarung zwischen Arbeitgeber und Betriebs- bzw. Personalrat abgeschlossen wird, wird – sofern ausreichende und angemessene Regelungen zur Verarbeitung der Beschäftigtendaten enthalten sind – eine für diesen Betrieb, für diese Behörde geltende Rechtsgrundlage für die Verarbeitung der Mitarbeiterdaten geschaffen. Diese stellt „eine andere Rechtsvorschrift“ im Sinne des Eingangs erwähnten § 4 BDSG dar und stellen somit eine Erlaubnis für die Verarbeitung der Beschäftigtendaten dar. Durch entsprechende Gestaltung von Betriebs- und Dienstvereinbarungen lassen sich Regelungslücken oder die schwierigen Abwägungen der unterschiedlichen Interessen im Bereich des Arbeitnehmerdatenschutzes vermeiden.

Betrieb- und Personalräte und der Arbeitnehmerdatenschutz

Rechtlich und theoretisch kommt den Betriebs- und Personalräten eine wichtige Aufgabe und eine

große Verantwortung bei der Umsetzung des Arbeitnehmerdatenschutzes zu. Dies gilt umso mehr, solange es kein Arbeitnehmerdatenschutzgesetz gibt, das den rechtlichen Rahmen für die Verarbeitung personenbezogener Daten absteckt. Die neuen technischen Entwicklungen ermöglichen und bedingen teilweise immer stärker die Erfassung von Beschäftigtendaten in den unterschiedlichen Bereichen. Bei der Betriebsdatenerfassung geht es schon seit geraumer Zeit nicht nur um die Erfassung der Betriebsdaten einer Maschine. Vielmehr wird auch erfasst, wer sie wann wie lange bedient und wer sie wann wie lange wartet. Zutrittskontrollsysteme, die in sensiblen Bereichen des Unternehmens der Behörde unvermeidlich sind, dienen ja nicht nur der Verhinderung des Zutritts Unbefugter sondern sie speichern im Allgemeinen auch, wer wann welche Tür öffnet.

Videüberwachungseinrichtungen werden immer kleiner, leistungsfähiger und kostengünstiger. Ihr Einsatz ist völlig unbemerkt möglich. Durch die Digitaltechnik ist eine lange Aufzeichnungsdauer ebenso möglich wie die Nutzung von Software zur automatischen Gesichtserkennung. Die Nutzung von PC und firmeninternen Netzwerk wird ebenso protokolliert wie der Zugriff auf das Internet und die Nutzung von E-Mail.

Die Nutzung der RFID-Technik in der Logistik lässt weitere detaillierte Auswertungen zu. Eine Ausweitung auf Firmen- oder Behördenausweise bietet vielfältige Möglichkeiten der Überwachung der Beschäftigten.

Sicher gibt es berechnete Interessen der Arbeitgeber für bestimmte Nutzungen und Auswertungen – auch zur Leistungs- und Verhaltenskontrolle. Bei allen Anwendungen ist aber sicher zu stellen, dass die schutzwürdigen Interessen der MitarbeiterInnen nicht überwiegen und noch nicht mal ein Grund für die Annahme eines Überwiegens besteht. Hier sind Betriebs- und Personalräte gefordert – unter Ausnutzung ihrer rechtlichen Möglichkeiten der Mitbestimmung – regulierend einzugreifen. Dazu gehört beispielsweise, dass in einer Betriebsvereinbarung zur Gleitzeit nicht nur geregelt wird, wer welches Gleitzeitmodell nutzen darf, sondern auch, wer warum auf welche Daten und Auswertungen zugreifen darf, wie lange die einzelnen Komm- und Gehtzeiten sowie die Zeitsalden aufbewahrt werden. Um dieser Aufgabe gerecht zu werden, muss sich ein Betriebs- bzw. Personalrat nicht nur ausreichend Zeit nehmen, sondern es muss auch Mitglieder der Arbeitnehmervertretung geben, die sich mit dem Thema Arbeitnehmerdatenschutz hinreichend tief beschäftigt haben. In der Praxis ist leider festzustellen, dass Betriebs- und Personalräte sich häufig nicht genug Zeit für diese Themen nehmen, was teilweise auch nachvollziehbar ist. Reaktionen auf Umstrukturierungen und Stellenabbau sind – zumindest kurzfristig – erstmal wichtiger.

Fazit

Die Anforderungen an betriebliche Datenschutzbeauftragte sowie Betriebs- und Personalräte im Bereich Arbeitnehmerdatenschutz steigen stetig, auch durch die fortschreitende technische Entwicklung. Der Gesetzgeber lässt die Beteiligten –hierzu zählen auch die Arbeitgeber – mit der Thematik alleine, obwohl die Aufstellung gewisser Rahmenregelungen die Arbeit von betrieblichen Datenschutzbeauftragten auf der einen Seite und von Arbeitgeber und Arbeitnehmervertretungen auf der anderen Seite wesentlich erleichtern würde.

Betriebliche Datenschutzbeauftragte sind ebenso wie Betriebs- und Personalräte aufgefordert, sich intensiv mit dem Thema Arbeitnehmerdatenschutz zu beschäftigen und auch die erforderlichen Fort- und Weiterbildungen in diesem Bereich wahrzunehmen. Und den betrieblichen Datenschutzbeauftragten, Betriebs- und Personalräten, deren Zeit scheinbar nicht ausreicht, sei zugerufen: „Nehmt Euch die Zeit die Ihr braucht: Ihr seid zur Erfüllung Eurer Aufgaben ausreichend freizustellen. Nehmt die Verantwortung, die Ihr Euren Kolleginnen und Kollegen gegenüber habt, auch im Bereich Arbeitnehmerdatenschutz wahr.“

Von Werner Hülsmann

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)

Das FIfF will, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Deshalb

- warnt es die Öffentlichkeit vor Entwicklungen in der In Fachgebiet, die wir für schädlich halten;
- setzt es möglichen Gefahren eigene Vorstellungen entgegen;
- kämpft es gegen den Einsatz der Informationstechnik zur Kontrolle und Überwachung;
- engagiert es sich für eine Abrüstung der Informatik in militärischen Anwendungen;
- fördert es die Entwicklung von ökologisch verträglichen Wirtschaftskreisläufen mit Hilfe von Informationstechnik;
- unterstützt es die menschenrechte Gestaltung von Arbeitsprozessen;
- setzt es sich bei Gestaltung und Nutzung der Informationstechnik für die Gleichberechtigung von Menschen mit Behinderungen ein;
- arbeitet es gegen die Benachteiligung von Frauen in der Informatik;
- wehrt es sich gegen jegliche rassistische und sexistische Nutzung oder andere diskriminierende Nutzung der Informationstechnik;
- setzt der Vorherrschaft der Öko-

nomie eine humane und ökologische Orientierung entgegen.

Das FIfF hat etwa 800 Fachleute der Informatik und Informationstechnik, die bei ihrer Arbeit auch über deren soziale und gesellschaftliche Konsequenzen nachdenken. Sie wissen, dass nicht alle Probleme technisch lösbar sind. Es sind alle willkommen, die Informationstechnik verwenden oder sich Gedanken über ihre gesellschaftliche Rolle machen.

Das FIfF will allen, die sich mit Informatik und Informationstechnik beschäftigen – in der Ausbildung im Beruf oder danach, in Wissenschaft und Praxis – ein Forum für eine kritische und lebendige Auseinandersetzung bieten – offen für alle, die mitarbeiten möchten oder auch einfach nur informiert bleiben wollen.

Die Arbeit des FIfF wird vom Vorstand koordiniert. In wissenschaftlichen Fragen unterstützt uns der wissenschaftliche Beirat des FIfF. Das FIfF kooperiert mit zahlreichen in- und ausländischen Initiativen und Organisationen, wie zum Beispiel der Deutschen Vereinigung für Datenschutz (DVD) e.V., dem FoeBuD e.V. und European Digital Rights (EDRI) und beteiligt sich auch an der jährlichen Verleihung der BigBrotherAwards.

In zahlreichen Veröffentlichungen dokumentiert das FIfF seine Arbeit. Die kritische Computerzeitung FIfF-Kommunikation erscheint vierteljährlich.

Aktuelle Informationen und Diskussionen gibt es in der FIfF-Mailing-Liste. Weitere Informationen: <http://www.fiff.de> oder E-Mail: fiff@fiff.de

Anonym im Netz – eine kleine Einführung

Seit dem die Diskussion um die zunehmende Überwachung des Internet mittlerweile auch die Mehrheit der Massenmedien und damit auch die Bevölkerung erreicht hat, stellt sich die berechtigte Frage nach dem im Grundgesetz verankertem Grundrecht auf informationelle Selbstbestimmung [1] im Internet. Wie du das Internet auch anonym nutzen kannst, will ich dir hier mit kostenloser Software vorstellen.

Deine Daten im Internet

Darüber welche Daten du über dich im Internet preisgibst, kannst du nur bedingt entscheiden. Klar wenn du deine Anschrift oder deine Mailadresse bei der Bestellung eines neuen Notebooks bei einem der unzähligen Online-Shops angibst, dann entscheidest du selbst darüber, wer welche Daten von dir bekommt. Vielen Internetnutzer_innen ist jedoch nicht bewußt, dass weitaus mehr Datenspuren durch das bloße Surfen im Internet unverschlüsselt übertragen werden. Das beginnt mit der Version des verwendeten Internet-Browsers, der Betriebssystem-Version und endet

letztlich mit einer globalen eindeutigen IP-Adresse. Wer sich ein wenig mehr für die Funktionsweise des Internet interessiert, dem sei eine gut gemachte Folge von „Sendung mit der Maus“ [2] empfohlen.

Deine IP-Adresse ist im übertragenden Sinne deine Anschrift im Internet, an die die angeforderten Daten, zum Beispiel eine Webseite, geschickt werden. Damit die Daten auch an die Richtige Adresse geschickt werden können, sind IP-Adressen immer eindeutig und weltweit einmalig. In Verbindung mit Uhrzeit und Datum stellen sie somit personifizierbare Daten da. Dein Internet-Service-Provider (ISP), der dir deine DSL-Flatrate (oder auch jegliche andere Internetanbindung) verkauft, kann mit diesen Daten die verwendete IP-Adresse eindeutig auf deinen Telefonanschluss zurückführen. Die Nutzung des Internet ist somit alles andere als anonym. Aber nicht nur dein ISP kann die Daten verwenden, auch die Gegenseite der Kommunikation (zum Beispiel beim Aufruf einer Homepage) kann diese Daten automatisiert speichern und für ihre Zwecke auswerten. Ohne dass du als Nutzer_in etwas hiervon mitbekommst.

Grund genug sich hierüber einmal fünf Minuten Gedanken zu machen. Um dein Grundrecht auf informationelle Selbstbestimmung zumindest beim bloßen Surfen im Internet zu sichern, werde ich dir in diesem Bericht erläutern, wie du die notwendige (OpenSource) Software installieren und nutzen kannst.

Software für mehr Anonymität im Internet

Als Grundlage für die anonyme Nutzung des Internets wird dir die Software „Twisted Onion Routing“ TOR [3] zur Seite stehen. Normalerweise erfolgt die Kommunikation im Internet unverschlüsselt und direkt zwischen den Kommunikationspartnern. Und genau an diesem Punkt wird TOR zwischen geschaltet. Um dich nun nicht unnötig mit technischen Details zu verwirren, werden ich nicht auf die konkrete Funktionsweise von TOR eingehen. Wenn du mehr hierüber erfahren möchtest, dann kannst du dich auf der Homepage zum TOR-Projekt [4] informieren. Die wichtigsten Fakten sind, dass die Kommunikation verschlüsselt wird und nicht mehr direkt, sondern über mehrere TOR-Knoten und somit anonym abläuft. Weder der Endpunkt der Kommunikation, noch einer der TOR-Knoten, kann den vollständigen Weg der Kommunikation rückverfolgen.

Installation von TOR

Aber kommen wir zur Installation von TOR auf einem Windows-PC. TOR kannst du kostenlos unter [5] herunterladen. Genaugenommen besteht das heruntergeladenen Programme aus mehreren einzelnen Programmen - TOR, Privoxy und Vidalia – die aber direkt zusammen benötigt und installiert werden. Zusätzlich empfehle ich die Nutzung von Firefox [6] als Webbrowser, weil dieser recht einfach für die Nutzung mit TOR eingerichtet werden kann.

Ich gehe daher im Weiteren davon aus, dass du mit Firefox arbeitest.

Nach dem Download, startest du die Installation von TOR durch einen Doppelklick auf die heruntergeladene Datei. Die beiden folgenden Anzeigen bestätigst du einfach mit einem Mausklick „NEXT“, die vorgefertigten Einstellungen kannst du ruhig so belassen. Nach Beendigung des Installationsvorganges ist auch schon fast alles geschafft und du müsstest eine kleine Zwiebel in der Windows-Task-Leiste (unten rechts) finden. So einfach kann die anonyme Nutzung des Internets sein. :-)

Nun musst du noch den Firefox-Browser zur Nutzung von TOR vorbereiten. Auch dies geht ebenso einfach. Unter [7] kannst du dir eine Erweiterung für deinen Browser installieren. Nach Aufruf der Seite musst du einfach auf „Install now“ klicken und die Erweiterung installiert sich auf deinem Rechner. Nun musst du den Browser einmal vollständig beenden und neu starten. Nach dem Neustart des Browsers findest du am unteren Rand des Browsers einen neuen Button.

Nun können wir uns daran machen, das erste mal anonym mit TOR im Internet zu surfen. Mit einem Rechtsklick auf die Zwiebel in der Windows-Task-Leiste und der Auswahl von Start wird TOR gestartet [Bild 4]. Nun kannst du im Browser mit einem Klick auf den neuen TOR-Button auf „Tor enabled“ Firefox für die Nutzung von TOR einstellen. Ab jetzt bist du mit einer Tarnkappe im Netz unterwegs.

Um zu testen ob alles funktioniert hat, kannst du die Seite [8] aufrufen. Wenn dich nun eine grüne Schrift begrüßt hat alles geklappt. Ansonsten lies doch bitte die Anleitung nochmal durch und schau ob du auch alle Schritte durchgeführt hast.

Wenn Probleme auftreten ...

Ist die Zwiebel in der Windows-Task-Leiste grün? Ansonsten musst du mit einem Klick der rechten Maustaste TOR starten. Findest du auch einen grünen/ oder blauen Kreis ebenfalls in der Task-Leiste? Wenn nicht, dann musst du Privoxy über den Start-Button -> Alle Programme -> Privoxy starten.

Ich wünsche dir viel Spaß mit deinem zurückeroberten Grundrecht auf informationelle Selbstbestimmung.

- [1] <http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm>
- [2] http://stat.wdr.de/cgi-bin/wdr/RD/www.wdr-maus.de/service/download/dateien/vid_www.zip
- [3] <http://tor.eff.org/>
- [4] <http://tor.eff.org/overview.html.de>
- [5] <http://tor.eff.org/download.html.de>
- [6] <http://www.firefox-browser.de/windows.php>
- [7] <https://addons.mozilla.org/firefox/2275/>
- [8] <http://lefkada.eecs.harvard.edu/cgi-bin/ipaddr.pl?tor=1>

Wer die Kontrolle hat, dem gehört die Zukunft!

Versuch einer Reflektion über den Wunsch hinter der Überwachung in fünf Textskizzen und einer kurzen These.

1.

Nacht. Schwarz. Nur der Vollmond leuchtet hell in die Dunkelheit. Eine Frau sitzt auf einem Stuhl, neben ihr steht ein Mann. Er hält mit seinem Daumen und Zeigefinger die Lider ihres linken Auges auf. Eine schmale Wolke durchschneidet den Mond, genauso wie der Mann mit einem Rasiermesser das Auge der Frau durchteilt.

1929 drehte Luis Buñuel zusammen mit Salvador Dalí den Film ‚Un Chien Andalou – Ein andalusischer Hund‘. Die Sequenz des Augenschnittes ist berühmt, der Film ist ein Meisterwerk des Surrealismus. Das Auge ist ein immer wiederkehrendes Motiv in der Kulturgeschichte der Menschheit. Es ist lichtchenkendes Sinnesorgan, es ist ein Spiegel der Seele, des Lebendigen vom Menschen. Das schöpferische Auge ist eine Gabe der Künstler. Das göttliche Auge ist ein Zeichen für den omnipräsenten Blick auf die Menschheit. Nur dieses Sinnesorgan

lässt uns eine klare Orientierung im dreidimensionalen Raum finden. Es schafft Grenzen in Linien und Formen und dadurch Ordnung und Ruhe in unserer Wahrnehmung. Was wir durch unser Auge wahrnehmen, halten wir für wahr. Selbst unser Intellekt findet seine Erkenntnis, indem wir etwas erkennen.

Wahrheit und Erkenntnis, Ordnung und Grenzen. Unser Blick auf die Welt ist ein Blick von Innen nach Aussen.

Was passiert, wenn dieser Blick nun verkehrt wird? Das Auge soll biometrisch erfasst werden. Eine Iris-Scanner Kamera schaut in uns hinein. Der Kunstwissenschaftler Martin Henatsch schreibt in seiner Einführung zu der von ihm im Jahr 2004 kuratierten Ausstellung ‚Firewall‘ : „Der Schnitt durch das Auge (der schematische Schnitt des scannenden Lichtstrahls, d. Verf.), ein Organ, das traditionell einen außerordentlich hohen Rang auf der Skala des Schreckens, des Gewissens, der Macht einnimmt, ist erneut zum zentralen Sinnbild für die Veränderung von Wahrnehmungsgewohnheiten erklärt.“ Henatsch erläutert weiter, dass zwar das Auge und damit der Mensch nicht physisch verletzt wird wie bei Buñuel, aber dennoch jetzt seine Identität als Mensch in Frage gestellt wird.

Der Blick der biometrischen Kamera in unsere Augen ist nicht nur ein technischer, sondern vor allem ein psychologischer Blick, der sagt: Ich kann Dich sehen. Ich kann in Dich hineinschauen. Ich weiß, wer Du bist. Ich weiß alles über Dich.

2.

Den Menschen Gleichgültigkeit zu lehren ist ein Mittel um sie zu kontrollieren.

Der in New York lebende Künstler Alfredo Jaar installierte im Jahr 2002 auf der Documenta XI drei leuchtende weiße Texttafeln nebeneinander in einem fast komplett abgedunkelten Raum. Seine Arbeit trug den Namen ‚Lament of images – Klage der Bilder‘.

Der linke Text handelte von dem Moment, als Nelson Mandela, die Gallionsfigur des Kampfes gegen das Apartheid-Systems Südafrikas, nach über 25 Jahren Isolationshaft aus dem Gefängnis entlassen wurde. Jaar beschrieb, wie die Kameras den von zu langer Dunkelheit blinzelnden Mandela in Empfang nehmen.

Der Text in der Mitte der Installation beschäftigte sich mit dem Aufkauf eines der größten Fotobildarchive der Welt durch den Microsoft-Gründer Bill Gates und seiner Verbringung in ein unterirdisches, hermetisch abgeriegeltes Lager. Daraus ergab sich, dass ein Teil des visuellen Gedächtnisses der Menschheit privatisiert und unzugänglich gemacht wurde.

Der an der rechten Seite montierte Text informiert schließlich über den Aufkauf sämtlicher privater Satelliten-Bilder von Afghanistan während der Angriffe der USA gegen das Taliban-Regime. Und das obwohl die eigenen militärischen Satelliten zehnmal so genau fotografieren konnten. Unabhängige Beobachtungen von aussen über Art und die Folgen des Krieges und der in ihm eingesetzten

Waffen der US-Armee waren nicht mehr möglich. Die Macht über alle Bilder war somit die Macht über die Wahrheit.

Alfredo Jaar: „Das Werk ist eine Metapher der Blindheit in unserer Gesellschaft. Ich denke, wir leben heute in einem großen Paradox. Einerseits werden wir von tausenden Bildern bombardiert, aber andererseits waren diese nie zuvor so kontrolliert, sei es durch die Regierungen oder durch einen gewissen Teil des privaten Sektors. Deswegen glaube ich, dass wir die Fähigkeit, zu sehen und von Bildern ergriffen zu werden, verloren haben. Nichts mehr bewegt uns, nichts mehr hat einen Sinn.“

Nach dem Lesen der auf der schwarzen Wand leuchtenden Texte gingen die Besucher durch einen dunklen, labyrinthartigen Gang und wurden im nächsten Raum von gleißend hellem Licht geblendet.

3.

Der in diesem Jahr verstorbene Schriftsteller Stanislav Lem schrieb 1961 ein Buch mit dem Titel ‚Memoiren – Gefunden in der Badewanne‘.

„Memoiren, gefunden in der Badewanne ist eine satirische Farce, eine surrealistische Anti-Utopie und eine Schmähschrift auf die absolute Bürokratie und den totalen Polizeistaat, in dem alles und jeder gelenkt, einem geheimen Zweck untergeordnet und von Spitzeln überwacht wird. Das ‚Gebäude‘, eine Spionagezentrale, ist ‚unbesiegbar‘;

im Verlauf seiner Entwicklung ständig gewachsen, steht es im unaufhörlichen Kampf mit einem AntGebäude, einer gegnerischen Spionagezentrale, die es durchdrungen hat und von der es ebenso durchdrungen worden ist. Ob es die beiden »Gebäude« wirklich gibt oder ob der Widerstreit bloß eine gedankliche Konstruktion ist, das weiß kein Mensch mehr so genau. Auf jeden Fall sind Chaos und Ordnung, Zufall und Notwendigkeit, Sinn und Unsinn nicht zu unterscheiden - Memoiren, gefunden in der Badewanne: ein Zukunftsalptraum.“

In Lems Erzählung erfährt der Leser von einem Historiker, dass es eine globale Katastrophe in der Menschheitsgeschichte gab, durch die alles Papier und damit alle bisher erfassten Daten vernichtet worden sind. Eine Konstruktion des Autors als Voraussetzung für den schon untergegangenen totalitären Staat, den Lem durch Historiker erforschen lässt.

Zurück in ‚unserer Zeit‘ führen die immer weiter ausgebauten Überwachungssysteme zu enormen Datenmengen. Fast alles wird heutzutage digital erfasst. Die zunehmende Technisierung der Gesellschaft bringt ein Paradox mit sich. Um die Daten zu sichern und zu kontrollieren, braucht es weitere Systeme oder wie Soziologe David Lyon sagt, produzieren „mehr Systeme mehr Unsicherheiten, die

die Notwendigkeiten für mehr Systeme schaffen“. Vielleicht ist der Alptraum von Stanislaw Lem dann gar nicht mehr so unreal. Was passiert, wenn ein sinflutartiger Verlust aller digitalen Daten stattfinden würde? Der Tod unserer digitalen Identitäten? Reale Historiker verweisen immer wieder auf die

Geschichte antiker Städte wie Babylon und Niniveh und ihrem Untergang, obwohl oder gerade, weil es sich um abgekapselte Kulturen handelte, die sich gegen An-

griffe von außen durch Mauern und auf Maschinen basierende Sicherheitssysteme schützen wollten. Das trojanische Pferd zumindest hat es schon als Begriff für eine Art Spionage-Software in das Digitale Zeitalter geschafft.

4.

„So geheimnisvoll Software-Codes auch aussehen mögen, sie sind niemals neutral, niemals unschuldig. In ihnen zeichnen sich die Wünsche und Ziele derer ab, die die Systeme entworfen (...) haben.“

Biometrische Überwachungssysteme sind Maschinen, die automatisiert Entscheidungen treffen. Die Ergebnisse dieser Entscheidungen sehen immer ganz einfach aus. Sie lauten entweder Ja oder Nein, sind Positiv oder Negativ. Hat ein System ausreichend Informationen erhalten und abgeglichen, ist also eine bestimmte Schwelle überschritten, dann fällt diese Entscheidung. Je nachdem, wo die Schwelle liegt, also wie empfindlich das

Kontrolle ist gut,
Vertrauen ist menschlicher.
Dr. phil. Gerald Dunkl

System eingestellt ist, reagiert es. Biometrische Erkennungssysteme arbeiten mit Wahrscheinlichkeiten und können nie eine hundertprozentige Sicherheit bieten.

Selbst bei einer unrealistischen Trefferquote von 90 % wäre jede 10. Entscheidung ein Fehler, ein Fehlalarm. Jeder 10. Mensch würde falsch eingestuft.

„So wäre es ein ‚falsches Negativergebnis‘, wenn ‚der Terrorist an der Kontrolle nicht erkannt würde, aber ein ‚falsches Positivergebnis‘, wenn der unbescholtene Bürger in Verdacht geriete. Das Dilemma besteht darin, daß Testverfahren nicht in beiderlei Richtung gleichzeitig optimiert werden können, so daß sie einerseits möglichst jeden Verdächtigen erfassen, andererseits aber praktisch nie falschen Alarm auslösen würden.“

Was passiert nun aber, wenn jemand falsch eingestuft würde? Wem wird mehr geglaubt? Der Technik?

Die neuen Technologien führen vielleicht zu einem Verlust der eigenen, erfahrbaren Realität und schaffen hingegen mediale Wahrheiten. Ein virtuelles Richtig und Falsch, ein technologisches Gut und Böse. Das digitale Denken ist binär, ist 0 oder 1, ein Dazwischen gibt es nicht.

5.

Warum werden weltweit immer mehr Überwachungssysteme installiert, miteinander vernetzt, in den privaten Raum übertragen, wenn diese doch kaum zur Sicherheit beitragen, wenn die riesigen

Datenmengen gar nicht ausgewertet werden können und wenn die Systeme doch so ‚fehlerhaft‘ bleiben? Eine paradoxe Antwort könnte sein, dass die Überwachung der Gesellschaft gar nicht das primäre Ziel ist, sondern ein Instrument der ‚Überwacher‘ um damit eine soziale und eine psychologische Kontrolle auszuüben. Ziel derjenigen, die diese Techniken verantworten, ist nicht zu überwachen, sondern zu zeigen, dass sie überwachen.

David Lyon schreibt darüber: „Überwachung muss heute immer auch als Prozess sozialer Auslese verstanden werden, welcher vor allem ausschließende Konsequenzen beinhaltet. (...) In der Tat erlaubt es die automatische Überwachung, Distanz zwischen Privilegierten und Armen zu halten.“

Überwachung hat eine psychologische Funktion. Wer weiß, dass er überwacht wird, der versucht sich ‚normal‘ zu verhalten und nicht aufzufallen. Der gläserne Bürger ist ein normierter Bürger und der lässt sich steuern. Kreativität, Ideen und Gedanken, die geistige Freiheit des Menschen, werden durch seine Kontrolle eingeschränkt. Sein Handeln wird voraussehbar. Das Erschreckende dabei ist doch, dass für die Lenkung einer Gesellschaft heutzutage kein totalitäres System mehr notwendig ist. Es reicht einzig und allein, die Macht über die Daten zu besitzen.

Vielleicht steckt hinter dem Wahn der Überwachung von Menschen durch Staat und privater Hand ein alter Menschheitstraum. Der Traum von

dem Blick in die Zukunft und die Möglichkeit, diese zu beeinflussen. Doch das Resultat ist wohl ein einziger Alptraum. Wer die Kontrolle hat, dem gehört dann die Zukunft. Und wem die Zukunft gehört, dem gehört die Welt.

Jan Andreas Enste

Jan Andreas Enste ist AStA-Vorsitzender der Kunstakademie Münster. Im Jahr 2005 organisierte er ‚Befreit die Freiheit‘, einen Vortragsmarathon in der Kunstakademie Münster über die gesellschaftlichen Auswirkungen von Überwachung.

Wichtige Quellen:

Surveillance-Studies – ist eine Initiative, die sich der Vernetzung von Forschung zu Überwachung widmet.

www.surveillance-studies.org

Initiative Nachrichtenaufklärung – Ziel der Initiative Nachrichtenaufklärung ist es, wichtige Nachrichten und Themen, die in den Medien nicht genügend berücksichtigt wurden, stärker in das Bewusstsein der Öffentlichkeit zu bringen.

www.nachrichtenaufklaerung.de



Die Deutsche Vereinigung für Datenschutz

Wer sind wir? Was machen wir?

Die DVD sieht ihre Aufgabe weniger darin, Datenskandale aufzudecken, sondern vorrangig darin, die Bevölkerung über Gefahren des Einsatzes elektronischer Datenverarbeitung und der möglichen Einschränkung des Rechts auf informationelle Selbstbestimmung zu beraten und aufzuklären.

Inhaltlich beschäftigen wir uns mit so unterschiedlichen Fragestellungen wie dem Datenschutz in Polizei und Justiz, dem Arbeitnehmerdatenschutz, Verbraucherschutz und Datenschutz im Internet – um nur einige zu nennen. Dabei sollen durch verschiedene Aktivitäten unterschiedliche Personengruppen erreicht werden, u.a. durch

- Öffentlichkeits- und Medienarbeit zu aktuellen Themen, Pressekonferenzen und Presseerklärungen
- Herausgabe der Datenschutz-Nachrichten (DANA)
- Teilnahme an Expertenanhörungen in Parlamenten zu allgemeinen und bereichsspezifischen Datenschutzgesetzen in Bund und Ländern
- Teilnahme an öffentlichen Veranstaltungen und Diskussionen
- Durchführung von Tagungen in Zusammenarbeit mit Partnerorganisationen
- Mitarbeit bei der Verleihung der jährlichen Big Brother Awards
- Durchführung von Seminaren, wie z. B. für Betriebs- und Personalräte
- Vermittlung von Referenten zu aktuellen Themen des Datenschutzes
- Zusammenarbeit mit Partnerorganisationen wie Fiff, FoeBud, HU u.a.

Bonner Talweg 33 - 35
53 113 Bonn
Telefon: 0228/ 222 498
Telefax: 0228/ 243 847 0
dvd@datenschutzverein.de
www.datenschutzverein.de

Impressum

2007

Redaktion Altan Ari
V.i.S.d.P. Rabea Duscha
Layout Lena Schall
Illustrationen Johannes Munding
Lena Schall
Druck Druckerei Buschmann
Auflage 1000 Stück

„Wer die Freiheit einschränkt,
um Sicherheit zu gewinnen,
wird am Ende beides verlieren.“
(Benjamin Franklin, 1706..1790)