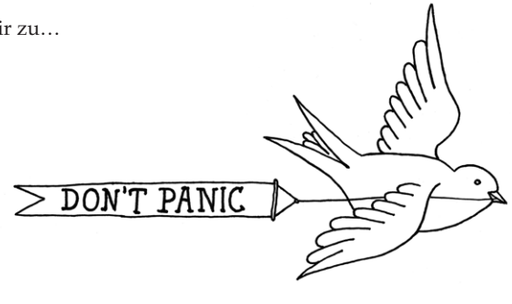
Ein Reader über den Datenschutz,
die Informationelle Selbstbestimmung
und den ganzen Rest

Inhalt



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 Information 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 Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.«

In der soeben zitierten Passage aus dem Volkszählungsurteil des Bundesverfassungsgericht von 1983, auf das sich DatenschützerInnen und BürgerrechtlerInnen immer wieder beziehen, wird sehr anschaulich geschildert warum die Informationelle Selbstbestimmung der Menschen grundlegend für eine demokratische Gesellschaft ist.

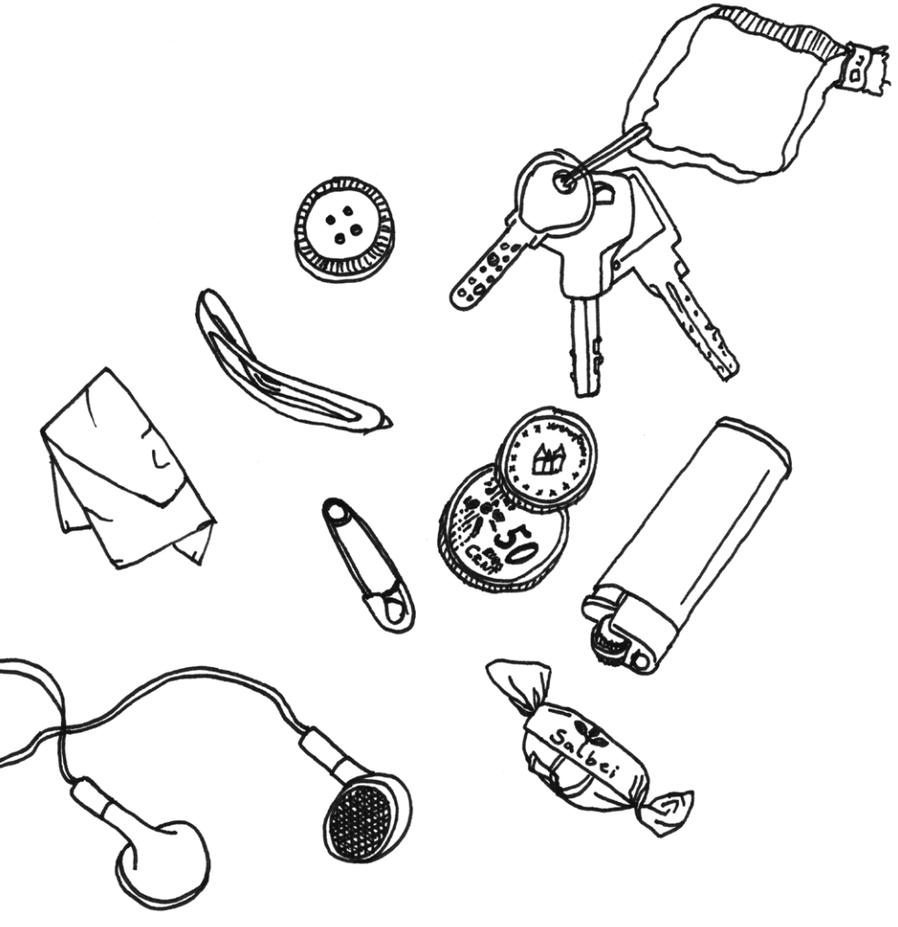
In den letzten Jahren wurden demokratische Grundrechte massiv eingeschränkt, Gesetze wurden unter dem Vorwand der »Terrorbekämpfung« verschärft und die Möglichkeiten, Bürgerinnen und Bürger zu überwachen wurden extrem ausgeweitet. Vorratsdatenspeicherung, Kameraüberwachung, elektronische Ausweise und Krankenkassenkarten (…) können einen gläsernen Menschen erzeugen.

Gleichzeitig schleudern viele Menschen ihre Daten durch die weite Welt des World Wide Web. Internetcommunities wie Myspace, Facebook oder StudiVZ haben einen erheblichen Zulauf, ohne dass sich die Mehrzahl der NutzerInnen über den Schutz ihrer Daten Gedanken macht oder sich der Gefahr, ihr gesamtes Privatleben im Internet offen zu legen, bewusst ist. Diese Themen werden in den verschiedenen Artikeln beleuchtet. Zudem gibt es Tipps und Tricks wie ihr eure Daten schützen könnt.

Mit »Don't Panic – über den Datenschutz, die Informationelle Selbstbestimmung und den ganzen Rest« haltet ihr den dritten Reader zum Themenfeld Datenschutz in den Händen, der vom AStA der Fachhochschule Münster herausgegeben wurde. Wir danken allen Autorinnen und Autoren für ihre Artikel, dem AK Vorratsdatenspeicherung Münster für die gelungene Zusammenarbeit, der Referentin für IT und Datenschutz, vom AStA der Universität Münster, Katharina Maria Nocun für ihre Unterstützung und Luise von Grebe für die Gestaltung.

Euer AStA der FH Münster im Herbst 2009

Ich habe doch nichts zu verbergen



Diesen Satz hat jedeR von uns schon so oder in einer seiner zahlreichen Varianten gehört und vielleicht auch gesagt – sei es im Freundeskreis, im Fernsehen oder in politischen Diskussionen. Eine einfache und klare Aussage, die leicht von den Lippen geht und kaum noch Aufmerksamkeit erzeugt, mit der sich ein Mensch anderen Menschen gegenüber als offen und unverdächtig präsentiert.

Angesichts der Debatten um den fortschreitenden Ausbau der Überwachungspolitik im Namen der inneren Sicherheit und des zunehmenden Interesses der privaten Wirtschaft an Details aus unserem alltäglichen Leben ist diese Aussage jedoch eines der am häufigsten verwendeten Argumente gegen datenschutzrechtliche Bedenken geworden.

Persönliche Aussage oder doch politisches Argument?

Flächendeckende Überwachungsmaßnahmen wie die Vorratsdatenspeicherung oder die Rasterfahndung werden damit gerechtfertigt: wer nichts zu verbergen hat, hat schließlich auch nichts zu befürchten. Gleichzeitig werden damit KritikerInnen dieser Maßnahmen in die Defensive gedrängt, da ihnen implizit unterstellt wird, sich vor negativen strafrechtlichen oder gesellschaftlichen Konsequenzen schützen zu wollen – wer dagegen ist, hat auch etwas zu verbergen. Die Weitergabe persönlicher Daten an Dritte wird mit ihr relativiert – was mein Lieblingsfilm oder meine Lieblingsband ist kann, ja soll vielleicht sogar, jedeR wissen, in der Hinsicht habe ich nichts zu verbergen.

Auf dieser Basis Diskussionen zu führen ist schwierig und endet leider häufig mit wenig konstruktiven, unsachlichen und überspitzten Attacken – wer nichts zu verbergen hat, kann ja auch gleich nackt rumlaufen.

Wer flüstert lügt?

Dabei lohnt es sich durchaus, die Aussage eingehender zu betrachten, da sie viel weitreichender ist, als es auf den ersten Blick erscheint. Eng verbunden mit der Aussage ist die Annahme, dass verdächtiges Verhalten mit Heimlichkeit einhergeht. Diese begleitet uns von frühester Kindheit an und hat eine sehr hohe Akzeptanz in unserer Gesellschaft – wer flüstert lügt. In bestimmten Fällen ist diese Annahme durchaus zutreffend, jedoch stehen ihr im alltäglichen Leben mindestens ebensoviele Gegenbeispiele gegenüber. So würden vermutlich nur wenige Menschen freiwillig gegenüber den Nachbarn auf ihr Briefgeheimnis verzichten. Eine Pauschalisierung ist hier demnach nicht so einfach möglich.

Dennoch hält sich die Assoziation von Heimlichkeit und kriminellem Verhalten hartnäckig.

Dennoch hält sich die Assoziation von Heimlichkeit und kriminellem Verhalten hartnäckig. Auch die oftmals von PolitikerInnen eingebrachte Verschärfung der Aussage, Datenschutz sei TäterInnenschutz, beruht auf dieser Verknüpfung. So würde schließlich eine effektive Strafverfolgung und präventive Strafvereitelung erschwert oder sogar gänzlich verhindert. In diesem Zusammenhang sei darauf hingewiesen, dass das geltende Rechtssystem in der Mehrheit der Situationen die Grundrechte eines einer Straftat verdächtigten Menschen gegenüber der möglichen Aufklärung einer Straftat als höheres Gut einstuft. Wer bereits den Datenschutz als TäterInnenschutz be-

greift, kann rechtsstaatlichen Prinzipien wie dem Recht auf eine AnwältIn oder auf Aussageverweigerung eigentlich nicht positiv gegenüberstehen.

Generell richtig, aber was geht mich das an?

Die Gleichgültigkeit vieler Menschen gegenüber aus Sicht von DatenschützerInnen kritischen Eingriffen in private Lebensbereiche ist jedoch mit der obigen Argumentation nicht zu erklären. Ein aktueller Ansatz findet sich bei Daniel J. Solove[1] und Sandro Gaycken[2]. Demzufolge neigen viele Menschen bei der Beurteilung von Eingriffen in ihre Privatsphäre dazu, die (möglichen) Konsequenzen in einem zu kleinen Rahmen zu betrachten. So wird häufig vergessen, dass heute erhobene Daten zeitlich unbegrenzt gespeichert werden können und eine spätere Löschung angesichts ihrer gegebenenfalls nicht transparenten Weitergabe in dezentralen Organisationsformen und Netzwerken schwierig ist – »das Internet vergisst nicht«[3]. Die zukünftige Verwendung der Daten und die damit verbundenen Konsequenzen sind also nicht absehbar. Alte, »längst vergessene« Fotos aus sozialen Netzwerken wie StudiVZ oder MySpace können in der Arbeitswelt und im Privatleben später unvorhergesehene Brisanz entwickeln.

Zudem sollten neben den Konsequenzen für sich selbst auch die möglichen Folgen für die Mitmenschen betrachtet werden, bevor Eingriffe als unbedenklich bewertet werden. Die Akzeptanz der Sammlung von Daten zu einem bestimmten Thema ist gleichbedeutend mit der Akzeptanz der gesamtgesellschaftlichen Auswirkungen dieses Eingriffs in die Privatsphäre. Für die Mehrheit der Menschen in einer Gesellschaft harmlos erscheinende Angaben können für Minderheiten schwerwiegende Folgen haben. Ein Beispiel dafür sind die an deutschen Hochschulen eingeführten verpflichtenden Befragungen für ausländische Studierende, die sogenannten Gesinnungstests. Eine Frage nach der eigenen Religionszugehörigkeit hat für Menschen muslimischen Glaubens derzeit sicherlich andere Konsequenzen als für Angehörige christlichen Glaubens, obwohl dafür keine Begründung, geschweige denn eine Rechtsgrundlage besteht.

In einigen Fällen ist ein effektiver Schutz der Privatsphäre auch nur in einer sich homogen verhaltenden Gruppe möglich. Nehmen große Teile der Gruppe die Möglichkeit zum Schutz ihrer Privatsphäre nicht wahr, fallen genau die Menschen auf, die ihr Recht auf den Schutz der eigenen Privatsphäre aktiv umsetzen. Eine unberechtigte Verdächtigung wird dann wahrscheinlich, wohingegen eine solidarische Ablehnung der Eingriffe meist ohne Konsequenzen für die UnterstützerInnen bleibt.

Nehmen große Teile der Gruppe die Möglichkeit zum Schutz ihrer Privatsphäre nicht wahr, fallen genau die Menschen auf, die ihr Recht auf den Schutz der eigenen Privatsphäre aktiv umsetzen.

Und nun?

So einfach und klar die Aussage »Ich habe nichts zu verbergen« anfangs erscheint, ist sie nach eingehender Betrachtung – wie so viele alltägliche Ansichten – doch weitaus tiefgehender und komplexer. Sich diese Bedeutung immer wieder klar zu machen oder gar ein Bewusstsein für diese weitreichenden Zusammenhänge zu schaffen scheint schwierig. Um eine konstruktive Auseinandersetzung mit alltäglichen Eingriffen in unsere Privatsphäre möglich zu machen ist es jedoch notwendig. Die gute Nachricht ist: Es ist einfach, damit anzufangen. Mit der Aussage: »Natürlich habe ich etwas zu verbergen.« Keine Angst – was das genau ist braucht Mensch auf Basis dieser Aussage dann nun wirklich nicht erklären.

durito, AK-Vorrat Münster

1 Daniel J. Solove, »I've Got Nothing to Hide« and Other Misunderstandings of Privacy, San Diego Law Review, Vol. 44, p. 745, 2007, papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

2 Sandro Gaycken, Opening of the 25C3 25th Chaos Communication Congress – Nothing to hide, events.ccc.de/congress/2008/

3 Dr. Dres. h.c. Hans-Jürgen Papier, Festvortrag zur Veranstaltung aus Anlass des 25. Jahrestages der Verkündung des Volkszählungsurteils des Bundesverfassungsgerichts am 15. Dezember 2008 in Karlsruhe www.sueddeutsche.de/computer/895/451606/text/

Videoüberwachung
Eine Frage der Akzeptanz?

Die polizeiliche Videoüberwachung öffentlicher Plätze ist nicht das erhoffte Wundermittel zur Bekämpfung von Kriminalität. Zu diesem Ergebnis kommt der Autor dieses Artikels, Florian Glatzner, in seiner Magisterarbeit »Die staatliche Videoüberwachung des öffentlichen Raumes als Instrument der Kriminalitätsbekämpfung – Spielräume und Grenzen«. Auch die Autoren früherer Artikel für die Broschüren des AStA »Achtung, diese Hochschule wird videoüberwacht« und »What the fuck is Informationelle Selbstbestimmung« formulierten ähnliche Schlussfolgerungen.

Dieser Artikel soll auf diesen Ergebnissen aufbauen und die weiterführende Frage stellen, warum die Videoüberwachung trotz dieser eindeutig negativen Ergebnisse einen so starken Rückhalt in der Bevölkerung besitzt, wie viele Umfragen es vermuten lassen. Ziel ist es, die Diskussion um die Videoüberwachung um neue Aspekte zu erweitern und Anregungen für zukünftige Forschungen zu geben, und nicht, diese Frage abschließend zu beantworten.

Die bisherigen Erkenntnisse zusammengefasst

Die Ergebnisse von Evaluationen hinsichtlich der Kriminalitätsbekämpfung haben gezeigt, dass die Videoüberwachung geeignet sein kann, bestimmte Vergehen, wie zum Beispiel Eigentumsdelikte, in Einzelfällen zu verhindern. Allerdings machen die Ergebnisse deutlich, dass die generelle Wirkung der Videoüberwachung, insbesondere auf Affekt-Taten oder die Gesamtkriminalität – wenn überhaupt vorhanden – sehr gering ist. Die Videoüberwachung ist also ein Instrument, das in seiner Wirksamkeit eng begrenzt ist. Zudem können Verschiebungseffekte, wie eine Verlagerung der Kriminalität in nicht-überwachte Räume, auftreten, durch die eine Überschätzung der Videoüberwachung bei gleichzeitiger Verminderung der tatsächlichen Wirksamkeit erfolgen.

Ebenso zeigt sich die Videoüberwachung bei der Bekämpfung der Kriminalitätsfurcht nahezu nutzlos. Dem gegenüber werden die Kosten der Videoüberwachung häufig nicht umfassend betrachtet und eine ausreichende Finanzierung nicht sichergestellt. Auch dadurch kann es zu weiteren Einschränkung des Nutzens und der Wirksamkeit der Überwachung kommen. Darüber hinaus gibt es praktische Probleme, welche die Wirksamkeit der Maßnahme verringern, beispielsweise durch Langeweile oder Überforderung beim Überwachungspersonal oder durch Vermeidungsstrategien der DelinquentInnen (zum Beispiel Vermummung). Außerdem können gesellschaftlich Effekte auftreten, die im Wesentlichen negativ zu bewerten sind. Dazu zählen unter anderem die Einschränkung von Bürger- und Freiheitsrechten, sowie die gezielte Verdrängung von (unerwünschten) Randgruppen aus den Innenstädten.[1]

Die (begrenzte) Wirksamkeit der Videoüberwachung des öffentlichen Raums zur Kriminalitätsbekämpfung ist also weitgehend erforscht. Wie kann es aber angesichts dieser Ergebnisse möglich sein, dass ein Instrument, dessen eingeschränkte Wirksamkeit in vielen Studien festgestellt wurde und dessen gesellschaftliche Nachteile deutlich erkennbar sind, einen solchen Boom erlebt?

Da ein gesamtgesellschaftliches Interesse an der Videoüberwachung allein auf Grund der wenigen positiven kriminologischen Auswirkungen bei gleichzeitig deutlich negativen Wirkungen nahezu ausgeschlossen werden kann, könnte man zu dem Schluss kommen, dass nicht Sachargumente, sondern sachfremde Interessen oder politisches Kalkül ausschlaggebend sind[2]. Zumindest die aktuellen Diskussionen legen nahe, dass ein großer politischer Wille besteht, die Videoüberwachung »um jeden Preis« zu nutzen und auszuweiten. Waren die Kameras ursprünglich zur Prävention von Verbrechen legitimiert und installiert worden, ging es in den anschließenden Diskussionen um die Ermittlung und Strafverfolgung von TerroristInnen sowie jugendlichen StraftäterInnen[3]. Es scheint, als würden jetzt – da wissenschaftliche Studien die relative Unwirksamkeit der Videoüberwachung zur Kriminalitätsbekämpfung belegen – immer neue Argumente gesucht, um die Videoüberwachung voran zu treiben. Es drängt sich hier die Frage auf, ob solche zweifelhaften Prozesse, Überlegungen und Vorhaben überhaupt möglich wären, wenn es nicht bereits einen starken Rückhalt für solche Maßnahmen in der Bevölkerung gäbe. Doch wie kommt es zu dem guten Ruf der Videoüberwachung?

Auffällig ist, dass es oft einseitig oder unsauber durchgeführte Studien sind, die von den Medien, so genannten Experten und Politikern aufgegriffen und als Argumentationsbasis herangezogen werden[4]. Auffällig ist auch, dass gerade in den zwei Fällen, die die Diskussion um die Videoüberwachung in den letzten Jahren neu entfachten – den der »Koffer-Bomber« und der »Münchner U-Bahn-Schlägerei« – die Videoüberwachung keine nennenswerte Rolle bei der Ermittlung der

Allerdings machen die Ergebnisse deutlich, dass die generelle Wirkung der Videoüberwachung – wenn überhaupt vorhanden – sehr gering ist.

Das Recht auf Informationelle Selbstbestimmung besagt, dass jeder Mensch selbst entscheiden können soll, was mit eigenen persönlichen Daten geschieht.

StraftäterInnen spielte. Im ersten Fall kam der entscheidende Tipp zur Ergreifung von Youssef Mohamad al-Hajdib vom libanesischen Geheimdienst[5], im zweiten Fall kamen die FahnderInnen den Tätern über die Ortung eines gestohlenen Mobiltelefons auf die Spur[6]. Diese Umstände werden aber durch die Medien und die Politik kaum thematisiert, der Fahndungserfolg wird implizit weiterhin der Videoüberwachung zugeschrieben, was zu dem allzu positiven Bild dieser Maßnahme beitragen könnte[7,8].

Der damit erzeugte Glaube an die Effektivität der Videoüberwachung könnte zur Folge haben, dass die behauptete Erforderlichkeit der Videoüberwachung weniger kritisch hinterfragt wird, Alternativen seltener geprüft werden und die Wirksamkeit installierter Anlagen seltener evaluiert wird. Dies mag zu einer pauschal positiven Grundhaltung der Bevölkerung bei gleichzeitig starker Unwissenheit und Desinformation beigetragen haben. Grundsätzlich scheint die vermeintliche Wirkungsweise der Videoüberwachung einleuchtend und gut kommunizierbar zu sein, während (erst) bei näherer Betrachtung eine tatsächlich hohe Komplexität der Maßnahme festzustellen ist.

Diese Frage nach der Akzeptanz durch die Bevölkerung kann auch auf andere Diskussionen zum Thema »Innere Sicherheit durch Überwachung« übertragen werden. Die Probleme, die hier in Bezug auf die Videoüberwachung aufgetreten sind – wie mangelnde Belege der Wirksamkeit, praktische Probleme, negative Auswirkungen auf die Gesellschaft und hohe langfristige Kosten – treten auch bei anderen Überwachungsmaßnahmen auf, wie bei der Nutzung der Mautdaten, der Vorratsdatenspeicherung oder der Nutzung biometrischer Informationen zur Identifikation von Personen. All diese Maßnahmen wirken vielleicht auf einzelne Delikte oder in bestimmten Situationen, während die negativen Auswirkungen auf das Individuum und die Gesellschaft durch die Masse an Überwachungsmaßnahmen gebündelt werden und sich gegenseitig verstärken können. Trotzdem scheinen sie in der Bevölkerung weitestgehend akzeptiert zu werden.

Das Recht auf Informationelle Selbstbestimmung besagt, dass jeder Mensch selbst entscheiden können soll, was mit eigenen persönlichen Daten geschieht. Wenn dies schon bei der Videoüberwachung so undurchsichtig und schwierig ist, wie soll es dann für den/die BürgerIn möglich sein, dieses Grundrecht angesichts der absehbaren Masse an Überwachungsmaßnahmen durchzusetzen, durch die in letzter Konsequenz die gesamte Kommunikation und Bewegungen der BürgerInnen erfasst werden?

Offensichtlich aber möchte der »Durchschnittsbürger« dieses Recht überhaupt nicht in Anspruch nehmen. Noch im Jahr 1983 ging ein Aufschrei durch die Bevölkerung, als persönliche Daten im Rahmen der Volkszählung abgefragt wurden – Daten die viele Menschen heute ohne zu zögern in sozialen Netzwerken angeben. Wie kommt es, dass im Informationszeitalter – in dem Informationen die wichtigste Ressource sind – dem Recht auf Informationelle Selbstbestimmung ein so geringerer Stellenwert beigemessen wird, als den anderen Grundrechten?

Offensichtlich ist der »normale Bürger« sehr schnell bereit, sich der Überwachung durch den Staat zu unterwerfen, wenn ihm ein – sei es ein noch so kleiner – Sicherheitsgewinn versprochen wird. Dabei scheint es nicht wichtig zu sein, ob dieser Benefit in Folge auch tatsächlich eintritt. Der vermeintliche oder erhoffte Zuwachs an Sicherheit wird hier über sonstige Risiken für die Gesellschaft oder anderen Menschen gestellt. Es ist also zu erwarten, dass es erst zu einem Widerstand in der Breite der Bevölkerung gegen die zunehmende Überwachung kommt, wenn eben diese Masse an Menschen konkret und unmittelbar durch die negativen Auswirkungen der Überwachung betroffen ist. Allerdings ist es dann möglicherweise zu spät sich dagegen zu wehren.

Diese Annahmen bieten einen weiten Raum für zukünftige Untersuchungen, die dabei helfen könnten, eine realistischere Bewertung der Vor- und Nachteile der (Video-) Überwachung bei Politik und BürgerInnen zu erzielen und damit zu einer sinnvollen und angemessenen Nutzung der Sicherheitsinstrumente beizutragen.

Florian Glatzner, FoeBuD e.V.

Literatur

Die Magisterarbeit von Florian Glatzner zum Thema Videoüberwachung im öffentlichen Raum kann unter folgender ISBN 3836497026 bestellt werden.

1 Glatzner, Florian; 2006: Die staatliche Videoüberwachung des öffentlichen Raumes als Instrument der Kriminalitätsbekämpfung – Spielräume und Grenzen. URL: https://www.foebud.org/video/magisterarbeit-florian-glatzner.pdf (15.02.2008). S. 42ff

2 Glatzner, Florian; 2006: Die staatliche Videoüberwachung des öffentlichen Raumes als Instrument der Kriminalitätsbekämpfung – Spielräume und Grenzen. URL: https://www.foebud.org/video/magisterarbeit-florian-glatzner.pdf (15.02.2008). S. 75ff

3 Forsa; 2007: Privatsphäre achten!. In: Stern 24/2007: Widerstand gegen Schäuble-Pläne. S. 27

4 Glatzner, Florian; 2006: Die staatliche Videoüberwachung des öffentlichen Raumes als Instrument der Kriminalitätsbekämpfung – Spielräume und Grenzen. URL: https://www.foebud.org/video/magisterarbeit-florian-glatzner.pdf (15.02.2008). S. 30ff

5 Focus Online; 2006: Entscheidender Hinweis kam aus Libanon. URL: www.focus.de/politik/deutschland/kofferbomber_aid_114060.html (15.02.2008)

6 Rheinische Post Online; 2007: Haftbefehle nach U-Bahn-Überfall. URL: www.rp-online.de/public/article/aktuelles/panorama/deutschland/514819 (15.02.2008)

7 Spiegel Online; 2006: Unionspolitiker fordern Videoüberwachung und Kontrollen. URL: www.spiegel.de/politik/deutschland/0,1518,429888,00.html (15.02.2008)

8 Süddeutsche Zeitung Online; 2007: U-Bahn-Schläger: Viele Straftaten, keine Reue. URL: www.sueddeutsche.de/muenchen/artikel/211/149846/ (15.02.2008)

Abschreckung durch Beobachtung

Am achten Mai diesen Jahres wurde vom Oberverwaltungsgericht (OVG) NRW bundesweit das erste Urteil zu Videoüberwachung an Hochschulen gesprochen. Drei Studierende hatten im Jahr 2006 gegen drei Videoüberwachungsanlagen an der Uni Münster geklagt, um ihr Recht auf Informationelle Selbstbestimmung einzufordern. Daraufhin entfernte die Universitätsverwaltung zwei der beklagten Anlagen schon vor dem ersten Gerichtstermin. Zu der letzten wurde jetzt festgestellt, dass in der Bibliothek des kommunalwissenschaftlichen Instituts zwar weiter gefilmt, aber nicht mehr gespeichert werden darf.

»Überwachungskamera-Wildwuchs«[1] und Ignoranz

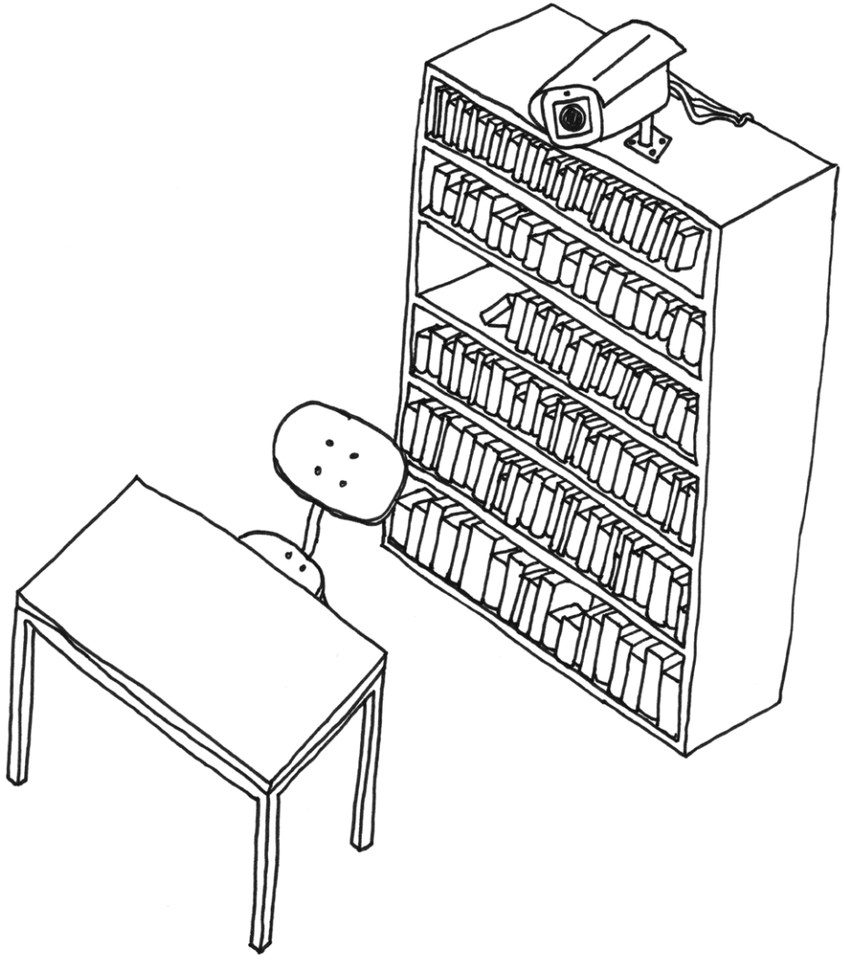
Gegen Ende der 90er Jahre wurden an der Uni Münster diverse Videoüberwachungsanlagen von den einzelnen Instituten, Verwaltungseinheiten und sonstigen Verantwortlichen ohne zentrale Koordinierung, Betreuung oder auch nur rechtliche Überprüfung installiert[2], bis dann ca. 30 Standorte durch etwa 60 Videokameras überwacht wurden.

Zu Beginn des Jahres 2004 fielen die Videokameras eher zufällig der damaligen AStA-Referentin für politische Bildung und demokratische Rechte auf, die schnell feststellte, dass den datenschutzrechtlichen Bestimmungen keinerlei Beachtung geschenkt wurde. Mit Unterstützung der Hochschulgruppe der Kritischen JuristInnen wurden in der Folge die Studierenden mit öffentlichen Aktionen sowie Pressearbeit über die Situation informiert und es wurde versucht, die Universitätsverwaltung dazu zu bringen, das Datenschutzgesetz (DSG) einzuhalten. Dazu wurde auch die Landesdatenschutzbeauftragte (LDB) des Landes NRW eingeschaltet, die ihrerseits die Uni mehrfach und nachdrücklich auf die datenschutzrechtliche Auskunftspflicht hinwies. Insgesamt wurde das sensible Thema Datenschutz von der Universitätsverwaltung jedoch nicht sehr ernst genommen, so dass sich trotz vieler Bemühungen die Situation bis zum Jahr 2006 nur wenig geändert hatte.

Die Informationelle Selbstbestimmung einklagen

Zu diesem Zeitpunkt beschlossen drei Studierende ihr Recht auf Informationelle Selbstbestimmung einzuklagen und zogen mit Unterstützung des AStA gegen drei Videoüberwachungsanlagen vor Gericht: eine befand sich im Foyer des Schlosses, eine im Lesesaal der ULB sowie eine in der kommunalwissenschaftlichen Bibliothek.

Während die Universitätsverwaltung die beiden erstgenannten Anlagen noch vor dem ersten Gerichtstermin entfernte, wurde die Überwachung der kommunalwissenschaftlichen Bibliothek das Thema zweier Verhandlungen in Münster: am 19. Oktober 2007 vor dem Verwaltungsgericht (VerwG) sowie am achten Mai 2009 bei dem Oberverwaltungsgericht (OVG). Die Position der Universität war dabei jeweils die gleiche, die sie auch bei den mittlerweile abgehängten Anlagen vertreten hatte: sie seien zur Bekämpfung von Diebstahl und Vandalismus notwendig und auch wenn niemand mehr sagen konnte, wann die Anlage genau installiert



wurde, so war man sich doch sicher, dass seitdem nichts mehr gestohlen worden sei. Gleichzeitig wurde zugegeben, dass der Monitor, auf den die Kamerabilder übertragen werden, von der Aufsichtsperson faktisch nicht beobachtet werde und die Wirkung der Kameras aus bloßer Abschreckung bestehe. Letztlich folgten das VerwG und das OVG der Argumentation der KlägerInnen nur teilweise und sie entschieden jeweils, dass die Aufzeichnungen zwar grundsätzlich nicht gespeichert werden dürften, die bloße Videoüberwachung jedoch zulässig sei. Damit wurden die hohen Hürden des DSG NRW für die Speicherung von Daten – die

Das Thema Datenschutz wurde von der Universitätsverwaltung nicht sehr ernst genommen, so dass sich nach zweijährigen Auseinandersetzungen nur sehr wenig geändert hatte.

Speicherung muss für den verfolgten Zweck unverzichtbar sein – bestätigt. Bei der Frage der Zulässigkeit der Aufzeichnungen (ohne Speicherung) entschieden die Gerichte, dass zwar eine erheblicher Grundrechtseingriff vorliege, das Interesse der Universität an einer intakten Bibliothek jedoch überwiege – zumindest dann, wenn wie im vorliegenden Fall die losen Blattsammlungen nicht mit physischen Sicherungsmethoden geschützt werden können.

Ende gut?

Nach fast fünf Jahren der Auseinandersetzung zwischen Studierenden und der Universität um den Umfang und die datenschutzrechtliche Zulässigkeit der Videoüberwachung kann resümiert werden, dass die Zahl der Überwachungsanlagen deutlich zurückgegangen ist und die Universitätsverwaltung in Bezug auf die Einhaltung der datenschutzrechtlichen Bestimmungen sensibilisiert wurde[3].

Andererseits wird weiterhin an 10 bis 20 Stellen videoüberwacht und die Frage der Notwendigkeit von Überwachung kann von denen, die überwachen und von denen die überwacht werden durchaus unterschiedlich beantwortet werden. Zudem kündigte die Justiziarin der Universität vor Gericht an, nun neue technische Verfahren ausprobieren zu wollen, um die Speicherung doch noch durch zusetzten. Im übrigen könne man dies ja auch aus Allgemeinen Studienbeiträgen (sic!) bezahlen, da intakte Bibliotheken ja eine Verbesserung der Lehre seien.

Obgleich letztere Aussage wohl eher dem Unmut über eine weitestgehend verlorene Auseinandersetzung und nicht einer rationalen Analyse des Möglichen entsprungen sein dürfte, weist dieser Ausblick darauf hin, dass die Auseinandersetzungen um Überwachung und Informationelle Selbstbestimmung permanente sind und ansatzweise erträgliche Standards mit den verschiedensten Methoden immer wieder neu durchgesetzt werden müssen.

Tim Ackermann und Annelie Kaufmann

Literatur

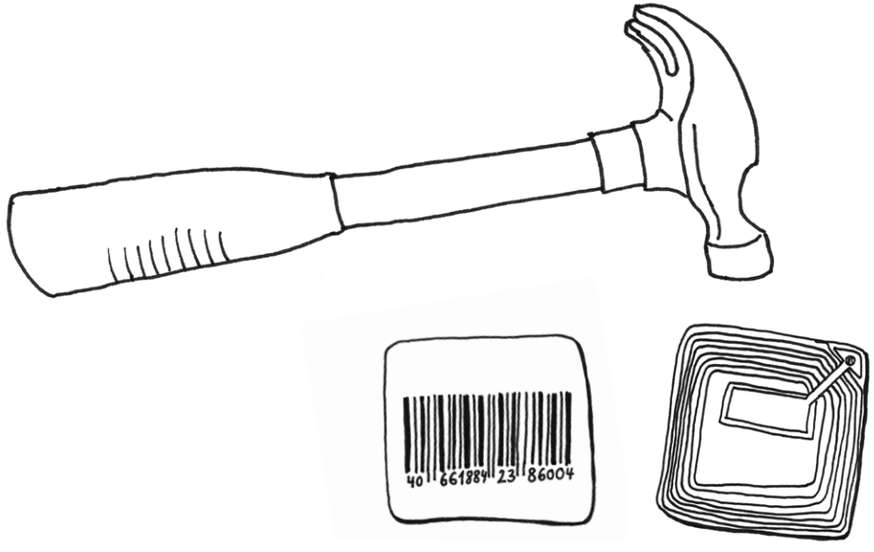
Kalitschke, Martin 2009: Kontroverse um Videoüberwachung, in: Westfälische Nachrichten vom 23. Januar 2009, verfügbar über: www.westfaelische-nachrichten.de/lokales/muenster/nachrichten/946763_Kontroverse_um_Videoueberwachung.html, 25.01.2009.

1 Der Pressesprecher der Uni Münster, Norbert Frie, bezeichnete mit diesem Begriff die Situation an der Uni vor den Auseinandersetzungen mit dem AStA, der Landesdatenschutzbeauftragten und den KlägerInnen, vgl. Kalitschke 2009.

2 Das Datenschutzgesetz des Landes NRW (DSG NRW) trat allerdings erst am 31. Mai 2000 in Kraft, bis dahin galt die Dateienregisterverordnung vom 11. April 1989. Jedoch hätten laut § 35 (1) DSG NRW die Verarbeitungen personenbezogener Daten, die zum Zeitpunkt des In-Kraft-Tretens des Gesetzes bereits begonnen worden waren, innerhalb von drei Jahren nach In-Kraft-Treten mit den Vorschriften des Gesetzes in Übereinstimmung gebracht werden müssen.

3 Vgl. die Aussage des Pressesprechers der Uni Münster, Norbert Frie, in der WN vom 23.01.2009: man überwache nur noch dort, »wo es absolut erforderlich ist« (Kalitschke 2009).

RFID (Radio Frequency Identification)
oder wie zerstöre ich meine elektronische Identität



Immer wieder verändert der technische Fortschritt das Leben der Menschen grundlegend. Viele Neuerungen erleichtern den Alltag und verringern den erforderlichen Arbeitsaufwand. Doch gab es trotz aller Vorteile, die die Entwicklung mit sich brachte, immer auch ernstzunehmende kritische Stimmen, sowie ethische und politische Bedenken.

So wurde in den 70er Jahren der Barcode eingeführt. Die auf Etiketten gedruckten Streifen unterschiedlicher Breite waren bald auf jedem Produkt, von Büchern bis zu Bettdecken, zu entdecken. Bedeutete dies für Logistikunternehmen eine wahre Revolution, sahen andere bereits eine große Gefahr in dem schwarz-weißen Strichcode: Den Alptraum des gläsernen Menschen. Doch die Technik hat vor den Bedenken nicht Halt gemacht. Zehn Jahre später hielt die kontaktlose RFID-Technik Einzug in Industrieanwendungen. Erstmals erfahrbar wurde die Technik in Bekleidungsgeschäften durch die tellerförmigen Buttons, die lediglich an der Kasse beim Bezahlen zu entfernen sind und an den großen Leiterschleifen kurz vor dem Ausgang des Geschäfts.

Bald wurde der RFID-Chip auch zur Zugangskontrolle von »sicherheitsrelevanten« Bereichen eingesetzt. ArbeitgeberInnen entdeckten ebenfalls die neue Technik als einfaches Mittel zur Arbeitszeiterfassung ihrer Angestellten.

Mittlerweile laufen die kleinen Scheiben dem Barcode den Rang ab, so dass inzwischen in und auf vielen Gebrauchsgegenständen RFID-Chips anzutreffen sind, die sich meist unter einer Folie, einem Umschlag oder ähnlichem verstecken. Selbst unter der Haut werden sie zum Beispiel BesucherInnen einiger Edel-Diskotheken eingepflanzt.[1]

How does it work?[2]

Trotz der vielen verschiedenen Möglichkeiten, RFID-Geräte aufzubauen, möchte ich hier lediglich auf die gängigste Art eingehen: RFID-Technik basiert auf zwei unabhängigen Komponenten. Zum einen ist das Schreib-/Lesegerät zu betrachten, welches grob eine Antenne, einen Sende- beziehungsweise Empfangsteil, sowie die passende Steuerung enthält. Weiterhin wird eine Auswerteeinheit benötigt, die ein Computer oder eine einfache Elektronikschaltung zur Erkennung oder Registrierung des Transponders sein kann. Das Lesegerät benötigt einen Anschluss an eine Stromversorgung.

Der zweite und lästigere Teil ist der Transponder, oder auch Tag genannt. Untergebracht in einer Chipkarte, zwischen einlaminierter Folie auf einer Lebensmittelverpackung oder ähnlichem, enthält dieser eine Antenne, sowie eine integrierte Schaltung (Chip). Der Transponder braucht keine Stromversorgung, da er sich während der Kommunikation, die nötige Energie vom Lesegerät besorgt. Das Lesegerät kann von diesem Transponder Daten lesen und auch wieder zurückschreiben.

Kommt nun ein Transponder in den Lesebereich, wird es zunächst durch das magnetische Feld, welches vom Lesegerät erzeugt wird, mit Strom versorgt. Es wartet auf eine Meldung des Lesegeräts, ob gesendet werden darf.[3] Sobald diese Meldung empfangen wurde, meldet sich der Transponder mit seiner Seriennummer an. Dabei läuft die gesamte Kommunikation ebenfalls über das magnetische Feld. Nach dieser Anmeldeprozedur erfolgt der eigentliche Informationsaustausch.

Durch den eingebauten Prozessor kann der Transponder Informationen auch verarbeiten. Somit ist es zum Beispiel möglich, dass die Funkstrecke verschlüsselt werden kann. Die Arbeitsreichweite eines Transponders liegt bei etwa 15 cm beziehungsweise 1,5 m (abhängig von der verwendeten Technologie).

What's the problem with RFID?

Durch die eindeutige Seriennummer ist ein Transponder nahezu weltweit eindeutig einem Objekt (egal ob Lebewesen, Joghurtbecher oder Kleidungsstück) zugeordnet. Trotz der unterschiedlichen Anwendungsfälle werden die meisten Transponder von den unterschiedlichsten Auslesegeräten registriert. Die Benutzerausweisnummer eines Büchereiausweises würde somit nicht nur von der betreffenden Bücherei gelesen werden können, sondern auch von sämtlichen anderen Lesegeräten. Bei Vernetzung beziehungsweise Einspeisung der Informationen in Datenbanken lassen sich dadurch leicht Bewegungsprofile erstellen.

Doch nicht nur Lesegeräte, die als solche erkannt werden, schwirren in den Einkaufsparadiesen herum. RFID-Reader wurden schon im Fußboden, unauffällig an Türrahmen oder Regalen entdeckt.

Das Gegenstück dazu, die Transponder, sind bei einem Stückpreis von 10 Cent[4] so kostengünstig, dass es kein Problem mehr darstellt, einfach an allem einen Transponder anzuheften. Unbemerkt werden diese »Schnüffel-Chips« auch in Kleidungsstücke eingenäht oder wie im Fall der »BahnCard 100[5]« in Chipkarten einlaminiert. Zur Fußball-WM 2006 konnten Transponder in den Eintrittskarten wiedergefunden werden – zur Verhinderung von Schwarzmarkthandel[6]. Zur Bezahloptimierung werden in einigen Städten Tickets des ÖPNV mit Transpondern ausgestattet. Das Ausleihen von Büchern ist in manchen Städten soweit automatisiert, dass RFID-Chips in jedes Buch eingeklebt und entsprechende Ausleih- und Rückgabegerä-

te installiert wurden.[7] Um Prämienpunkte beim Kundenbindungsprogramm Payback sammeln zu können wird eine entsprechende Chipkarte benötigt die, unbemerkt für die Nutzer des Systems, einen RFID-Transponder trug. Auch dem im November 2007 eingeführten »elektronischen Reisepass« wurde eine RFID-Komponente eingefügt. Zudem soll auch der zukünftige digitale Personalausweis, zur besseren Feststellung der Identität, einen Transponder enthalten.[8]

An diesen Beispielen ist leicht erkennbar, in welchem Ausmaß RFID-Transponder in unserem täglichen Leben enthalten sind. Das dadurch Begehrlichkeiten an sensibelsten Daten entstehen, sollte einleuchten.

Die Frage nach der eigentlichen Sicherheit der RFID-Systeme ist ebenfalls strittig. Die Arbeitsreichweite liegt zwar lediglich bei maximal 1,5 m, was dabei jedoch oft vergessen wird ist die Entfernung der passiven Kommunikation – sprich dem Abhören. Diese liegt nach Versuchen des BSI[9] bei etwa 3 m[10]. Es kann sich also eine AngreiferIn beispielsweise einem Büchereiausleihgerät auf etwa zwei Meter nähern, um sämtliche ausgeliehenen Bücher und Ausweise mitzulesen. Auch wenn dabei die eigentliche Kommunikation aufgrund der Verschlüsselung nicht ausgespäht werden kann, enthalten Transponder jedoch eine nicht-kryptierte Seriennummer. Ausserdem konnte die Kryptierung der Kommunikation bereits bei der weltweit meistgenutzten Chipkarte entschlüsselt werden[11].

What to do?

Doch um nun die RFID-Paranoia ein bisschen zu mildern, einige alltagstaugliche Abwehrtips:

Die einfachste Möglichkeit sich gegen unbewusstes Auslesen zu schützen, ist die Antenne abzuschirmen. Am einfachsten wird dazu Alu-Folie um die Cipkarte gewickelt. Die integrierte Schaltung empfängt nun nicht mehr ausreichend Energie und kann somit auch nicht mehr senden. Sollen allerdings Bücher aus der örtlichen, vollautomatischen Bücherei gegen ein Auslesen geschützt werden, kann eine Kühltasche aus dem Lebensmittelmarkt von Nutzen sein. Diese ist Innen mit einer Aluminiumfolie ausgeschalt und meist ausreichend groß um größere Gegenstände transportieren zu können.

Um den »Schnüffelchip« dauerhaft gegen das Auslesen zu schützen, kann möglichst viel Rumbiegen helfen. Zunächst sollte die Antenne abgetastet werden, um entdecken zu können, wo sich der Chip befindet. An einer Stelle macht sich dieser durch eine kleine Erhöhung bemerkbar. Dies ist die schwächste Stelle des Transponders. Entweder diese Stelle gezielt verbiegen, oder aber die integrierte Schaltung mit einem kleinen Hammerschlag zerstören.

Durch die eindeutige Seriennummer ist ein Transponder nahezu weltweit eindeutig einem Objekt (egal ob Lebewesen, Joghurtbecher oder Kleidungsstück) zugeordnet

Da, beispielsweise in einer Chipkarte, der RFID-Chip nicht immer zu erkennen ist, gibt es noch den Mikrowellen-Tod. Hierzu wird die Karte in der Mikrowelle »vergessen« und diese für Bruchteile einer Sekunde eingeschaltet. Durch die hohe Feldstärke wird der beinhaltete Chip unwiderruflich zerstört. Bei dieser Methode kann das Ausweisdokument allerdings einen sichtbaren Schaden nehmen. Daher sollte der Mikrowellenherd wirklich nur für einen kurzen Augenblick eingeschaltet werden. Trotz der Zerstörung der elektronischen Komponente des E-Pass beziehungsweise des elektronischen Personalausweises bleibt die Gültigkeit weiterhin gewährleistet. Allerdings kann es zu Problemen beim Vorzeigen beziehungsweise der Registrierung kommen.

Es gibt zahlreiche weitere Möglichkeiten, RFID-Geräte zu manipulieren, deren Diskussion hier aber zu weit führen würde.[12]

The End my Friend?

Wie weit sich diese Technik noch in unser Alltagsleben integrieren wird, ist eine Frage der Zeit und des Umgangs mit der RFID-Technologie. Die Vorteile, die durch die fortschreitende Informatisierung und Automatisierung entstehen, stehen einigen Gefahren gegenüber, die wir nicht aus den Augen lassen dürfen. So sollten zum Beispiel RFID-Lesegeräte wie -Transponder durch geeignete Maßnahmen gekennzeichnet werden. Beispiele dafür lieferte der FoeBuD mit einem Wettbewerb für ein RFID-Warnlogo.

Ähnlich wie bei Benutzung einer Bankkarte in sämtlichen Geschäften oder das Mitmachen von Gewinnspielen, entstehen durch die RFID-Technologie personenbezogene Daten. Ob diese Daten erhoben und verwendet werden sollte jedem und jeder selbst überlassen werden. Dementsprechend ist ein verantwortungsvoller Umgang mit den »Schnüffelchips« notwendig, notfalls auch deren Zerstörung.

Winston, AK-Vorrat Münster

1 www.heise.de/tr/RFID-im-Koerper--/blog/artikel/118959

2 rfid-handbook.de/

3 www.elektor.de/Uploads/Files/060132-WII.pdf

4 www.rfid-journal.de/rfid-kosten.html

5 www.foebud.org/rfid/bahncard-mit-rfid-schnueffelchip

6 de.wikipedia.org/wiki/Fußball-Weltmeisterschaft_2006/Eintrittskarten#Sicherheit_und_Datenschutz

7 www.muenster.de/stadt/buecherei/selbstverbuchung.html

8 ➳ Artikel: Der elektronische Personalausweis

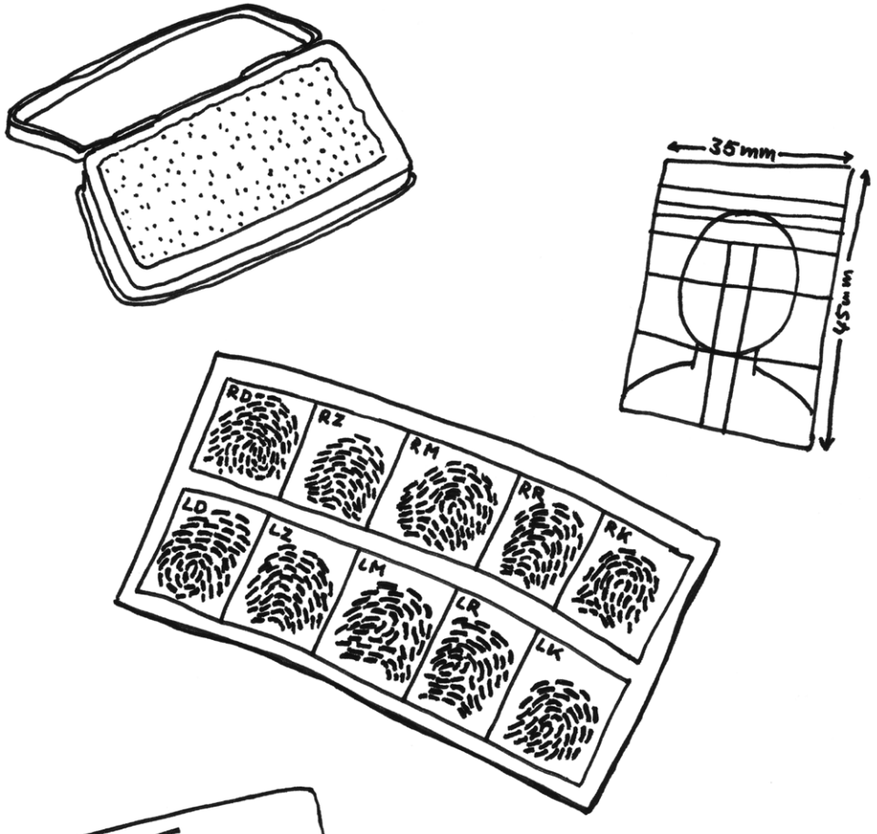
9 Bundesamt für Sicherheit in der Informationstechnik

10 www.bsi.de/fachthem/rfid/index.htm

11 www.want2pay.com/mifarebug.pdf; chaosradio.ccc.de/creo98.html

12 Empfehlenswert ist das 8. Kapitel des »RFID-Handbuch« von Klaus Finkenzeller

Der elektronische Personalausweis



Unser Alltag im Informationszeitalter ist geprägt von einem ständigen technologischen Wandel. Vom klobigen Walkman zum Mini-MP3-Player, vom Desktop-PC mit laut röhrendem Lüfter zum handtaschenkompatiblen Netbook, vom übergroßen Mobiltelefon mit ausziehbarer Antenne zu vielseitig einsetzbaren Smartphones – vieles wird kleiner, leistungsfähiger, manchmal sicherer und oftmals auch bunter. Diesem Trend will nun auch die Bundesregierung folgen und führt zum 1. November 2010 einen neuen elektronischen Personalausweis (ePA) ein.

Frau Mustermann hat einen neuen Haarschnitt – das Format

Der ePA wird gerade mal so groß wie eine Scheckkarte sein. Auf der Vorderseite werden wie beim heutigen Ausweis persönliche Daten und ein – jetzt ebenfalls kleineres – Foto aufgedruckt sein. Das Foto muss – wie auch beim elektronischen Reisepass (ePass) – den Standards der Bundesdruckerei für biometrische Bilder entsprechen, das heißt die Position des Gesichts und der Gesichtsausdruck müssen in eine Schablone[1] passen, um eine automatische digitale Identifikation der abgebildeten Person zu ermöglichen. Mit der Einführung ist also die Zeit von freundlichen Gesichtern auf Passbildern endgültig passé.

Ähnlich wie der 2005 eingeführte elektronische Reisepass wird der ePA einen kontaktlos auslesbaren RFID-Chip[2] beinhalten, auf dem die Daten der InhaberIn gespeichert werden. Neben den bekannten Personendaten wie Name, Vorname, Anschrift, Geburtsdatum und so weiter, wird auch eine digitalen Kopie des biometrischen Fotos gespeichert. Zusätzlich können (vorerst) freiwillig noch zwei Fingerabdrücke hinterlegt werden.

Frau Mustermann im Web – mehr als nur ein Ausweis

Die Hauptfunktion des ePA wird weiterhin die Identifikation von Menschen bei hoheitlichen Kontrollen und Prozessen, zum Beispiel Verkehrs- und Alterskontrollen oder Behördengängen, sein. Zusätzlich werden mit dem »Internetausweis« (kostenlos) und der »qualifizierten elektronischen Signatur« (kostenpflichtig) zwei weitere Zusatzfunktionen angeboten[3]. Während Letztere der Verifizierung von geschäftlichen Dokumenten dient und sich eher an Geschäftsleute richtet, soll der Internetausweis in Zukunft die bisherigen Identifikationsmechanismen im Internet, zum Beispiel die Benutzeranmeldung in Online-Shops, ablösen und neue Möglichkeiten der Kontaktaufnahme mit Behörden ermöglichen.

> Mit der Einführung des ePA ist also die Zeit von freundlichen Gesichtern auf Passbildern endgültig passé.

Die Sicherheit der Daten auf dem Chip soll dabei durch verschiedene Maßnahmen gewährleistet werden. Grundsätzlich werden alle auf dem Chip abgelegten Daten verschlüsselt. Um die Daten zu entschlüsseln bestehen dann zwei Möglichkeiten:

Im Rahmen von hoheitlichen Kontrollen werden spezielle vom Staat autorisierte Lesegeräte zum Einsatz kommen. In Kombination mit einer im Klartext auf dem ePA aufgedruckten PIN können diese Geräte die gespeicherten Daten abrufen. Dieses Merk-

Neben den bekannten Personendaten wie Name, Vorname, Anschrift, Geburtsdatum und so weiter wird auch eine digitalen Kopie des biometrischen Fotos gespeichert. Zusätzlich können (vorerst) freiwillig noch zwei Fingerabdrücke hinterlegt werden.

mal dient dem Zweck, ein Verhindern der Kontrolle durch eine Verweigerung der PIN-Angabe unmöglich zu machen.

Die zweite Möglichkeit ist das Einlesen des ePA mit einem frei erhältlichen über einen PC mit dem Internet verbundenen Lesegerät unter Eingabe einer geheimen, nur der InhaberIn bekannten PIN.

Angesichts der hohen Sicherheit des bisherigen Personalausweises, welcher auch laut Aussagen der BefürworterInnen des ePA »eines der fälschungssichersten Ausweisdokumente überhaupt«[4] darstellt, ist die Frage nach den Beweggründen für und dem Nutzen der Umstellung, durchaus berechtigt. Warum also der ganze Aufwand für Frau Mustermann? Eine kritische Betrachtung…

Frau Mustermann bekommt ein neues Türschloss – die Sicherheit des ePA

Als eines der Hauptargumente der BefürworterInnen des ePA wird eine Verbesserung eben dieser hohen Sicherheit des alten Personalausweises angeführt. So soll durch das biometrische Foto eine Verwendung von Ausweisen ähnlich aussehender Menschen verhindert werden, vor allem aber die Sicherheit bei der Identifikation im Internet durch den Internetausweis gesteigert werden. Beim derzeitigen Stand der (dem Bund flächendeckend zur Verfügung stehenden) Technik[5] kann dem ersten Punkt der FürsprecherInnen jedoch schnell widersprochen werden. Eine stärkere Veränderung des Aussehens, wie zum Beispiel die Kürzung der Haare oder das Tragen eines Vollbartes, senkt den Erkennungsgrad der biometrischen Systeme in kritischem Maß herab. Jedoch ist mit Blick auf neue Entwicklungen im Bereich der Bilderkennungssysteme, die unter anderem auch schon im privaten Bereich verfügbar sind[6], davon auszugehen, dass dieses Sicherheitsmerkmal in absehbarer Zukunft greifen wird.

Bezüglich der Sicherheit bei Online-Transaktionen ist ein abschließendes Urteil in diesem frühen Stadium schwer möglich. Allerdings haben die zahlreichen Datenschutzskandale des letzten Jahres in der Privatwirtschaft gezeigt, dass nicht die Übermittlung, sondern die Speicherung, Weiterverarbeitung und Aufbewahrung von Daten das größte Gefahrenpotential bergen. Dies wird sich mit Einführung des ePA nicht ändern, da dieser lediglich die Übermittlung und Identifikation der KommunikationspartnerInnen schützt.

Des Weiteren ist über die vom Bundesministerium für Sicherheit in der Informationstechnik (BSI) entwickelten Sicherheitstechniken wenig bekannt. Auch wenn Grundprinzipien genannt werden[7,8], bleiben wichtige Details, zum Beispiel über verwendete Algorithmen und Prozesse, unbekannt (die angegebene technologische Richtlinie[7] wurde bis zur Veröffentlichung dieses Readers noch nicht veröffentlicht). Was bei so einem kritischen Thema logisch erscheint, ist jedoch im Bereich der Sicherheitstechnik seit Jahrzehnten nicht mehr aktueller Stand. Denn nur eine Veröffentlichung der Systemspezifikation ermöglicht eine genaue Prüfung der Mechanismen durch unabhängige ExpertInnen aus Wissenschaft und IT-Community. Viele unbekannte Mechanismen[9,10] enthielten letztendlich Lücken, die nach kurzer Zeit entdeckt und ausgenutzt wurden.

Auch die Möglichkeit, die zentrale PIN des ePA zu ändern, also den Chip zu beschreiben, wird nicht zur Sicherheit des gesamten Systems beitragen. Diese Zugriffsmethode wurde für den Fall, dass eine NutzerIn ihre PIN vergisst oder diese bekannt wird, konzipiert. Jedoch sollen unter anderem sämtliche Botschaften und Meldeämter, das heißt eine große Zahl verschiedener staatlicher Stellen im In- und Ausland, in der Lage sein, diesen Vorgang durchzuführen. Um die Sicherheit des ePA nicht zu gefährden, müssen an all diesen Stellen strenge Sicherheitsvorkehrungen, zum Beispiel der kontrollierte Zugang zu den Lese-/Schreibgeräten, eingehalten werden. KritikerInnen sehen es jedoch als sehr wahrscheinlich an, dass hier nicht in allen Institutionen für ausreichende Sicherheit gesorgt werden kann[11].

Eine Benachteiligung von Menschen, die auf dem ePA keine biometrischen Daten hinterlegen wollen oder können, durch staatliche Institutionen oder Akteure aus der Wirtschaft ist ebenfalls nicht auszuschließen.

Frau Mustermann und die Behördengänge

Von BMI und BSI sind bisher fast ausschließlich Beispielanwendungen für die Privatwirtschaft entwickelt und gezeigt worden. Das durch den ePA entstehende Potential für e-Government wird nach aktuellem Stand in den nächsten Jahren nicht ausgeschöpft werden. Grund hierfür sind unter anderem die massiven Investitionen in die technische Infrastruktur der Behörden. Die Zeit der papierbasierten Behördengänge ist also mitnichten vorbei.

Der Bedarf für qualifizierte elektronische Signaturen ist aktuell eher gering und es existieren etablierte und sichere Lösungen[12]. Angesichts der entstehenden Kosten für die AusweisinhaberIn und den Aufbau einer flächendeckenden Infrastruktur auf Seiten von Staat und Wirt-

schaft sollte eine Prognose zur Verbreitung dieser Zusatzfunktion eher vorsichtig ausfallen. (Die Kosten der Umstellung des Personalausweises auf den ePA wurden von BMI und BSI bisher nicht beziffert oder geschätzt, eine qualifizierten elektronische Signatur soll für 30 Euro erworben werden können.)

Frau Mustermann im Glashaus

Neben diesen eher technischen Argumenten ist aus Sicht von Datenschützern noch ein weiteres, schwerwiegendes Argument anzuführen:

Die verpflichtende Speicherung eines biometrischen Merkmals (Foto) und die Schaffung der Infrastruktur zur Speicherung weiterer Merkmale ist ein erster Schritt in die verpflichtende biometrische Totalerfassung der Menschen. Anfragen von Organisationen wie der Gewerkschaft der Polizei (GdP) zur Aufnahme der Fingerabdrücke in den ePA bestehen bereits und auch der derzeitige Innenminister Wolfgang Schäuble wollte sich nicht darauf festlegen, dass es bei der Freiwilligkeit der Abgabe von Fingerabdrücken bleibt[4]. Eine Benachteiligung von Menschen, die auf dem ePA keine biometrischen Daten hinterlegen wollen oder können, durch staatliche Institutionen oder Akteure aus der Wirtschaft ist ebenfalls nicht auszuschließen. Dies gilt auch für Menschen, die Probleme mit der Bedienung des Systems, zum Beispiel dem Umgang mit privaten Lesegeräten oder den PINs haben. Die Gründe für die Umstellung auf den ePA sind, wie oben ausgeführt, hinsichtlich der Sicherheit des Ausweises fragwürdig.

Zudem weisen Länder wie Spanien, die bereits seit Jahrzehnten biometrische Daten in den Ausweisen speichern, keine besseren Aufklärungsquoten für Kriminalfälle auf. In Kombination mit anderen lebenslang gültigen elektronischen Dokumenten beziehungsweise Kennungen wie der elektronischen Gesundheitskarte[13] oder der neuen SteuerID und der fortschreitenden Vernetzung von Datenbanken steigen »Qualität« und Umfang der über jede und jeden von uns verfügbaren Informationen. Fraglich ist dann, wer diese Möglichkeiten entdeckt und was er/sie damit anstellt…

Frau Mustermanns Weg aus dem Brunnen...

Nach Verabschiedung des neuen Personalausweisgesetzes durch Bundestag und Bundesrat ist die Einführung des ePA beschlossene Sache. Sollte sich Frau Mustermann – vielleicht auch nach dem Lesen entsprechender Artikel – entscheiden, dass sie es mit der Verwendung des ePA nicht allzu eilig hat, kann sie dementsprechend nur auf unglückliche Zufälle hoffen. Der alte Personalausweis wird noch bis Oktober 2010 mit den derzeit geltenden Gültigkeitsfristen ausgegeben, ein ePA wird auch ohne funktionsfähigen RFID-Chip[2,14] gültig bleiben…

durito, AK-Vorrat Münster

Die verpflichtende Speicherung eines biometrischen Merkmals (Foto) und die Schaffung der Infrastruktur zur Speicherung weiterer Merkmale ist ein erster Schritt in die verpflichtende biometrische Totalerfassung der Menschen.

1 Passbild-Schablone der Bundesdruckerei, Chip-Download.Archiv, http://www.chip.de/downloads/Passbild-Schablone_18918538.html

2 ➳ Artikel: RFID

3 Bundesamt für Sicherheit in der Informationstechnik, Der elektronische Personalausweis, www.bsi.de/fachthem/elekausweise/epers-ausweis.htm

4 Krempl, S., Opposition lehnt elektronischen Personalausweis geschlossen ab, heise Online, 17.10.2008, http://www.heise.de/newsticker/Opposition-lehnt-elektronischen-Personalausweis-geschlossen-ab--/meldung/117525

5 Evaluierung biometrischer Systeme – Fingerabdrucktechnologien – BioFinger, BSI Studie, http://www.bsi.de/literat/studien/BioFinger/BioFinger_I_I.pdf

6 Garfinkel, S. Rosenberg, B., Gesichtserkennung: Clever oder unheimlich?, Technology Review 03/2009, http://www.heise.de/tr/Gesichtserkennung-Clever-oder-unheimlich--/artikel/134269

7 Bender, J., Kügler, D., Margraf, M., Naumann, I., Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis, Datenschutz und Datensicherheit 03/2008

8 Ein Personalausweis für die reale und elektronische Welt, Andreas Reisen, Innovative Verwaltung, 03/20http://www.bundesnetzagentur.de/enid/Elektronische_Signatur/Zertifizierungsdiensteanbieter_ph.html09

9 Hacker liest unbemerkt RFID-Personaldokumente von US-Bürgern aus, heise security, 03.02.2009, http://www.heise.de/security/Hacker-liest-unbemerkt-RFID-Personaldokumente-von-US-Buergern-aus--/news/meldung/126819

10 NutzerInnen eines weit verbreiteten Betriebssystems können alternativ einen Blick auf die Liste der notwendigen und kritischen Sicherheitsupdates ihres Systems werfen…

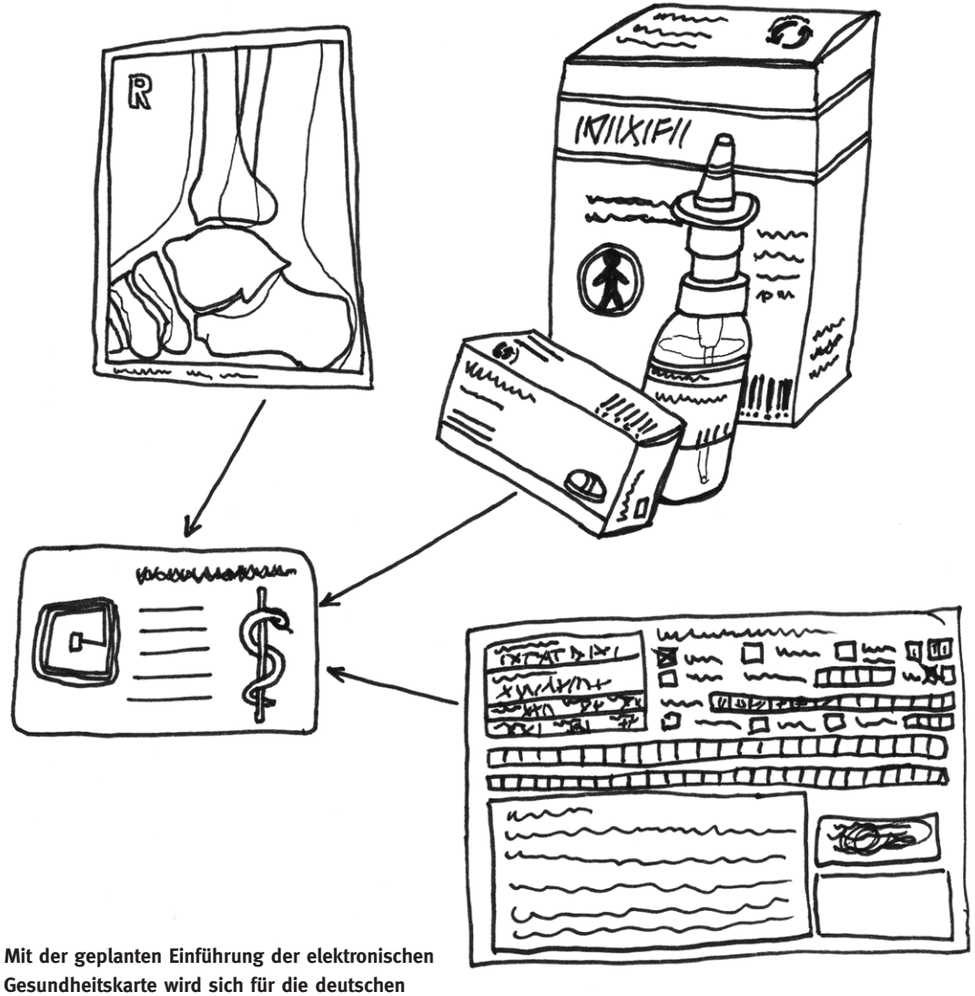
11 Kurz, C., Starbug, Der elektronische Personalausweis, 25C3, Berlin, 2008

12 Zertifizierungsdiensteanbieter (ZDA), Bundesnetzagentur,

13 Artikel elektronische Gesundheitskarte

14 Netzpolitik TV, Frank Rosengart über den ePA, http://www.youtube.com/watch?v=tboZsy4qG5Y

Elektronische Gesundheitskarte



Mit der geplanten Einführung der elektronischen Gesundheitskarte wird sich für die deutschen PatientInnen einiges ändern. Denn zukünftig können nicht nur diese ihre »Gesundheitsdaten selbst in die Hand nehmen«, wie es das Bundesministerium für Gesundheit (BMG) so schön formuliert, sondern auch andere.

Was ist auf der Karte gespeichert?
Auf der elektronischen Gesundheitskarte werden alle Angaben der PatientInnen bezüglich ihrer Versicherung gespeichert, wie zuvor bereits auf der uns bekannten Krankenkassenkarte. Optional können weitere Behandlungsdaten in einer zentralen Datenbank festgehalten werden. Notfallrelevante Informationen sollen in einem speziellen Datensatz gespeichert werden können, der auch ohne Patientenschlüssel im Ernstfall zugänglich ist. Arztbriefe und Röntgenbilder werden aufgrund ihres Datenumfangs nicht auf der Karte gespeichert (auf die Karte selbst passen nur 32 kB), sollen jedoch von einer zentralen Datenbank aus abgerufen werden können. Der Löwenanteil der Daten wird somit zentral in speziellen Datenbanken gespeichert werden um bei Bedarf abrufbereit zu sein.

Wann man wie und von wem behandelt wurde brauche ich mir dann nicht mehr zu merken, die behandelnde ÄrztIn entnimmt es automatisch dem Datensatz. Rezepte werden in Zukunft nur noch in elektronischer Form ausgestellt. Für Personen über 15 Jahren gilt, dass ihr Ausweis mit einem Foto zwecks Identifikation ausgestattet werden soll. Einige Krankenkassen bestehen gar auf ein biometrisches Foto der Versicherten.

Was erhofft sich der Staat davon?
Durch die Möglichkeit auf die Krankengeschichte der PatientInnen zurückgreifen zu können sollen Doppeluntersuchungen, Arzneimittelunverträglichkeit, Allergien und andere Risiken und Kosten erkannt und ausgeschlossen werden. Langfristiges Ziel ist laut BMG der Aufbau einer elektronischen Patientenakte sowie eines einheitlichen europaweiten elektronischen Gesundheitsdienstes. Um jedoch eine vollständige elektronische Patientenakte erstellen zu können, müsste sich jedeR PatientIn dazu bereit erklären, ihre Daten bei jeder Behandlung speichern zu lassen – es sei denn dies wird in Zukunft für alle BürgerInnen verpflichtend sein.

Wer kann auf meine Daten zugreifen?
Planmäßig soll jedeR PatientIn Zugriff auf ihre/seine Daten erhalten und darf diese somit beliebig verändern, freigeben oder löschen. Dies soll voraussichtlich an Giroautomaten der Sparkassen möglich sein. Vollständiger Zugriff ist allerdings nur zusammen mit der PIN-Nummer der PatientIn in Verbindung mit der einer weiteren Karte zugehörigen PIN, dem elektronischen Heilberufsausweis möglich. Jeder Zugriff soll protokolliert werden. Die PatientIn darf von Dritten nicht dazu gedrängt werden die Daten zugänglich zu machen.

Vorerst sollen ÄrztInnen, ZahnärztInnen und ApothekerInnen damit ausgestattet werden. Pflegekräfte dürfen vorerst ausschließlich die Notfalldaten einsehen. Die Datenübertragung von dem Kartenlesegerät in die Datenbank findet verschlüsselt statt. Weitere medizinischen Berufe sollen jedoch folgen, da der berechtigte Zugriffskreis für die medizinische Praxis relativ unrealistisch scheint. Beispielsweise sind in einer Apotheke meist nur ein oder zwei ApothekerInnen und mehrere Pharmazeutisch-Technische AssistentInnen (PTA) mit der Ausgabe von Medikamenten beschäftigt. PTAs würden da-

her nach geltendem Recht dazu gezwungen sein die Karte der ApothekerIn mitzunutzen um ihren Beruf weiter ausüben zu können.

Die Kosten werden sich nach Selbsteinschätzung der GesellschafterInnen auf 1,4 Milliarden Euro belaufen.

Wer stellt die Infrastruktur

Die Berliner gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH)[1] ist für die Entwicklung und Bereitstellung der Infrastruktur verantwortlich. Und diese ist nicht ganz ohne, wenn man bedenkt, dass 80 Millionen Versicherte mit der elektronischen Gesundheitskarte bestückt werden sollen. Zusätzlich sind da noch über 200.000 medizinische Angestellte, die sowohl mit Karten als auch mit den notwendigen Lesegeräten ausgestattet werden müssen. Diese werden voraussichtlich von den Krankenkassen finanziert werden, welche die Kosten mit Sicherheit auf die Versicherten abwälzen werden.

Als GesellschafterInnen der gematik GmbH fungieren die Bundesärztekammern, die Kassenärztlichen Bundesvereinigungen, die Deutsche Krankenhausgesellschaft und der Deutsche Apothekerverband. Die Kosten werden sich nach Selbsteinschätzung der GesellschafterInnen auf 1,4 Milliarden Euro belaufen[2]. Folgekosten sind zu erwarten. Die finanzielle Last soll der Staat tragen, welcher hofft, dass sich die Investitionen durch Einsparungspotentiale an anderen Stellen wieder auszahlen werden.

Schadenspotential der elektronischen Gesundheitskarte

Mit wachsenden Möglichkeiten steigen leider meist auch die Begehrlichkeiten. Dass die elektronische Gesundheitskarte durchaus in einigen Fällen wie beispielsweise bei Arzneimittelunverträglichkeiten Nutzen stiften kann ist unbestreitbar. Fraglich ist jedoch, wie dieser Nutzen im Verhältnis zu dem möglichen Schadenspotential dieser Neuerung steht.

Die Bundesärztekammer sieht sich durch die Verpflichtung eine online-Anbindung für die elektronische Datenverarbeitung der Behandlungsergebnisse einzuführen in ihrer Berufsfreiheit eingeschränkt. Durch die elektronische Erfassung von Rezepten könne, so die ÄrztevertreterInnen, die ärztliche Schweigepflicht mit wenig Aufwand umgangen werden. Durch die Analyse verordneter Medikamente kann leicht zurückverfolgt werden, mit welchen Beschwerden sich die/der PatientIn an die behandelnde Ärztin bzw. den behandelnden Arzt gewendet hat.

Bereits in der Testphase kam es zu zahlreichen Problemen sowohl von Seiten der ÄrztInnen als auch der PatientInnen. Ein vollständiger Systemausfall Anfang 2008 zeigte, dass das System bislang noch unausgereift ist. Die Entwicklungs- und Einführungskosten sind immens und es scheint daher fraglich, ob dies durch Einsparungen an anderen Stellen wieder ausgeglichen werden kann. Denn auch die Behandlungsabläufe werden durch die elektronische Erfassung komplexer und somit zeitaufwendiger und kostenintensiver werden. Es stellt sich auch die Frage, wie das auf einer PIN basierende System bei behinderten und pflegebedürftigen Menschen greifen soll. Auf dem Deutschen Ärztetag 2007 in Münster haben daher die Mehrheit der TeilnehmerInnen gegen die Einführung einer elektronischen Gesundheitskarte in ihrer derzeitigen Form gestimmt.

Wachsende Möglichkeiten schaffen leider oft auch wachsende Begehrlichkeiten. Unternehmen, Krankenkassen aber auch der Staat haben ein großes Interesse an unseren Patientendaten. Für Unternehmen könnte es beispielsweise finanziell äußerst reizvoll sein auf Krankendaten zugreifen zu können, da sie so »kostspielige« ArbeitnehmerInnen mit hohem Erkrankungsrisiko oder langer Krankengeschichte frühzeitig aussortieren können um ihre Ausgaben zu senken.

Privatunternehmen wären mit Hilfe der Datensätze in der Lage ihre Produkte genau auf die KundInnen abzustimmen, was besonders für Pharmakonzerne äußerst reizvoll sein wird. Krankenkassen wären mit diesen sensiblen Daten in der Lage »Risikokunden« mit höheren Beiträgen zur Kasse zu bitten.

Mit wachsenden Möglichkeiten steigen leider meist auch die Begehrlichkeiten.

FinanzdienstleisterInnen würden es sich bei einigen MitbürgerInnen genau überlegen, zu welchen Konditionen sie eine Versicherung oder einen Kredit anbieten wollen. Das Solidaritätsprinzip des Lastenausgleichs und der Risikostreuung, nach der Versicherungen heute funktionieren, würde ausgehebelt werden, wenn ein Zugriff auf die Daten ermöglicht wird. Bedenklich ist vor diesem Hintergrund vor allem die Ankündigung, dass der Zugriff der Patienten auf ihren Datensatz von Bankautomaten aus möglich sein soll.

Auch der Staat hat ein Interesse an unseren Daten. Zum Zwecke der Rasterfahndung, der »effizienteren« Gestaltung der Gesundheitsversorgung oder der Terrorbekämpfung.

Kritisiert werden sollte auch der Aufbau der Planung und die technische Realisation, welche unter Ausschluss der Öffentlichkeit statt findet. Ob das System wirklich zumindest minimalen Sicherheitsanforderungen entspricht lässt sich schwer sagen, da der Quellcode der Software bisher nicht offen gelegt wurde und dies in Zukunft auch nicht geschehen soll. Durch die zentrale Speicherung erhöht sich das Ausmaß des möglichen Schadens im Falle eines unerlaubten Zugriffs oder Verlustes der Daten immens. Einem System, welches derart unausgereift scheint, dessen Realisation sich bereits seit Jahren aufgrund von Problemen weiter hinausschiebt, soll nun mit den hoch sensiblen Krankendaten aller BundesbürgerInnen gefüttert werden. Verantwortungsbewusstes Handeln sieht anders aus.

Allen Sicherheitsmaßnahmen zum Trotze kann menschliches Versagen niemals vollständig ausgeschlossen werden. Durch Unachtsamkeit, Verlust oder eine strafbare Handlung einer zugriffsberechtigten Person könnte es passieren, dass die Daten in die Hände Dritter gelangen.

In falsche Hände wäre da noch eine weit untertriebene Formulierung, da das Schadenspotential eines Datenlecks immens ist. Die Offenlegung von Erbkrankheiten würde nicht nur unsere Generation, sondern auch die unserer Kinder schwer treffen. Ein derartiger Informationeller Supergau kann dann nicht mehr Rückgängig gemacht werden, wenn die sensiblen Daten erst einmal in die mediale Atmosphäre entwichen sind. Dabei geht es nicht nur um finanzielle Einbußen für die Betroffenen. Unfreiwillig als HIV-positiv infizierte, psychisch erkrankte oder als sonst wie gesundheitlich nicht der Norm entsprechend »geoutete« Menschen setzen sich der Gefahr einer Stigmatisierung aus. Wer argumentiert, er habe schließlich nichts zu verbergen und sehe daher auch keine Gefährdung durch eine elektronische Gesundheitskarte, sollte sein Blickfeld weiter spannen und auch das langfristige Schadenspotential nicht aus den Augen lassen. Denn ein wenig Solidarität hat bekanntlich noch niemandem geschadet.

Katharina Maria Nocun, Ak Vorrat Münster,
Referat für Datenschutz und Informationelle
Selbstbestimmung im Uni-AStA

Literatur

Broschüre des Grundrechtekomitees: www.grundrechtekomitee.de/ub_showarticle.php?articleID=222

Bericht von der Bundesärztekammer: www.bundesaerztekammer.de/downloads/111StenoWortbericht1.pdf

1 Die gematik: www.gematik.de

2 Link zur Kostenkalkulation: www.ccc.de/updates/2006/krankheitskarte?language=de

Die Plastikkarte kommt?!

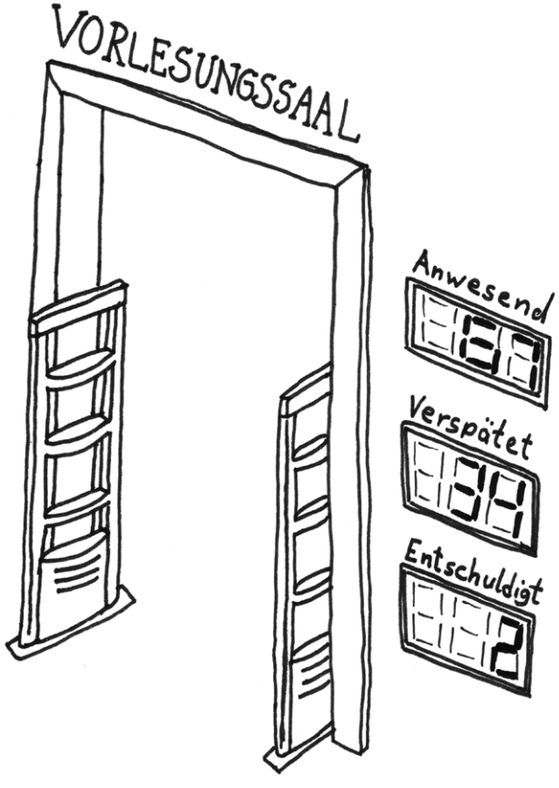
An fast allen deutschen Hochschulen gibt es Bestrebungen UniCards einzuführen, die potentiell den gesamten Unialltag regeln könnten. Auch an den Hochschulen in Münster wird in Arbeitsgruppen diskutiert, wie der Studierendenausweis modernisiert werden kann und welche neuen Funktionen integriert werden sollen. Problematisch dabei ist, dass darüber die Menge an personalisierten Daten massiv wächst und über die Verknüpfung verschiedener Daten umfassende Persönlichkeitsprofile möglich werden.

Am vierten Februar diesen Jahres verkündeten die Westfälischen Nachrichten (WN), dass das letzte Stündlein für den alten Studierendenausweis an der Uni Münster geschlagen habe und nach dem Willen der Uni möglichst zum Wintersemester 09/10 eine neue Plastikkarte im Geldbeutel der Studierenden seinen Platz beanspruchen würde.[1] Nachdem im Frühjahr 2007 die alten Kopierkarten mit der weiterhin bestehenden Mensakarte zusammen gelegt wurden, sollte die neue Karte über einen Barcode als Ausweis für die Unibibliothek, über ein austauschbares Hologramm als Semesterticket und über erweiterbare Funktionen auch als Bezahlchip in der Mensa dienen.[2] Alles was der WN dazu für die Studierenden einfällt ist, dass das »Studentenleben« praktischer werde.[3]

Diese Meldung erwies sich zwei Tage später als Presseente, als der Kanzler der Uni, Dr. Schwartze, nach einem Gespräch mit dem AStA in einer Pressemitteilung verkündete, dass die »Diskussion an der Universität Münster um die Ablösung des bisherigen Studentenausweises durch eine Plastikkarte läuft und (…) noch nicht entschieden oder abgeschlossen«[4] ist. Dennoch arbeitet eine Arbeitsgruppe unter Einbeziehung von VertreterInnen der Studierenden in einem »ergebnisoffenen Prozess« an der Einführung eines neuen Studierendenausweises. Bei dieser neuen Karte ist auch das Studentenwerk involviert. Auch die Fachhochschule Münster sowie die Kunstakademie haben Interesse signalisiert, wodurch fast 50.000 Studierende betroffen wären.

»Beinahe alle Hochschulen haben Projektgruppen eingesetzt mit dem Ziel der Optimierung von internen und externen Geschäftsprozessen«, was unter anderem zu einer »[k]undenorientierte[n] Optimierung der Verwaltungsabläufe« führen soll. Als Haupthindernis zur Umsetzung dieser Pläne gilt »die fehlende Chipkarte«[5]. Abgesehen davon, dass hier die Studierenden direkt als »Kunden« gesetzt werden, was die Bezahlung der in Anspruch genommen Dienstleistungen impliziert, wird hier deutlich, um was es bei der Einführung multifunktionaler Studierendenkarten geht: Die Studierenden- und Personalverwaltung soll effizienter und vor allem kostengünstiger gestaltet werden.

Die Studierenden- und Personalverwaltung soll effizienter und vor allem kostengünstiger gestaltet werden.



Dies wird den Studierenden dann verkauft als etwas, was »praktisch« sei[6], oder gar ein »mehr an Service« biete.

Und es funktioniert: immerhin gibt es an der Uni Listen, die sich der Wahl zum Studierendenparlament stellen und die brav eine »neue UniCard im Kreditkartenformat«, »in der alle Funktionen vereint sind« fordern. Damit wäre dann »endlich Schluss!« mit »dem Stück Papier als Semesterticket, der zusätzlichen Ausleihkarte für die ULB, der Mensakarte und dem weiteren Papierabschnitt, die alle zusammen Euer Portmonee überfüllen«. Irgendwie soll dieses »ganze(s) Uni-Leben im Kreditkartenformat« dann »praktischer, unkomplizierter und datensicherer« sein.[7] Während letztere Behauptung erst einmal amüsant und nicht wirklich nachvollziehbar ist, könnte der Rest dieser Forderung auch von dem Pressesprecher einer beliebigen Universität oder Fachhochschule kommen, der daran gleich die Erklärung anhängen würde, dass dies ja alles der Vereinfachung des Studiums und damit auch irgendwie der »Verbesserung der Lehre«[8] diene, was die Bezahlung aus Studiengebühren legitimieren könnte.

Betrachtet man die potentiellen Anwendungsmöglichkeiten einer Chipkarte genauer, wird der Slogan »Das ganze Uni-Leben im Kreditkartenformat« zur realen Möglichkeit: So könnte unter anderem die Anmeldung zu Praktika und Seminaren; Semesterrückmeldungen; Prüfungsanmeldungen; die Zahlung von Gebühren; die Teilnahme an Wahlen; der Zugang zu Labors, Räumen oder Arbeitsplätzen; der Bibliotheksbesuch und die Ausleihe von Büchern; das Arbeiten im Rechenzentrum und die Nutzung von PC-Pools; die Zugangsberechtigung für Wohnheime und Parkplätze; das Zahlen in der Mensa und vieles mehr über die Chipkarten geregelt werden.[9] Somit könnten die Universitäten jede Menge Geld darüber sparen, wenn sie – ganz kundenorientiert – die Arbeit der Verwaltung der Studierenden an diese selbst übertragen würde. Dabei ist es noch möglich, die Zinsen für das auf den Karten gespeicherte Geld zu kassieren und ganz nebenbei entsteht auch ein riesiger Datenberg.

Der lässt sich natürlich auch nutzen. Restriktiv über die Koppelung des BAföG sowie der Studienkredite an überprüfbare und auf der Karte gespeicherte Studienleistungen und die Kontrolle des Zugangs zu bestimmten Hochschulbereichen. Oder auch zur Erstellung umfassender Persönlichkeits- und Bewegungsprofile – beispielsweise darüber, welche Themen für Arbeiten gewählt und welche Bücher ausgeliehen wurden, wann und wo sich eine Person an der Hochschule aufgehalten hat, ob sie regelmäßig ihre Seminare besucht hat, was die Person in der Mensa isst… Darüber, dass Geld- und Verwaltungsdaten auf einem einzigen Chip gespeichert würden, sind alle diese Daten potentiell miteinander verknüpfbar und der/die gläserne Studierende Realität. Daneben ist auch vorstellbar, dass über Karten mit Bezahlfunktion auch Serviceleistungen abrechenbar werden, die derzeit umsonst verfügbar sind, da die Abrechnung über Bargeld zu aufwendig wäre.

Und die Studierenden? Die scheinen mit der bisherigen Regelung sehr zufrieden zu sein. Ohne den Ranking-Wahn affirmieren zu wollen, ist es doch aufschlussreich, dass bei den Rankings der kostenlosen Unizeitung Unicum die Uni Münster bei der Frage »Gibt es für die Hochschule ein einheitliches Kartensystem (Studentenausweis, Kopierkarte, Mensakarte, Bibliotheksausweis)?« vier von fünf möglichen Sternen[10] und die FH Münster viereinhalb[11] erhält. Einen größeren Verbesserungsbedarf scheint es für die HauptnutzerInnen also nicht zu geben.

Für die Hochschulen ergeben sich also mannigfaltige Vorteile: die Einsparung von Verwaltungskosten und die Möglichkeit neuer Einnahmen ebenso wie umfangreiche »Steuerungseffekte« auf die Studierenden. Daneben dürften auch die staatlichen Repressionsorgane wie Polizei und Geheimdienste ein Interesse an diesen Daten haben. Schon bei der unnützen, die Informationelle Selbstbestimmung der Studierenden missachtenden und verfassungswidrigen Rasterfahndung im Jahre 2001 wurde auf die Daten zugegriffen, die die Hochschulen über ihre Studierenden gesammelt hatten. Damals wurden allein in NRW 5,2 Millionen Datensätze von Einwohnermeldeämtern, dem Ausländerzentralregister und eben den Universitäten an die Polizei weitergeleitet.[12] Irgendwelche islamistischen TerroristInnen wurden dadurch nicht entdeckt.

Unklar ist noch, wie viel die Umstellung kosten wird und wer dies bezahlen soll.

Aber nicht jede UniCard ist gleich eine Chipkarte die über einen RFID-Chip[13] kontaktlos auslesbar ist. Möglich sind auch Lösungen, bei denen die Chips nur über ein Lesegerät auslesbar sind oder bei denen Daten nur mittels eines Barcodes gespeichert werden. Wichtig zur Unterscheidung ist auch, ob die Daten personenbezogen sind oder eben nicht. Bei der derzeitigen Mensa- und Kopierkarte der Uni Münster ist zwar nachvollziehbar, welche Karte wann was in der Mensa bezahlt und wo sie wie viele Kopien gemacht hat, aber nicht, wem diese Karte gehört. Die Bibliotheksausweise hingegen sind personalisiert, so dass die Universitätsverwaltung nachvollziehen kann, wer sich welche Bücher wie lange ausgeliehen hat.

An der Uni Münster gibt es nun, wie oben schon berichtet, eine »Arbeitsgruppe Studierendenausweis«, die mögliche Optionen für einen neuen Studierendenausweis erarbeiten soll. Dabei steht bisher lediglich fest, dass es eine Plastikkarte im Scheckkartenformat sein wird, es kein Bild auf der Karte geben wird, der bisherige Studierendenausweis dort eingebaut und der Bibliotheksausweis integriert werden soll. Unklar ist noch, wie viel die Umstellung kosten wird und wer dies bezahlen soll.[14] Ebenso unklar ist, ob der neue Studierendenausweis einen elektronischen Chip in sich tragen wird oder nicht. Während die meisten der Beteiligten dem eher ablehnend gegenüberstehen – beziehungsweise zum Teil nicht einmal wissen, wofür man diese neue Plastikkarte überhaupt brauchen soll – drängt das Rektorat auf einen elektronisch auslesbaren Chip.

Insgesamt sieht es demnach also nicht danach aus, als würden die oben skizzierten Horrorszenarien in Münster in absehbarer Zeit Wirklichkeit werden. Dennoch bleibt Vorsicht angebracht. Immerhin sind noch einige Fragen im Bereich der Finanzierung und des Datenschutzes offen.[15] Zudem werden auch in dem geplanten neuen Studierendenausweis neue Funktionen integriert und falls Kopier- und Mensakarte ebenfalls Teil davon werden würden, wäre ein nicht unwesentlicher Teil des Unialltags personalisiert geworden. Auch bleibt abzuwarten, wie stark das Rektorat auf den elektronischen Chip drängen wird und ob es sich gegen die anderen Beteiligten durchsetzen kann. Aufgabe der VertreterInnen der Studierenden in der »Arbeitsgruppe Studierendenausweis« bleibt es, kritisch nachzufragen, wie es denn mit dem Datenschutz aussieht und was man gegen die berechtigten Bedenken unternehmen wolle. Immerhin hat sich die Universität Münster bezüglich dieser Thematik in der Vergangenheit nicht gerade mit Ruhm bekleckert, es sei nur an die massenhafte Herausgabe von Daten im Rahmen der Rasterfahndung und die datenschutzrechtlich katastrophale Videoüberwachung erinnert. Aber auch ausserhalb der Arbeitsgruppe sollte dem Rektorat gezeigt werden, dass die Studierenden nicht gerade sehnsüchtig auf irgendwelchen teuren Schnickschnack mit bedenklichen Potentialen warten.

Und überhaupt könnte auch mal nachgefragt werden, was dieses ganze Prozedere denen, die es letztendlich wahrscheinlich bezahlen sollen, den Studierenden, überhaupt bringt und ob das überhaupt nötig ist. Schliesslich sollte nicht vergessen werden, dass gerne Karten mit wenig umstrittenen Funktionen eingeführt werden, um eine breite Akzeptanz zu schaffen, während die umstritteneren Funktionen zu geeigneter Zeit nachgerüstet werden.

So bleibt zu hoffen, dass die Frage der Einführung sowie die noch offenen Punkte von den VertreterInnen der Studierendenschaft möglichst unnachgiebig im Sinne der Studierenden verhandelt werden. Wer das ausserhalb dieser Arbeitsgruppe unterstützen will, ist in der Datenschutz und Freie Software AG (Kontakt: asta.datenschutz@uni-muenster.de) des Referats für IT und Datenschutz im AStA der Uni Münster sicher bestens aufgehoben.

Tim Ackermann

1 vgl. Völker, Karin: Die Plastikkarte kommt, in: Westfälische Nachrichten, 04.02.09.

2 vgl. ebd.

3 vgl. ebd.

4 Pressemitteilung des upm – Mediendienst der Universität Münster: Noch keine Entscheidung über Studentenkarte. »Ergebnisoffene Diskussion« an der Universität Münster geht weiter, 06.02.09.

5 beide Zitate: Haverkamp, Wilhelm und Jan von Knop 2001: E-Business in der Hochschule: Wirklichkeit, Vision und Voraussetzungen, S.155, verfügbar über: http://subs.emis.de/LNI/Proceedings/Proceedings09/E-BusininderHochsch_16.pdf, 15.04.2009.

6 vgl. Völker, Karin: Die Plastikkarte kommt, in: Westfälische Nachrichten, 04.02.09.

7 Alle sechs Zitate: Listenwerbung des RCDS, in: Semesterspiegel Nr. 378 November 08, S.11.

8 Wenn eine Maßnahme der »Verbesserung der Lehre« dient und nicht kompensatorischer Art ist – also kein bisher existierendes Angebot ersetzt – kann sie aus Studiengebühren bezahlt werden. Die praktischen Erfahrungen vieler Fachschaften an der Uni Münster, die sich an den Kommissionen zur Verteilung der Studiengebühren beteiligen, zeigen, dass beide Begriffe recht dehnbar sind.

9 Haverkamp, Wilhelm und Jan von Knop 2001: E-Business in der Hochschule: Wirklichkeit, Vision und Voraussetzungen, S. 165, verfügbar über: http://subs.emis.de/LNI/Proceedings/Proceedings09/E-Businin-derHochsch_16.pdf, 15.04.2009.

10 vgl. http://www.unicum.de/hochschulverzeichnis/Nordrhein-Westfalen/M%FCnster/Westf%E4lische_Wilhelms-Universit%E4t_M%FCnster, 20.01.2009.

11 vgl. http://www.unicum.de/hochschulverzeichnis/Nordrhein-Westfalen/M%FCnster/Fachhochschule_M%FCnster, 20.01.2009.

12 vgl. heise newsticker vom 23.05.06: Rasterfahndung nach 11. September 2001 verfassungswidrig, verfügbar über: http://www.heise.de/newsticker/Rasterfahndung-nach-11-September-2001-verfassungswidrig--/meldung/73430, 15.04.2009.

13 → Artikel: RFID

14 Alle Informationen dieses Absatzes stammen aus einer Mail von Hannes Papenberger, dem damaligen studentischem Mitglied der »Arbeitsgruppe Studierendenausweis«, vom 17.04.2009 an den Autor.

15 vgl. JusoHSG: Noch keine Entscheidung über Studierendenkarte – Kanzler rudert zurück, Meldung vom 09.02.2009.

Warum ist Privacy wichtig für die Demokratie?

Ein Mensch, der ständig beobachtet, registriert, vermarktet und von speziell auf ihn abgestimmte Vorschlägen und Angeboten begleitet wird, verändert mit der Zeit sein Verhalten und richtet es nach den Erwartungen derer aus, die seine Daten auswerten. Auf Individuen abgestimmte Manipulationsmöglichkeiten, die durch die zunehmende Erfassung zum Beispiel von Konsumverhalten und Bewegungsdaten sowie faktischer Anpassungsdruck führen zu einer zunehmenden Fremdbestimmung.

Dabei ist nicht nur zweckentfremdender Daten»missbrauch« möglich, vielmehr ist bereits der Daten»gebrauch« problematisch. Die Sammlung, Speicherung, Akkumulation, Kombination, Auswertung und Nutzung von vielen banalen Daten aus dem alltäglichen Leben – Informationen, die jeweils für sich gesehen keineswegs »geheim« sind – birgt somit bereits Gefahren für die Informationelle Selbstbestimmung. Werden diese Daten vernetzt, können sie zu weitreichenden Persönlichkeitsprofilen zusammengestellt werden. Anonyme Maschinerien, auf die die BürgerInnen keinen Einfluss haben, von deren Existenz sie oftmals nicht einmal wissen, ordnen sie nach Merkmalen und Verhaltensweisen in verschiedene Typisierungen ein[2] und sorgen dafür, dass sie fortan entsprechend der Typisierung behandelt werden. Von den Daten kann nicht nur abhängen, welche Werbung ihnen zugeschickt wird, sondern auch welchen Job, welche Versicherung, welche Wohnung sie bekommen – und ob überhaupt. So kann eine derartige Typisierung zu einer erheblichen Einschränkung der persönlichen Handlungsspielräume führen.

Wer sich dieser Datenerfassung nicht bewusst ist, tauscht sorglos Privatsphäre gegen Bequemlichkeit ein. Das Machtgefälle zwischen BürgerInnen und Verwaltung beziehungsweise zwischen VerbraucherInnen und Wirtschaft verstärkt sich. Merke: Der »mündige Verbraucher« wird von der Wirtschaft immer dann herbeizitiert, wenn er über den Tisch gezogen werden soll.

Da die Speicherung und Auswertung vieler Datenspuren für die BürgerInnen nicht transparent ist, und weil negative Folgen für die Individuen nicht direkt spürbar sind, sondern möglicherweise erst viele Jahre nach der Datenspeicherung auftreten und die Ursache oft nicht erkennbar ist, findet hier ein substantieller Kontrollverlust der Bürgerinnen und Bürger statt. Sie werden nicht unvoreingenommen in der Gegenwart betrachtet und auch nicht mehr gefragt, sondern sie werden auf Grundlage von Daten aus der Vergangenheit kategorisiert und gemäß einer Prognose für die Zukunft behandelt: Firmen interessiert in der Regel weder der Einzelfall noch die Wahrheit, es geht um Gewinnmaximierung im Gesamtergebnis.

Wer sich dieser Datenerfassung nicht bewusst ist, tauscht sorglos Privatsphäre gegen Bequemlichkeit ein.

Zur Disposition stehen vielmehr zunehmend Grundrechte, die nicht verhandelbar sind, sondern unverzichtbar.

Jede Bürgerin und jeder Bürger ist aber ein Einzelfall – ihnen gehen Handlungsoptionen und Entscheidungsfreiheit verloren. Wer die möglichen Folgen der Datensammelwut nicht kennt, wird zur Manövriermasse derer, die Zugriff auf die Daten haben und diese für sich verwerten. Wer sich hingegen bewusst ist, dass eben diese Art der Informationsauswertung stattfindet, wird sich bemühen, sein oder ihr Verhalten anzupassen. Das kann je nach Situation bedeuten: sich unauffällig (oder auch besonders auffällig) benehmen, die (vermutete) Erwartung des Beobachters erfüllen oder aber auch ausweichen, sich verbergen, sich nicht äußern, anonym bleiben, lügen.

Wer sich aber laufend beobachtet fühlt, wird nicht nur in der freien Entfaltung der Persönlichkeit behindert, sondern nimmt auch von der Verfassung garantierte Rechte wie freie Meinungsäußerung und Versammlungsfreiheit möglicherweise nicht mehr in Anspruch. So zerstört der Verlust der Informationellen Selbstbestimmung die Fähigkeit zur Kommunikation und zur Partizipation. So gehen die Ideen, Meinungen und Talente dieser Menschen nicht mehr in die Allgemeinheit ein und damit auch das Engagement für etwas, das über die eigenen Interessen hinaus geht, für die Gesellschaft verloren.

Hier geht es also keineswegs nur um private Bedürfnisspielräume, die jeder ohne Schaden für sich selbst aushandeln könnte. Zur Disposition stehen vielmehr zunehmend Grundrechte, die nicht verhandelbar sind, sondern unverzichtbar für Gemeinwohl und Demokratie.

Warum nicht den Datenschutz dem freien Markt überlassen?

Von Seiten der Wirtschaft wird oft das Argument vorgetragen, die Menschen seien doch mündige Verbraucher und könnten selbst entscheiden, was sie wollen. Im Folgenden einige Gründe, warum das mit dem selbständigen Aushandeln der Datenschutzbedingungen zumeist nicht klappt.

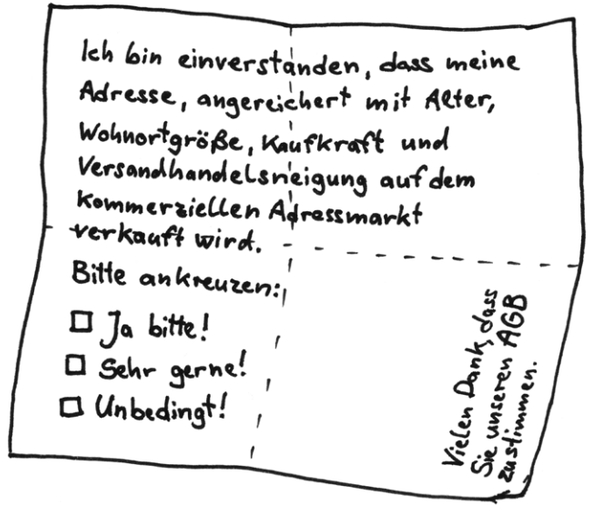
- Die VerbraucherInnen haben keine oder nur sehr rudimentäre Information über mögliche langfristige Folgen.
- Die Vertragsbedingungen, denen sie zustimmen sollen, sind meist völlig unlesbar. Es ist schlicht nicht zumutbar, erst seitenlange, in Juristensprache verfasste AGB kritisch zu lesen, um zum Beispiel eine Bestellung aufzugeben.
- Oft wird eine Irreführung der VerbraucherInnen auch mehr als billigend in Kauf genommen. Welcher Verbraucher ahnt schon, dass »Ihre Daten werden vertraulich behandelt, sie werden grundsätzlich nicht an unberechtigte Dritte weitergegeben.« keineswegs heißt, dass die Daten nicht weitergegeben würden. Sondern vielmehr, dass das zwar »grundsätzlich« so ist, aber das

»grundsätzlich« keine Verstärkung der Aussage ist, sondern bedeutet, dass es Ausnahmen gibt, und zwar bei »berechtigten« Dritten. Und dass berechtigte Dritte diejenigen sind, die die Adresse auf dem Adressmarkt, angereichert mit Alter, Wohnortgröße, Kaufkraft und »Versandhandelsneigung« kaufen. So geschehen bei Tchibo direct[3], die die Daten ihrer KundInnen über AZ direct, Arvato, Bertelsmann zum Kauf anbieten. Diese »Ausnahme« ist übrigens die Regel – fast alle Versandhandelsunternehmen »vermieten« oder verkaufen die Adressen ihrer Kunden. An diesem Beispiel einmal durchexerziert: Damit die Verbraucher verstehen, um was es geht, müsste der Vertragstext etwa so lauten (Wie viele da wohl »ja« ankreuzen würden?):

»Ich bin einverstanden, dass meine Adresse, angereichert mit Alter, Wohnortgröße, Kaufkraft und Versandhandelsneigung auf dem kommerziellen Adressmarkt verkauft wird.«
Hier ankreuzen, falls ja.

» Oder wer weiß, dass die »Informa Unternehmensberatung«, mit der viele Direktbanken laut ihrer Vertragsbedingungen Daten austauschen, keine Unternehmensberatung ist, sondern ein Scoring-Unternehmen?
» Verbraucher verlassen sich in Deutschland a) auf die Gesetze, b) darauf dass, wenn etwas schief geht, sich schon irgendeine Institution für sie darum kümmern wird. (Also erst einmal fleißig Rabatt in Anspruch nehmen und sich dann bei den Datenschutzbeauftragten oder bei den Big Brother Awards zu beschweren.)
» Und: Der einzelne Verbraucher verhält sich zunächst einmal egoistisch und keineswegs so, wie es für die Gesamtheit der Verbraucher von Vorteil wäre. Langfristig ist das ein Nachteil auch für den einzelnen.
» Divide et impera. (Teile und herrsche) Solange die negativen Folgen nur andere betreffen, ist alles egal. (Es geht ja nur um Terroristen, Sexualstraftäter, Schwarzfahrer, Arbeitslose oder auch nur um die nervigen LKWs auf der Autobahn etc., das betrifft mich also nicht oder es nützt mir vielleicht sogar.) Diese Haltung hat Martin Niemöller in seinem bekannten Zitat [4] gut charakterisiert.
» Das Sein bestimmt das Bewusstsein: Solange jemand eine Senator Card von der Lufthansa hat und als »A-Kundin« hofiert wird, findet sie das »Miles and More«-Konzept toll. Wenn sie ihr entzogen wird, weil Lufthansa mitbekommen hat, dass sie wegen Jobwechsel nicht mehr soviel verdient, findet sie das System plötzlich nicht mehr so gut.

Im Tante-Emma-Laden bin ich bekannt und man weiß dort, was ich gerne einkaufe. Aber ich kenne meinerseits eben auch Tante Emma.



» Die Argumentation mit dem Eigentumsbegriff (»Meine Daten gehören mir!«) hat sich als nicht hilfreich herausgestellt. Denn die Wirtschaft argumentiert, dass die einzelne Adresse nichts wert sei, kostbar werde eine Adresse erst dadurch, dass sie mit weiteren Informationen angereichert und mit anderen Adressen mit ähnlichen Merkmalen zusammengestellt wird.

Was ist der Unterschied zwischen dem Bekanntsein im Tante Emma Laden und der Payback-Karte?

Das ist ähnlich wie der Unterschied zwischen einem Polizisten, der Streife geht, und einer Videoüberwachung. Zum einen ist es eine Frage der Gegenseitigkeit. Im ersten Fall ist eine Person das Gegenüber, im anderen eine anonyme technische Struktur, wo verborgen bleibt, was eigentlich passiert. Bei einer Videokamera ist völlig unklar, ob sie funktioniert, wer auf den Monitor guckt, ob die Kamera in meine Richtung schaut, ob jemand am Monitor gerade auf meinen Ausschnitt zoomt oder auf das Buch, das ich auf der Parkbank lese. Guckt überhaupt jemand? An wie viele Stellen gleichzeitig wird übertragen? Wird aufgezeichnet? Wie lange wird die Aufnahme aufbewahrt? Wer hat Zugriff darauf? Und so weiter.

Im Tante-Emma-Laden bin ich bekannt und man weiß dort, was ich gerne einkaufe. Aber ich kenne meinerseits eben auch Tante Emma. Bei einer Kundenkarte liefere ich jedes Mal meinen kompletten Einkaufszettel ab, es ist unklar, wer diese Daten verarbeitet, wie lange sie aufbewahrt werden und wer welche Schlussfolgerungen aus ihnen zieht.

Wer in den 90ern häufiger besonders billiges Rindfleisch im Sonderangebot gekauft hat – und wir nehmen jetzt mal an, es hätte zu dieser Zeit schon Kundenkarten à la Payback gegeben – könnte so möglicherweise heute kein Angebot mehr für eine günstige Krankenversicherung bekommen, denn die möchte das Risiko einer Creutzfeld-Jacob-Erkrankung ausschließen. Dabei war das Fleisch für den Hund bestimmt, der längst in den ewigen Jagdgründen weilt – aber danach wird nicht mehr gefragt.

Tante Emmas Gedächtnis ist dagegen nicht ganz so gut und sie hat auch keinen Kontakt zu Krankenkassen, die mir ein Angebot machen wollen.

Der Unterschied liegt in der fehlenden Gegenseitigkeit, im Machtgefälle zwischen Mensch und anonymer Struktur, der fehlenden Transparenz und in der Dimension.

Rena Tangens gründete mit padeluun 1987 den FoeBuD e.V. und engagiert sich für Datenschutz, Bürgerrechte und eine lebenswerte Zukunft im digitalen Zeitalter. Dieser Text ist ein Auszug aus einem längeren Artikel. Diesen kann man auf der Homepage des FoeBuD e.V. nachlesen: www.foebud.org/datenschutz-buergerrechte/linsengericht

1 Linsengericht bezeichnet im übertragenen Sinne eine momentan verlockende, in Wahrheit aber geringwertige Gabe im Tausch für ein sehr viel höherwertiges Gut. Hintergrund dieser Bedeutung ist die biblische Erzählung (1. Buch Mose 25:29–34), derzufolge Jakob, der jüngere Sohn Isaaks, seinem älteren Bruder Esau dessen Erstgeburtsrecht angeblich gegen einen Teller Linsen abkaufte, als Esau von der Feldarbeit erschöpft heimkehrte.

2 Zum Beispiel beim sogenannten Scoring-Verfahren: Hier wird aus einer Vielzahl von persönlichen Daten, unter anderem Alter, Bundesland, Stadt, Wohnviertel, Nachbarschaft, Anzahl Umzüge, deren genaue Kombination aber nicht offen gelegt wird, für jede/n Bürger/in ein »Score« ermittelt – eine Zahl, die Auskunft über die Kreditwürdigkeit der Person gibt. Scoring ist ein automatisiertes Vorurteilssystem.

3 Tchibo erhielt dafür 2004 den Big Brother Award in der Kategorie Verbraucherschutz.

Mein virtuelles Leben

oder was wir aus StudiVZ so alles erfahren können

Die Studierenden von heute nutzen fast täglich das Internet. Die neuen Verwaltungsstrukturen der Uni zwingen uns quasi dazu. Denn ob nun Prüfungsanmeldung oder Vorlesungsskripte – fast alles steht im Netz zum Download bereit. Daher verbringen wir in der Bibliothek und daheim und überhaupt auch immer wieder Zeit am Rechner. Viele von uns schweifen dann gerne ab in die Tiefen von virtuellen sozialen Netzwerken wie Myspace, Facebook oder dem allseits beliebten StudiVZ. Wir, das sind genauer gesagt über 5 Millionen NutzerInnen mit steigender Tendenz.

StudiVZ und sein Profil

StudiVZ sei eine großartige Möglichkeit innerhalb des verstaubten Unialltags mal abschweifen zu können, Kontakte zu halten und Menschen kennen zu lernen, so die BetreiberInnen. Bis vor kurzem dachte auch ich, dass nichts dabei sei, all meine Hobbies und Freundschaften quasi öffentlich zu pflegen. Zu verbergen habe ich ja schließlich nichts. Dann jedoch, als im Dezember 2007 das StudiVZ medienwirksam seine Allgemeinen Geschäftsbedingungen, kurz AGB, änderte, schaute ich mir diese einmal genauer an und und wurde dann doch etwas nachdenklicher, was meine Privatsphäre betrifft.

Durch die neuen AGB wird es den BetreiberInnen der kommerziellen Onlineplattform, die sich ausschließlich über Werbung finanziert, ermöglicht, die Werbebotschaften an ihre KundInnen anzupassen. So lässt sich der Platz für ein Banner zu weitaus höheren Preisen an Unternehmen verkaufen, da personalisierte Werbung durchschnittlich weitaus höhere Klickzahlen durch die NutzerInnen provoziert. StudiVZ behält sich des Weiteren vor, meine Zugriffszeiten und Informationen über meinen verwendeten Browser zu speichern. Das heißt, StudiVZ merkt sich sechs Monate lang von welchem Rechner aus ich ihre Seite aufgerufen habe. Mein Klickverhalten wird durch spezielle Programme analysiert, um zu ermitteln, welchen Seiten innerhalb der Community ich mich mit Vorliebe zuwende. Meine persönlichen Angaben, meine Uni samt Fachrichtung sowie meine Hobbies, mein Wohnort und meine Gruppenmitgliedschaften dürfen dazu verwendet werden, Werbung noch besser auf mich zuschneiden zu können. Werbebotschaften dürfen jederzeit an mich übermittelt werden, wenn ich diesem Punkt der AGB nicht ausdrücklich widerspreche. Als hätte ich nicht bereits im realen Leben mehr als genug Werbung ins Altpapier befördern müssen. Falls der Staat aus Gründen der inneren Sicherheit meine Daten benötigt, werden diese selbstverständlich freundlicherweise von den BetreiberInnen weitergereicht. So weit so gut. Oder auch doch nicht.

Ich möchte nicht,
dass ich zum
gläsernen User werde.

Nach öffentlichen Protesten und der Reaktion zahlloser besorgten NutzerInnen, die ihre Namen in Arno Nymus oder Studentin umänderten, räumten die BetreiberInnen ein

sogenanntes Opt-Out Verfahren ein. Dies bedeutet für die NutzerInnen, dass sie, um Mitglied der Community zu bleiben, erst einmal den neuen AGB zustimmen müssen und dann anschließend die Möglichkeit haben die Nutzung der personenbezogenen Daten zu Werbezwecken wieder zu unter-

Denn schließlich muss nicht jeder wissen was wann mit wem geht. Es reicht mir ganz wenn ich es weiß.

sagen. Eine ziemlich kundenunfreundliche Vertragskonstruktion, wie ich finde, welche darauf abzielt, dass die Mehrheit aus Nachlässigkeit oder Desinteresse nicht auf die Änderung reagiert und somit personalisierter Werbung unbewusst zustimmt.

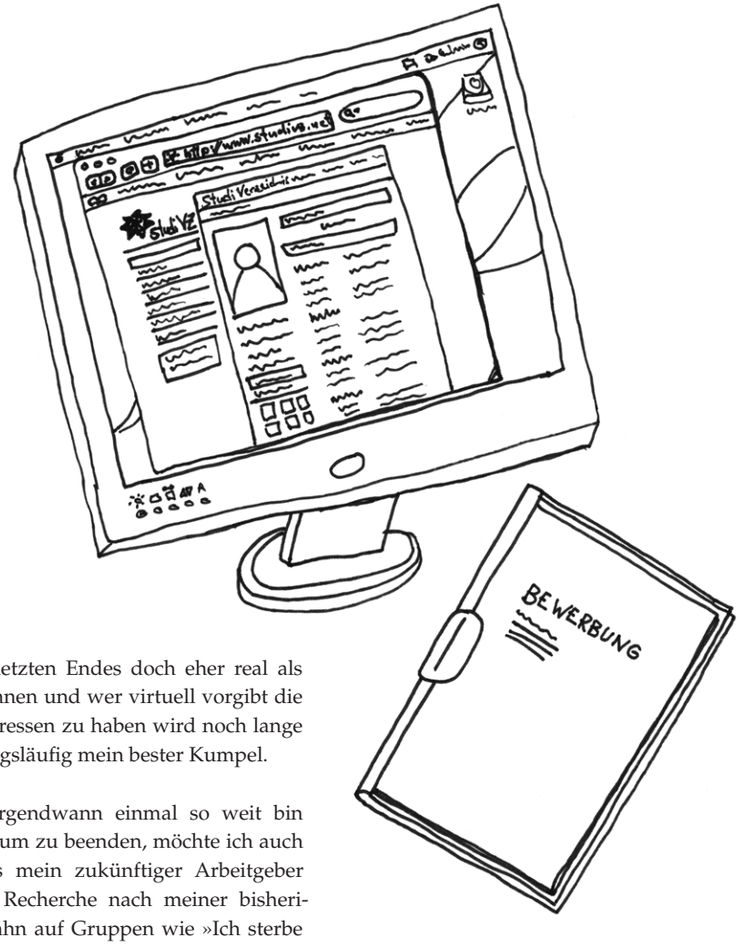
Deine ganz persönlichen Banner, Popup, Spam

Ich selbst stufe mich zwar nicht als kaufwütig ein, dazu fehlt mir seit der Einführung der Studiengebühren allein die nötige Kohle, aber trotz allem bin ich nicht gegen alle Versuchungen des Geldausgebens gefeit. Es geht mir ums Prinzip. Für mich ist Werbung kein interessantes Produktangebot, denn dazu ist sie nicht objektiv genug und sie ist auch nicht unterhaltsam oder witzig. Meistens nervt sie einfach nur und bewegt mich dazu, mir Dinge zu kaufen, die ich nicht brauche, denn wenn ich sie wirklich gebraucht hätte, wäre mir das ja wohl schon längst ohne Werbung in den Sinn gekommen. Letztendlich kann die mit Personalisierung einhergehende Kategorisierung und Klassifikation von Menschen auch zu ganz anderen Zwecken genutzt werden. Ich möchte nicht, dass ich zum gläsernen User werde. Denn ich selbst sehe für mich in personalisierter Werbung und der für diese notwendige Erfassung meines Verhaltens mehr Nach- als Vorteile.

Im Zuge der neuen AGB-Einführung habe ich noch ein wenig mehr über StudiVZ nachgedacht und bin zu dem Ergebnis gekommen, dass ich durch diese Plattform keine neuen Freunde gefunden habe – Womit im Übrigen einmal mehr bewiesen wäre, dass Werbung nicht immer ihr Wort hält. In meiner »Freundesliste« sind ehrlich gesagt lauter Menschen, die ich zuletzt zu Schulzeiten gesehen habe und mit denen ich abseits der Freundschaftseinladung und periodischen Gruschelattacken nichts am Hut habe. Wer meine Freunde sind merke ich nicht an Gästebucheintragungen, sondern an gemeinsamen Erlebnissen und Gesprächen.

Virtuelle best friends

Mir ist es unangenehm, wenn fremde Menschen Dinge über mich wissen, die ich ihnen nicht bewusst mitgeteilt habe. Wenn sie meinen Musikgeschmack auf die drei Bands in meiner Liste reduzieren, wenn sie glauben Sympathien zu erwecken wenn sie mein »Lieblingsbuch« auch so unglaublich toll finden. Dieser Umstand ist bei Privatunternehmen natürlich um einiges unangenehmer als bei Privatmenschen. Allerdings ist beides ehrlich gesagt nicht gerade der Knüller. Man



lernt sich letzten Endes doch eher real als virtuell kennen und wer virtuell vorgibt die selben Interessen zu haben wird noch lange nicht zwangsläufig mein bester Kumpel.

Falls ich irgendwann einmal so weit bin mein Studium zu beenden, möchte ich auch nicht, dass mein zukünftiger Arbeitgeber bei seiner Recherche nach meiner bisherigen Laufbahn auf Gruppen wie »Ich sterbe an Lungenkrebs und Leberzirrhose« stößt und sich daraufhin trotz meines gepflegten Erscheinungsbildes gegen mich entscheidet. Einer Lehrerin in den Vereinigten Staaten wurde ein Halloweenfoto, welches sie in einem Piratenkostüm mit einem Getränk in der Hand zeigte, zum Verhängnis. Ihr wurde gekündigt.

Und vielleicht stößt die Bundespolizei ja eines Tages doch noch auf das Kifferfoto, auf dem ein Bekannter von mir verlinkt ist und findet mich auch gleich mit verdächtig – Schließlich sind wir ja offiziell »befreundet«. Außerdem möchte ich Stalking, ob nun von staatlicher, wirtschaftlicher oder auch privater Seite nicht noch weiter vereinfachen.

Ich habe nichts zu verbergen, außer meiner Privatsphäre und meinem Recht auf Informationelle Selbstbestimmung. Daher gebe ich bei meinen Lieblingsfilmen nur noch »schwarz-weiß und auch in Farbe« und bei Hobbies »Atmen« an. Denn Falschangaben können laut Geschäftsbedingungen mit Geldstrafen geahndet werden und dies möchte ich doch tunlichst vermeiden.

Katharina Maria Nocun, Ak Vorrat Münster,
Referat für Datenschutz und Informationelle
Selbstbestimmung im AStA der Uni Münster

Fiberglas

Wie jede andere, ruhmgeile Diva habe auch ich gerne Fans, die mir mitteilen, wie toll sie mich finden. Bevor ich zum ersten Mal im WDR lief bekam ich schon dann und wann mal eine nette e-Mail oder eine Nachricht in irgendwelchen web2.0-Internetforen von Leuten, die mich mal auf einer Bühne gesehen haben und irgendeinen Text als besonders hörenswert empfunden haben. Solches Feedback finde ich natürlich nett. Dann habe ich hier im WDR einen Text gegen Schäubles Fibertraum von einem tollen Überwachungsstaat erzählt, und ja, der kam von Herzen und ja, ich war wirklich in Afrika. Nachdem dieser Text über den Äther geschickt wurde passierten zwei Dinge:

Erstens steht jetzt immer ein Lieferwagen mit verdunkelten Scheiben vor meinem Haus und es knistert in meinem Handy wenn ich telefoniere, bin also wohl zum Staatsfeind geworden, und zweitens haben sich die Mails von irgendwelchen Menschen an mich vervielfacht, bin also zum Randgruppenliebling geworden oder so. Eine dieser Mails möchte ich jetzt mal zitieren: »Total toll dass sich endlich mal jemand öffentlich gegen diesen Überwachungswahn einsetzt! Was man so macht geht doch echt mal keinen was an, da bekommt man ja richtig Angst. Ich steh auf (für) Dich, Stefanie«.

Für Stefanie ist dieser Text.

Stefanie Hitzer! Du wurdest am 6. Dezember 1984 in Recklinghausen geboren und studierst jetzt soziale Arbeit in Greifswald. Ich kenne all deine Lehrveranstaltungen. Deine Haare sind blond, deine Augen grünbraun und du bist 1,68 groß. Deine Lieblingsbücher sind Säulen der Erde und die Päpstin, deine Lieblingsfilme sind Crank, Adams Äpfel und Mikrokosmos. Du zitierst gerne Woody Allen. Du hast Angst vor Spinnen und Verweigerst das Bezahlen der Rundfunkgebühren. Das ist nur ein Ausschnitt deiner StudiVZ-Informationen. All diese Information bestätigst du bei myspace unter deinem tollen Nickname MissBeautyStar, nur erfahren wir hier noch viel mehr über Dich. Täglich berichtest du per bulletin, was du am Tag gemacht hast und was du am Abend vor hast. Du warst beispielsweise am 4. März beim Friseur, hast dir schwarze Strähnen machen lassen. Die Fotos bewiesen es noch am selben Tag. Seit dem 18. Dezember 2007 bist du Single, hast seitdem mit sechs Typen geknutscht, die meisten sahen deinem Exfreund ziemlich ähnlich. Du scheinst mehr wert auf Frisuren als auf Augenfarbe zu legen, alle hatten schwarze Haare, aber die unterschiedlichsten Augenfarben. In einem Erste-Hilfe-Forum für Geschlechtskrankheiten informierst du dich unter dem selben Nicknamen darüber, wie am besten mit einem Scheidenpilz zu verfahren sei. Dein Profil in dem Forum bestätig erneut deinen Namen und dein Geburtsjahr. Die Scheidenpilzanfrage kam genau drei Tage, nachdem du mit dem 4. Typen was hattest. Da hat also jemand nicht aufgepasst. Nebenbei kiffst du. Du sagst es nirgendwo explizit, bravo, aber bei Youtube sehen wir dich, wie du einmal mit deinem Exfreund zusammen eine Bong rauchst und ein anderes Mal auf einem Festival eine Tüte drehst. Du hast die Videos selbst hochgeladen. Soll ich weitermachen? Du wählst SPD, arbeitest neben dem Studium in eine Café für 7,20 die Stunde und konntest, was Dich geärgert hat, nicht zum ManuChao-Konzert, weil du arbeiten musstest. Ich könnte mehrere Stunden referieren, was du alles gemacht hast.

Was man so macht geht doch keinen was an, sagst du. Stimmt.

Aber warum reibst du es dann täglich jedem, der es nicht wissen will, brühwarm unter die Nase?

Liebe Stefanies und Stefans und wie ihr heisst, was ist kaputt bei Euch? Wenn ihr einen Pilz irgendwo habt, dann geht doch einfach zum Arzt! Der darf es nicht weiter erzählen. Sucht Euch Freunde, die mit Euch reden. Die ganze Welt ist bestimmt nicht euer Freund. Wenn ihr meint, dass der gläserne Mensch zerbrechlich ist, warum ersetzt ihr dann Tag für Tag für Tag eure schöne Haut durch Fieberglas?

Liebe Grüße, Genosse Strauß

Andy Strauß
www.establishmensch.de

Wer wann mit wem kommuniziert
die Vorratsdatenspeicherung schreibt mit

Kommunikation stellt einen maßgeblichen Teil unseres Lebens dar, denn immerhin ist der Mensch ein soziales Wesen, welches sich gerne anderen mitteilen möchte. Die durchschnittliche BundesbürgerIn nutzt tagtäglich mehrfach Telefon, Handy und womöglich auch das Internet, um sich mit ihren Mitmenschen zu verständigen. Ohne moderne Kommunikationsmedien könnte vieles in Gesellschaft, Wirtschaft, aber auch im privaten Bereich nicht ohne weitere Komplikationen abgewickelt werden – denn wir sind abhängig von diesen Medien.

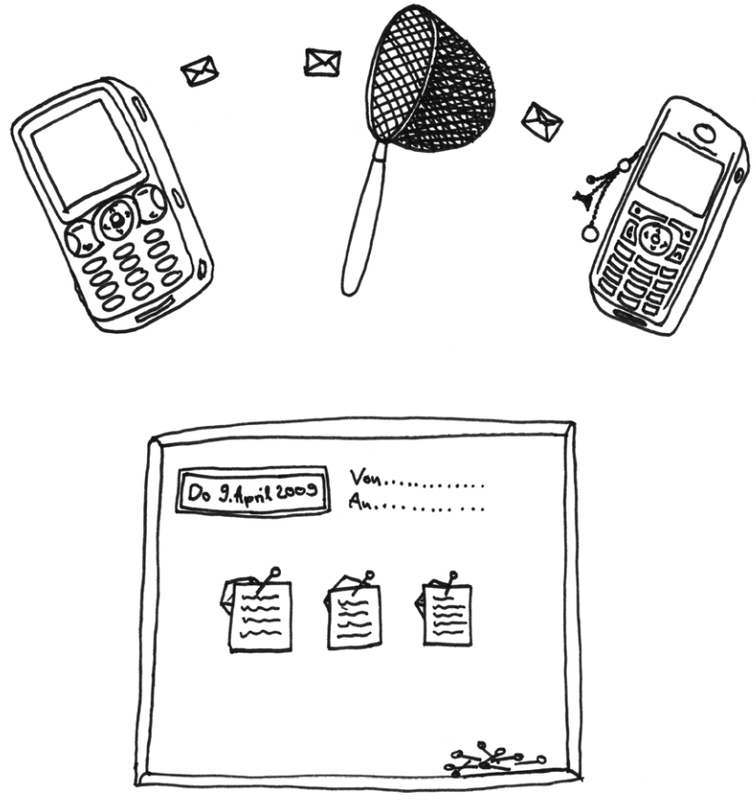
Seit dem 9. November 2007 haben sich jedoch die gesetzlichen Rahmenbedingungen für unser aller elektronische Kommunikation verändert. Denn wer wann mit wem auf elektronischem Wege kommuniziert wird nun protokolliert, und das auf Anordnung des Gesetzgebers.

Spätestens seit Januar 2009 müssen die Telekommunikationsanbieter sechs Monate lang speichern, von welchen Telefonnummern wann wer angerufen worden ist, von welcher IP-Adresse an welche IP-Adresse eine Nachricht versendet worden ist und bei Handyverbindungen wird noch zusätzlich der Standort der BenutzerInnen festgehalten. Dieses Verfahren nennt sich Vorratsdatenspeicherung und hat vielerorts kontroverse Diskussionen um Bürgerrechte »in Zeiten des Terrors« ausgelöst.

Die Umsetzung der auf europäischer Ebene beschlossenen Richtlinie 2006/24/EG zur Vorratsdatenspeichrung ist bei vielen Bürgerrechtsorganisationen nicht gerade auf Gegenliebe gestoßen. Denn Datensammlungen über das Kommunikationsverhalten der europäischen Bevölkerung bedeuten nicht nur eine Einschränkung der Grundrechte für die Betroffenen – sie wecken auch Begehrlichkeiten. Wo Daten anfallen, besteht natürlich auch früher oder später die Gefahr, dass sie auch benutzt werden. Es stellt sich dabei vor allem die Frage wofür und mit welcher Zielsetzung.

Man mag sich nun fragen, wofür der Staat derartige Datenberge über unser Kommunikationsverhalten horten möchte. Und es ist wohl so, dass sich die Behörden und Politiker davon eine Verbesserung der Strafverfolgungsmöglichkeiten versprechen. Es hat sich jedoch anscheinend gezeigt, dass diese Daten lediglich bei 0,006 % der Verfahren positiv zu der Aufklärung von Ermittlungsverfahren beitragen, so jedenfalls Vertreter des Arbeitskreises Vorratsdatenspeicherung. Das heißt, dass mindestens 99% der Bevölkerung vollkommen zu Unrecht überwacht werden. Das heißt auch, dass die TelekommunikationsanbieterInnen ohne jeden tieferen Zweck dazu gezwungen werden, sechs Monaten lang riesige Datenberge anzuhäufen. Für diese bedeutet das eine finanzielle Belastung, welche selbstverständlich an uns, ihre KundInnen, weitergegeben wird. Ganz davon abgesehen sind Verbindungsdaten allenfalls einem Anschluss und nicht einer konkreten Person zuordnbar – was ihre Beweis- und Aussagekraft stark einschränkt.

Aber die Ineffizienz dieser Maßnahme und die hierdurch produzierten Kosten sind es nicht, die Bürgerrechtsorganisationen die



Tränen in die Augen treiben. KritikerInnen sehen darin eine Einschränkung der Informationellen Selbstbestimmung und einen Eingriff in die Sphäre persönlicher Lebensgestaltung der europäischen Bevölkerung.

Letztendlich muss man sich auch die Frage gefallen lassen, inwiefern es förderlich für eine demokratische verfasste Staatsordnung sein kann, die eigene Bevölkerung derart zu überwachen. Denn aus Verbindungsdaten lassen sich nicht zuletzt soziale, politische und wirtschaftliche Netzwerkstrukturen rekonstruieren. Vor allem politisches Engagement könnte hierdurch leichter überwacht werden. Aber auch Berufsgruppen wie AnwältInnen, JournalistInnen, ÄrztInnen, Geistliche sowie soziale und ärztliche Anlaufstellen kritisieren die Maßnahme. Denn die Kontaktaufnahme allein lässt in einem bestimmten Kontext Rückschlüsse auf die Art der stattgefundenen Kommunikation zu. Man wird ja schließlich nicht grundlos mitten in der Nacht beim psychologischen Notdienst angerufen haben. Und die InformantIn, welche brisante Informationen aus Regierungskreisen an die Presse weitergeleitet hat, wäre dann auch schneller gefunden. Die Frage ist und bleibt dabei: sollte eine Demokratie derartiger Kontrollstrukturen bedürfen, die ihre BürgerInnen unter Generalverdacht stellt? Der Arbeitskreis Vorratsdatenspeicherung unterstützt daher eine Verfassungsbeschwerde gegen den Datenhunger der Behörden. Eine Entscheidung steht noch aus.

Katharina Maria Nocun, Ak Vorrat Münster,
Referat für Datenschutz und Informationelle
Selbstbestimmung im AStA der Uni Münster

Lächeln für das Gruppenfoto?

Aufnahmen von DemonstrationsteilnehmerInnen

Das Recht, an Demonstrationen teilzunehmen, und somit seine politische Meinung auch außerhalb der regelmäßigen Wahlen kundzutun, gehört zu unseren Grundrechten innerhalb einer Demokratie. Das ist richtig und wichtig, denn ohne dieses Grundrecht hätte die Bevölkerung kaum Möglichkeiten, ihrem Willen während der Legislaturperioden Ausdruck und Nachdruck verleihen zu können.

Teil einer streitbaren Demokratie sollte auch immer eine politisch interessierte und aktive Bevölkerung sein, die sich zwischen den Wahlen nicht einfach zurücklehnt und alle Entscheidungen, die von ihren gewählten RepräsentantInnen getroffen werden, willenlos, gleichgültig und somit politikverdrossen hinnimmt. Vielmehr sollte die Bevölkerung dazu angehalten werden sich aktiv an der Politik zu beteiligen. Sei es nun durch Parteiarbeit, durch ehrenamtliches Engagement in Nichtregierungsorganisationen oder aber durch die Teilnahme an Demonstrationen.

Was jedoch im Einzelfall »erhebliche Gefahren« sind, ist natürlich ein durchaus dehnbarer Begriff.

Wenn man sich dazu entschließt, für seine Meinung friedlich auf die Straße zu gehen, rechnet man nicht damit, dass es für einen selbst negative Konsequenzen haben könnte. Schließlich leben wir in einer Demokratie, denkt man sich doch. Schließlich ist es ein Recht, von dem man Gebrauch macht. Was aber, wenn die Polizei während Demonstrationen filmt und fotografiert? Was geschieht mit diesen Aufnahmen und welche Konsequenzen kann dieses für die Freiheit des Einzelnen haben?

Wann darf gefilmt werden?

Das Versammlungsgesetz nennt uns sehr detailliert die gesetzliche Grundlagen, die sich mit Demonstrationen befassen.

Der Paragraph 12 sagt uns: »Die Polizei darf Bild- und Tonaufnahmen von Teilnehmern bei oder im Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen.« Wenn eine Demonstration angemeldet und nicht verboten wird, dann werden diese Anhaltspunkte wohl kaum im Vorfeld gegeben sein, schließlich hätte man sie sonst nicht zugelassen, kann man argumentieren. Was jedoch im Einzelfall »erhebliche Gefahren« sind, ist natürlich ein durchaus dehnbarer Begriff.

Im konkreten Beispiel der Demonstration »Freiheit statt Angst« im Oktober 2008 in Berlin stellte dies ein Aufruf auf einer Internetseite mit der Aufforderung zu »konkreten Aktionen gegen Überwachungskameras« dar. Somit war das Filmen und Fotografieren tausender Demonstrationsteilnehmer dadurch gerechtfertigt worden, dass Einzelne zu Akten der Sachbeschädigung aufgerufen haben. Ein Aufruf, welcher – wohlgemerkt – nicht befolgt worden ist.

Natürlich könnte man sich auch einfach eine Kapuze über den Kopf und einen Schal übers Gesicht ziehen. Dann jedoch macht man sich wiederum strafbar.

Was geschieht mit den Aufnahmen?

Was passiert jedoch anschließend mit diesen Aufnahmen? Im zweiten Absatz heißt es weiter: »Die Unterlagen sind nach Beendigung der öffentlichen Versammlung oder zeitlich und sachlich damit unmittelbar im Zusammenhang stehender Ereignisse unverzüglich zu vernichten, soweit sie nicht benötigt werden[1]. für die Verfolgung von Straftaten von Teilnehmern oder 2. im Einzelfall zur Gefahrenabwehr, weil die betroffene Person verdächtigt ist, Straftaten bei oder im Zusammenhang mit der öffentlichen Versammlung vorbereitet oder begangen zu haben, und deshalb zu besorgen ist, daß von ihr erhebliche Gefahren für künftige öffentliche Versammlungen oder Aufzüge ausgehen.«

Ob von jemandem in abstrakter Zukunft erwartet werden kann, dass er eine Straftat begehen wird, ist natürlich Ansichtssache. Man sollte sich auch vor Augen halten, dass vor allem bei Großdemonstrationen eine schwer einschätzbare Menschenmasse zusammenkommt, bei der ein Veranstalter niemals ausschließen kann, dass Einzelne durchaus zu Sachbeschädigung und Körperverletzung bereit sind. Vielmehr kann niemals ausgeschlossen werden, dass vereinzelte Gruppierungen zu »konkreten Aktionen« gegen was auch immer aufrufen werden. So etwas kann selbst beim besten Willen nicht verhindert werden. Ist es jedoch gerechtfertigt auf dieser Grundlage gleich alles und jeden aufzuzeichnen?

Wie lange bleiben die Daten anschließend gespeichert, wenn es zu Gesetzesverstößen während einer Demonstration kommt?

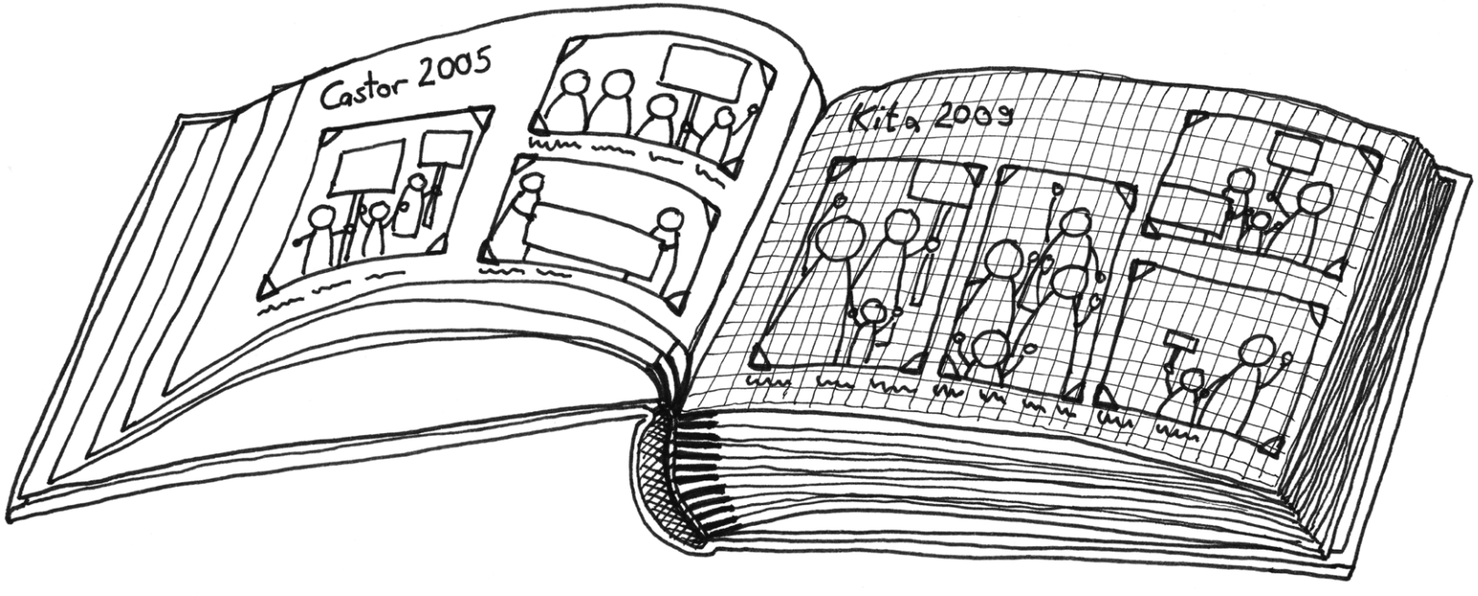
Das Versammlungsgesetz sagt uns: »Unterlagen, die aus den in Satz 1 Nr. 2 aufgeführten Gründen nicht vernichtet wurden, sind in jedem Fall spätestens nach Ablauf von drei Jahren seit ihrer Entstehung zu vernichten, es sei denn, sie würden inzwischen zu dem in Satz 1 Nr. 1 aufgeführten Zweck benötigt.« Also besteht die Gefahr, dass mein Foto oder eine Aufnahme, wie ich friedlich mein Transpi schwenke, im Zweifelsfall für drei Jahre irgendwo einsehbar ist. Nun gut.

Auswirkungen auf das Demonstrationsverhalten

Man muss sich auch die unmittelbare Auswirkung von derartigen Aufnahmen auf die Demonstranten vor Augen führen. Polizisten mit Videokameras und Fotoapparaten entwickeln eine durchaus einschüchternde Wirkung auf die Demonstrationsteilnehmer-

Innen. Auch wenn man friedlich für allgemein gesellschaftlich akzeptierte und anerkannte Ziele auf die Straße geht, bleibt da doch der bittere Beigeschmack des Irreversiblen zurück.

Auch wenn man von seinem Recht Gebrauch macht, auch wenn man nichts zu verbergen hat, wird einem doch die Kontrolle über die Nachweise der eigenen Teilnahme an einer politischen Veranstaltung aus der Hand genommen. Natürlich könnte man sich auch einfach eine Kapuze über den Kopf und einen Schal übers Gesicht ziehen. Dann jedoch macht man sich wiederum strafbar. Vermummungsverbot nennt sich das, denn laut Versammlungsgesetz ist es verboten »an derartigen Veranstaltungen in einer Aufmachung, die geeignet und den Umständen nach darauf gerichtet ist, die Feststellung der Identität zu verhindern, teilzunehmen oder den Weg zu derartigen Veranstaltungen in einer solchen Aufmachung zurückzulegen.« Dies kann dann mit Geldstrafen oder gar Freiheitsstrafen bis zu einem Jahr geahndet werden. Anonym sind wir demnach bei einer Demonstration längst nicht mehr und sollen es auch nicht sein. Obwohl die genannten Einschränkungen grundsätzlich zur Verhinderung von Straftaten aus einer anonymen Masse heraus konzipiert worden sind, treffen sie insbesondere in Zeiten aufkommender neuer technischer Möglichkeiten doch eher die große Masse der friedlichen Demonstranten, als eventuelle tatsächliche Straftäter. In Zeiten biometrischer Passbilder und automatischer Bilderkennungsprogramme, welche in einigen Jahren wohl technisch noch ausgereifter und erschwinglicher sein werden, eröffnen sich nun ganz neue Möglichkeiten für die Strafverfolgung.



Anonym sind wir bei einer Demonstration längst nicht mehr und sollen es auch nicht sein.

EinE PolizeibeamtIn ist verpflichtet uns auf Anfrage seine/ihre Dienstnummer zu nennen. Dies soll verhindern, dass PolizistInnen sich im Schutz der anonymen Masse einer Großveranstaltung Übergriffe erlauben. Es kam bei Demonstrationen schon vereinzelt zu sexuellen Übergriffen vor allem gegenüber weiblichen Demonstrationsteilnehmerinnen. Wer kann schon im Nachhinein sagen, ob der Griff an die Brust oder an den Hintern nun unbedingt »notwendig« war. Wenn Betroffene jedoch nach der Dienstnummer fragen, erhalten sie nur selten Auskunft. Der/die PolizeibeamtIn ist in seiner Uniform anonym. Und im Falle eines bewussten Verstoßes gegen die Dienstvorschriften, wäre es schließlich reichlich naiv davon auszugehen, dass der/die BeamtIn

Das Recht, für seine Meinung auf die Straße gehen zu dürfen, frei von staatlichen Kontroll- und Überwachungsmaßnahmen ist essenziell für die Funktionsfähigkeit einer wehrhaften Demokratie.

sich freiwillig selbst belasten würde. PolizistInnen sind somit größtenteils anonym, DemonstrantInnen müssen jedoch damit rechnen dies im Zweifelsfall nicht zu sein.

Wir als DemonstrationsteilnehmerInnen haben keinerlei Möglichkeit zu kontrollieren, was mit eventuellen Aufnahmen geschieht, es sei denn wir schicken eine konkrete Anfrage an das zuständige Amt, womit wir natürlich vollends unsere Anonymität der Masse aufgeben. Der/die Einzelne wird dies wohl kaum tun. Auch wissen wir nicht, ob es nicht zu Missverständnissen der Strafverfolgungsbehörden kommen kann. Sind wir, ohne es zu wissen, neben einem »potentiellen Gewalttäter Links/Rechts« gelaufen und haben den Anschein erweckt diesen zu kennen?

PolizistInnen mit Aufnahmegeräten sind einschüchternd, so viel ist sicher. Und sie tragen nicht gerade dazu bei, dass man sich auf einer Demo sicherer fühlt. Eher kriminalisiert. Denn die eigene Unsicherheit, was denn nun mit den Aufnahmen geschieht, können die BeamtInnen nicht beseitigen. Ob auf diese Weise politisches Engagement der Bevölkerung gefördert werden kann erscheint zumindest mehr als fraglich.

Die Föderalismusreform

Die Föderalismusreform von 2006 hat nun die Zuständigkeit für das Versammlungsrecht in den Kompetenzbereich der Bundesländer verlagert. Einige Länder wie Bayern und Niedersachsen haben daraufhin beschlossen, ihr Versammlungsrecht zu reformieren. Konkret wurde das Tragen als »militant« eingestufter Kleidung untersagt, die Erfassung von persönlichen Daten der Ordner ausgeweitet, die Haftungspflicht des Anmelders erhöht sowie die Straf- und Bußgeldvorschriften für Vergehen angehoben. Viele dieser Reformen sind im Falle des neuen bayerischen Versammlungsgesetzes im Zuge einer Eilentscheidung des Bundesverfassungsgerichtes als verfassungswidrig eingestuft und daher zurückgenommen worden. Die Verschärfungen der gesetzlichen Maßnahmen wurden mit dem Demonstrationsverhalten der radikalen linken und rechten Szene begründet, welches es zu regulieren gelte. Problematisch ist vor diesem Hintergrund die mangelhafte Konkretisierung der betroffenen Gruppen und Vergehen. Ob eine Kleidung einschüchternd wirkt, scheint in hohem Maße von der subjektiven Meinung des Beobachters abzuhängen, ebenso wie der beobachtete Grad der »Radikalität« der politischen Gruppierung. Einschränkungen, welche politische Randgruppen, wie beispielsweise die rechtsradikale Szene in ihrem Aktionsrahmen einschränken sollen, können somit auch andere Gruppierungen in ihren Rechten beschneiden.

Das Recht, für seine Meinung auf die Straße gehen zu dürfen, frei von staatlichen Kontroll- und Überwachungsmaßnahmen sowie unverhältnismäßigen gesetzlichen Sanktionierungen, ist essenziell für die Funktionsfähigkeit einer wehrhaften Demokratie. Dem/der BürgerIn muss die Möglichkeit offen stehen, seiner Regierung jederzeit ein Feedback geben zu können, ganz gleich ob dieses positiv oder negativ ausfällt.

Die weitere Entwicklung bleibt abzuwarten. Es kann jedoch festgestellt werden, dass eine deutliche Tendenz zur Verschärfung der gesetzlichen Rahmenbedingungen des Versammlungsrechts besteht. Es wäre wieder an der Zeit, für das Demonstrationsrecht demonstrieren zu gehen, damit die Demokratie nicht unter die Räder präventiver Sicherheitsgesetze gerät.

Katharina Maria Nocun, Ak Vorrat Münster,
Referat für Datenschutz und Informationelle
Selbstbestimmung im AStA der Uni Münster

Generell verdächtig
Kontrolle und Überwachung von MigrantInnen

Keine andere Gruppe der Bevölkerung ist so weitreichenden Überwachungs- und Kontrollmechanismen ausgesetzt wie MigrantInnen. Dies ist Ausdruck eines staatlichen Rassismus, der sich auf einen breiten Konsens in der Gesellschaft stützen kann.

Es sind die immer wieder gleichen Bilder: Die AusländerInnen wandern in die deutschen Sozialsysteme ein, sie liegen den anständigen deutschen SteuerzahlerInnen auf der Tasche und missbrauchen das ja so humanitäre deutsche Asylrecht. Und kriminell sind sie ohnehin, das hat nicht zuletzt der Münchener U-Bahn-Fall bewiesen und wird Jahr für Jahr durch die Polizeiliche Kriminalstatistik untermauert.

Wenn auch nicht immer in dieser Einfachheit formuliert, sind dies, selten unterbrochen durch freundlichere Zwischentöne, die hegemonialen Argumentationsmuster, die der ökonomischen und sozialen Exklusion von MigrantInnen zugrunde liegen.

Nicht nur die InnenministerInnen, sondern auch RichterInnen haben, wie die Mehrheitsgesellschaft in Deutschland, grundsätzlich wenig Probleme mit Datenerhebungen.

Ein Phänomenen wie das der sogenannten »Organisierten Kriminalität« oder tatsächliche Ereignisse wie die Terroranschläge des 11. September 2001 und die Existenz eines nebulösen islamistischen Terrornetzwerks sind nicht etwa der tatsächliche Ausgangspunkt, sondern vielmehr willkommene Feindbilder, um eine rassistische und stigmatisierende Politik vorantreiben zu können.

Rasterfahndung und Gesinnungstest

Offen zutage trat dies bei der sogenannten Rasterfahndung, die im Zuge der besagten Terroranschläge deutschlandweit praktiziert wurde. Bei der Rasterfahndung werden Personen oder Personengruppen aus den Datenbanken herausgefiltert, indem man nach Merkmalen sucht, von denen man annimmt, dass sie auch auf eine gesuchte Person zutreffen. Nach den Anschlägen in New York und Washington war klar: Besonders gefährlich sind männliche Studenten oder ehemalige Studenten, zwischen 18 und 40 Jahre alt, aus dem arabischen Raum stammend und islamischen Glaubens. Bei der Rasterfahndung, die ab Ende 2001 erstmals koordiniert in allen Bundesländern angewendet wurde, hatten Einwohnermeldeämter, Universitäten und das Ausländerzentralregister mehr als acht Millionen Datensätze – 5,2 Millionen allein in Nordrhein-Westfalen – an die Polizei weitergeleitet. Nach einer ersten Rasterung wurden 32.000 Datensätze an das Bundeskriminalamt übermittelt und dort in die Verbunddatei »Schläfer« eingestellt. Ein islamistischer Terrorist konnte nicht enttarnt werden. Die Aktion hatte indes keine konkrete Terrordrohung zum Anlass, sondern beruhte allein

auf vagen Vermutungen. Aus diesem Grund wurde die Aktion 2006 durch das Bundesverfassungsgericht auch für unzulässig erklärt, denn eine Rasterfahndung sei nur zulässig bei einer »konkreten Gefahr«.

Zwar per offener Befragung, aber nicht weniger pauschal und verdachtsunabhängig, unterziehen seit 2007 die Ausländerbehörden in NRW Menschen aus 26 Herkunftsländern bei der Erteilung oder Verlängerung ihres Aufenthaltstitels einer sogenannten Sicherheitsbefragung. Die Maßnahme wurde durch einen Erlass des Innenministeriums NRW angeordnet und betrifft wiederum vorrangig Menschen aus dem arabischen Raum. Neben Fragen zu Reisen und Aufenthalten in anderen Ländern geht es bei der Befragung etwa darum, ob die Betroffenen jemals für einen Geheimdienst eines anderen Staates gearbeitet haben. Die Antworten können an Polizei und Geheimdienste weitergeleitet werden, sollten sie auf eine »Gefährlichkeit« hinweisen. Wer falsch oder gar nicht antwortet kann seinen/ihren Aufenthaltstitel verlieren. Ein Student aus Münster hat gegen diese Praxis Klage vor dem Verwaltungsgericht eingereicht – nach den Maßstäben des Bundesverfassungsgerichts zur Rasterfahndung könnte eine derart pauschale Datenerhebung ebenfalls vor Gericht scheitern.

Ausländerzentralregister

Es gibt jedoch keinen Grund, sich auf das Bundesverfassungsgericht oder andere Gerichte zu verlassen. Nicht nur Wolfgang Schäuble und seine InnenministerkollegInnen treiben die Verschärfung sozialer Kontrolle voran. Auch RichterInnen haben, wie die Mehrheitsgesellschaft in Deutschland, grundsätzlich wenig Probleme mit Datenerhebungen, die eine pauschale Kontrolle von MigrantInnen vorsehen. Bislang von den Gerichten nicht gerügt, werden im Ausländerzentralregister die Daten aller AusländerInnen in Deutschland erfasst. Zugriff darauf haben nicht nur Polizeien, Nachrichtendienste und Ausländerbehörden, sondern auch Gerichte, Staatsanwaltschaften und andere öffentliche Stellen wie die Sozialämter und die Bundesagentur für Arbeit. Dabei werden in der Datei nicht nur der Aufenthaltsstatus und das Einreisedatum, sondern auch Verdachtsmomente über Schleusertum oder Terrorismus gespeichert. Damit kön-

nen die Daten nicht nur der Verwaltung der AusländerInnen, sondern auch der Strafverfolgung zugute kommen. Der Europäische Gerichtshof hat dies 2008 in Bezug auf BürgerInnen aus der Europäischen Gemeinschaft (EG) teilweise als unzulässig erklärt, da darin eine Diskriminierung gegenüber Deutschen zu sehen sei. Die »Diskriminierung« von Menschen aus Staaten außerhalb der EG kann damit jedoch aufrecht erhalten bleiben.

Zur noch stärkeren Bekämpfung der »illegalen Migration« wurde daneben im Mai 2006 das Gemeinsame Analyse- und Strategiezentrum illegale Migration (GASIM) eingerichtet. Das Zentrum bündelt migrationsrelevante Daten unterschiedlicher Behörden, darunter etwa des Bundeskriminalamtes, des Bundesnachrichtendienstes, des Auswärtige Amtes und des Bundesamtes für Migration und Flüchtlinge. Faktisch umgehen diese Vernetzungen das Trennungsgebot, wonach Polizei und Geheimdienst organisatorisch getrennt sein müssen.

Gentests ohne Rechtsgrundlage

Es braucht aber nicht immer derart großer Projekte – das rassistische Misstrauen setzen deutsche Behörden auch ohne gesetzgeberische Vorgaben in die Tat um. So etwa beim Familiennachzug von MigrantInnen nach Deutschland: Wenn Menschen nach Deutschland kommen wollen, um wieder mit ihrer Familie zusammen ziehen zu können, werden regelmäßig Gentests durchgeführt, um die biologische Verwandtschaft von Eltern und Kindern zu überprüfen – schließlich könnten die vorgelegten Dokumente gefälscht sein, und den MigrantInnen selbst kann man ohnehin nicht glauben. Jährlich werden in Deutschland DNA-Abstammungsgutachten in vierstelliger Zahl durchgeführt, eine Rechtsgrundlage dafür existiert bislang nicht. Ebenso wenig sind die Tests, wie bisweilen behauptet, »freiwillig«, denn als Alternative bleibt allein der Verzicht auf ein Bleiberecht in Deutschland.

Selektive Ermittlungsmaßnahmen

Eines der wesentlichen Argumentationsmuster für derart offene Rassismen im realpolitischen Diskurs der Mehrheitsgesellschaft ist die »hohe Ausländerkriminalität«. Dabei wird gerne auf die Polizeiliche Kriminalstatistik (PSK) zurückgegriffen, wonach die Anzahl von Straftaten durch »Nichtdeutsche«, gemessen am Anteil der Gesamtbevölkerung eindeutig über dem der Menschen mit deutschem Pass liegt – ein Steilvorlage für eine rassistische Innenpolitik. Dabei werden allerdings mehrere Aspekte verschleiert. So sind gut ein Sechstel der verzeichneten Taten solche des Asyl- und Ausländerrechts, die von Deutschen gar nicht begangen werden können. Vor allem aber offenbaren die Befunde aus der PSK, dass MigrantInnen besonders intensiv mit staatlichen Kontrollmaßnahmen konfrontiert sind. Denn die PSK verzeichnet nicht nur tatsächlich festgestellte Straftaten, sondern auch reine Verdächtigungen. Hier ist zu bedenken, dass MigrantInnen häufiger als andere Menschen Opfer polizeilicher Datenkontrollen und Verdächtigungen durch StreifenpolizistInnen sind, so etwa im Straßenverkehr. Seit den neunziger Jahren ist in den Polizeigesetzen des Bundes und der Länder zudem die Möglichkeit verdachtsunabhängiger Schleierfahndungen mit rassistischer Zielrichtung verankert. Diese zielen vor allem auf verstärkte Kontrollen in Zügen, auf Bahnhöfen und Autobahnen und dienen, so die Polizeigesetze, zuvorderst der »vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität«. Da es bei diesen Generalkontrollen nicht möglich ist, alle Menschen zu kontrollieren, bedarf es eines personenbezogenen Verdachtsprofils. Angesichts der Zielrichtung der Gesetze ist eine vornehmlich angewandte Methode hierbei das sogenannte »racial profiling«: Dabei ist das maßgebliche Merkmal der zu kontrollierenden Person ein »ausländisches Äußeres«. Aus Bayern beispielsweise ist bekannt, dass die Kriminalpolizei Fahndungsraster angelegt hat, die bei bestimmten Straftaten auf bestimmte Gruppen von AusländerInnen abstellen, so etwa die »rumänischen Tresorknacker« oder die »polnische Autoschieberbande« – hier weiß der/die handelnde BeamtIn also gleich, wen er/sie kontrollieren muss.

> Beim »racial profiling« ist das maßgebliche Merkmal der zu kontrollierenden Person ein ausländisches Äußeres.

Europäische Datenbanken

Die Kontrolle von MigrantInnen findet indes längst nicht mehr allein auf nationaler Ebene statt. Die Öffnung der europäischen Binnengrenzen hat dazu geführt, dass die Sicherung der europäischen Grenzen mittlerweile in erster Linie gemeinschaftlich vorgenommen wird. Eines der wesentlichen Aspekte dieses europäischen Grenzsicherungs- und Abschottungsregimes ist eine zunehmende Vernetzung der nationalen Grenzschutzbehörden, um den illegalen Aufenthalt von MigrantInnen zu unterbinden. Dabei kann derzeit in erster Linie auf drei Datenbanken zurückgegriffen werden.

Im Schengener Informationssystem (SIS) sind, neben anderen Daten, Personen vermerkt, die zur Einreiseverweigerung ausgeschrieben sind – 2006 waren dies etwa 750 000 Personen. Im Verdachtsfall können die nationalen Polizeibehörden auf diese Daten zugreifen. Das SIS soll demnächst durch das Schengener Informationssystem II ersetzt werden. Entscheidende Neuerung gegenüber dem alten System ist die Möglichkeit, biomet-

> Die Repression gegenüber MigrantInnen kann nur insgesamt kritisiert werden, indem die zugrundeliegenden rassistischen Argumentationsmuster der (deutschen) Gesellschaft aufgedeckt werden.

rische Daten in Form von Fingerabdrücken und Fotos der betroffenen Personen zu speichern. Daneben wird gegenwärtig ein VISA-Informationssystem (VIS) aufgebaut. Dies soll bis zu 70 Millionen Visaanträge pro Jahr speichern und sieht vor, die betroffenen Personen mit allen zehn Fingerabdrücken zu erfassen. Zum »Schutz vor Asylmissbrauch« schließlich wurde im Jahr 2000 mit der EURODAC-Verordnung des EU-Ministerrates aus dem Jahre 2000 eine weitere, in Luxemburg stationierte Datenbank eingerichtet. Alle Mitgliedsstaaten sind demnach verpflichtet, von jedem/jeder AsylbewerberIn und von jedem/jeder AusländerIn, der/die illegal die EU-Grenzen überschreitet, die Fingerabdrücke aller Finger zu nehmen. So soll verhindert werden, dass Asylsuchende in mehreren EU-Staaten zugleich Asylanträge stellen.

Langfristig hat die Europäische Kommission den Aufbau eines entry/exit-System vorgesehen, in welchem die Einreise wie auch die Ausreise jeglicher Menschen aus außereuropäischen Staaten registriert und ihre biometrischen Merkmale gespeichert werden sollen. Dies kann eine Datenmenge von bis zu 500 Millionen Menschen ergeben.

Was tun?

Menschen mit deutschem Pass sind nicht annähernd so stark von staatlicher Kontrolle erfasst. Die Erhebung und Speicherung zahlreicher Daten korreliert mit weiteren Repressionsmaßnahmen wie etwa den niedrigen Leistungen des Asylbewerberleistungsgesetz – welche noch unter dem Sozialhilfesatz liegen –, der Residenzpflicht und besonders unwürdigen Bedingungen in den deutschen Abschiebegefängnissen.

Angesichts dessen ist hier mit einem isolierten Rückgriff auf Grundrechte und die Verhältnismäßigkeit staatlicher Machtausübung nur wenig geholfen. Die Wirkung dieser Instrumente ist ohnehin beschränkt, vor allem da sie staatliche Herrschaft nicht insgesamt in Frage stellen. Sie können daher allenfalls strategische Argumente für eine emanzipatorische Politik sein und zur Skandalisierung gesellschaftlicher Zustände beitragen. Vor allem die Repression gegenüber MigrantInnen kann überdies nur insgesamt kritisiert werden, indem die zugrundeliegenden rassistischen Argumentationsmuster der (deutschen) Gesellschaft aufgedeckt werden.

Matthias Lehnert

Literatur

Achelpöhler, Wilhelm, Verfassungsgrenzen für die Rasterfahndung, in: Müller-Heidelberg, Till unter anderem (Hrsg.), Grundrechtereport 2007, S. 51–54.

Busch, Heiner, EU-Informationssysteme: Stand und Planung, Bürgerrechte & Polizei/CILIP 84 (2/2006), S. 29–43.

Brüchert, Oliver, Kriminalstatistik und Rassismus, in: Bürgerrechte & Polizei/CILIP 65 (01/2000), S. 21–28.

Herrenkind, Martin, »Schleierfahndung«. Institutionalisierter Rassismus und weitere Implikationen sogenannten verdachtstunabhängiger Kontrollen, in: Komitee für Grundrechte und Demokratie (Hrsg.), Verpolizeilichung der Bundesrepublik Deutschland, S. 99–143.

Holzberger, Mark, Analyse- und Strategiezentrum »Illegale Migration«, in: Bürgerrechte & Polizei/CILIP 89 (1/2008), S. 49–51.

Kant, Martina, MigrantInnen im Netz der Schleierfahndung, in: Bürgerrechte & Polizei/CILIP 65 (01/2000)

Kasparek, Bernd, Perfektion des Grenzregimes, analyse & kritik 527, 18. April 2008.

Lehnert, Matthias, Mit Blick auf die Ränder – Überwachung von Migrant_innen, in: Leipziger Kamera (Hrsg.), Kontrollverluste. Interventionen gegen Überwachung, 2009, S. 137–141.

Mauer, Albrecht/Kant, Martina, »Vergrenzung des Inlands, in: Bürgerrechte & Polizei/CILIP 89 (01/2008), 52–57.

Roggan, Frederik, »Irgendwas muss die Polizei ja machen». Rasterfahndungen nach dem 11. September 2001, in: Till Müller-Heidelberg unter anderem (Hrsg.), Grundrechtereport 2002, S. 46–50.

Walburg, Christian, Die üblichen Verdächtigen, in: Forum Recht 03/06, S. 94–96.

www.gesinnungstest-nrw.de.

Das Grundgesetz in Zeiten des internationalen Terrorismus

Seit den Anschlägen auf das World Trade Center in New York, die im allgemeinen Bewusstsein der massenmedial informierten Bevölkerung auch unter dem Synonym 11. September als Beginn des »Kampfes gegen den Terror« fungieren, hat sich einiges geändert.

Zum einen haben sich einige Staaten, allen voran die USA, dazu entschlossen, gemeinsam mit der »Koalition der Willigen«, die »Achse des Bösen«, im Zuge eines »Präventivschlages« anzugreifen. Zum anderen wurden viele Einschränkungen der Grundrechte innerhalb der Nationalstaaten der »Achse des Guten« vorgenommen, um die Gefahr von Terroranschlägen eindämmen zu können. Denn so schwarz-weiß und eindeutig die neuen ideologischen Grenzen dieses Konfliktes auch auf den ersten Blick erscheinen mögen: Gut gegen Böse, Rechtsstaat gegen Terrorismus, auf Angriff folgt Verteidigung – Der »Feind« scheint schwer zu fassen und auch nicht gerade einfach erkennbar zu sein. »Schläfer« und »Gefährder« können schließlich überall lauern. Auch inmitten der eigenen Bevölkerung. Abhilfe schaffen sollen in dieser denkbar schwierigen Lage die Ausweitung der Überwachung, die Verschärfung der Einreisebedingungen und die Schaffung neuer Ministerien und Gesetze, um die »Heimat« vor diesen neuen Gefahren zu schützen.

Doch nicht nur die »Koalition der Willigen« muss Einschränkungen ihrer Bürgerrechte zur Verteidigung ihrer »Freiheit« in Kauf nehmen. Auch innerhalb von Deutschland, dem zwischenzeitig chronisch unwilligen Bündnispartner, hat sich einiges verändert.

Wie beweist man eine böswillige Intention?

Die Anti-Terror-Paragraphen

Der Innenausschuss sah einigen Anpassungsbedarf der bisherigen Gesetze, welche bei Erfassung von »mutmaßlichen Terroristen« bisher greifen. Mit dem »Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten« sollte diese »Lücke« im Gesetz nun geschlossen werden – so jedenfalls der Plan. Der Bundesrat konnte diese Sicht der Dinge nur begrenzt teilen und nahm ihn in großen Teilen nicht an. Doch worum ging es bei diesem Gesetz, den neuen Anti-Terror-Paragraphen § 89a und § 91-E StGB nun eigentlich konkret?

Zur Erinnerung: Der Paragraph 89a ist eine recht neue Schöpfung und bezieht sich hauptsächlich auf die Vorbereitung, Planung und Intention einer als terroristisch eingestuften Handlung. Diese Handlung hat zu dem Zeitpunkt, an dem das Gesetz bereits greifen soll, wohlgemerkt noch nicht stattgefunden.

Der Strafrechtsausschuss der Bundesrechtsanwaltskammer lehnte den Entwurf erst einmal aus grundsätzlichen Beurteilungsgründen ab und stufte ihn als untauglich für einen demokratisch verfassten Bundesstaat ein. Demnach sei eine Grenze der Gefahrenabwehr kaum noch auszumachen, da die Beurteilung, wann eine Handlung strafbar gemäß § 89a wird, recht subjektiv und ungenau erscheint.

Des Weiteren dreht das neue »Antiterrorgesetz« die Grundprinzipien unseres Rechtsstaates um. Wie soll man eine Intention beweisen? Wie ordnet man eine Handlung, welche noch nicht stattgefunden hat einer konkreten Person zu? Wie beweist man eine böswillige Intention?

Eine Anekdote aus der Welt der Erasmusstudenten

In einer mittelgroßen französischen Universitätsstadt feiert ein Chemiestudent Geburtstag. Und wie das so ist, wenn StudentInnen feiern – Es wird getrunken und das nicht gerade wenig. Irgendwann kommen dann einige der jungen Männer auf die Idee, eine Sprengladung zu bauen. Einfach so, weil sie betrunken und jung und voller Testosteron sind. Die Zutaten sind einfach zu beschaffen, denn mit ein wenig Improvisation und Kreativität lassen sich einfachste Haushaltsgegenstände erfolgreich zur Bombe uminstrumentalisieren.

Doch wie das so ist, wenn man betrunken ist – etwas geht schief. Die Explosion hörte man in der ganzen Stadt. Viele unter den Anwesenden wurden schwer verletzt. Sie hatten laut eigener Aussage nicht die Absicht, die Sprengladung im Wohnheim hochgehen zu lassen. Wäre auch ein reichlich unausgereifter Plan gewesen, wenn man genauer darüber nachdenkt. Sie wollten irgendwo in der Einöde der Vorstadt, wo sie niemanden verletzen konnten, ihr Werk bei einem Kasten Bier begutachten. Nun ja, dazu ist es nicht mehr gekommen.

Sie haben grob fahrlässig gehandelt, alle miteinander, so viel war klar. Auch ihnen selbst.

Frage: Was wäre gewesen, wenn es sich nun um libanesische AustauschstudentInnen gehandelt hätte? Wie beweisen, dass der Geburtstag nicht Vorwand für ein konspiratives Treffen gewesen ist? Wie beweisen, dass es sich um einen Freundeskreis und keine terroristische Vereinigung handelt?

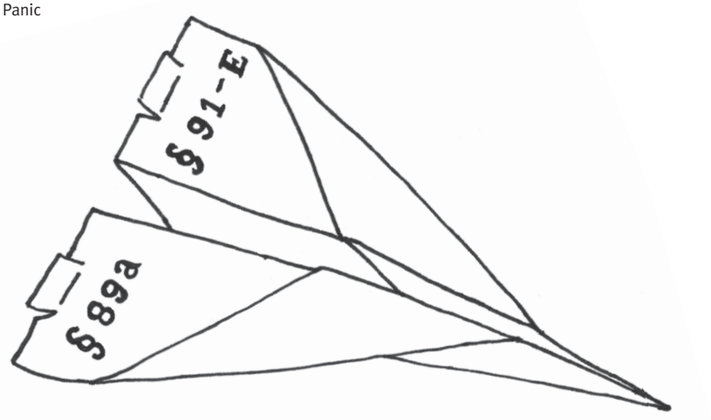
Die Schuldfrage

Angeklagte sind so lange unschuldig, bis man ihnen ihre Schuld nachweisen kann. Dies muss mit Hilfe von Beweisen geschehen. Doch wie nun die böswillige Intention beweisen? Sind wir nicht alle irgendwo irgendwann »Gedankenverbrecher« gewesen und haben gedanklich bereits dutzende von Leichen – die Chefin, der nervige Nachbar,… – In unseren unterbewussten Kellern?

In vielen Situationen mag die Sachlage eindeutig sein, in anderen Fällen gestaltet sich die Beweislage jedoch durchaus schwierig. Die Angeklagte ist so lange unschuldig, bis man ihr das Gegenteil nachweisen kann. Doch wie kann man Gedanken beweisen?

Dreht sich in solchen Situationen nicht vielmehr die Beweislast zu Ungunsten der Angeklagten um?

Der Strafrechtsausschuss der Bundesrechtsanwaltskammer schreibt in seinem Bericht[1]:



»Es besteht die Gefahr, dass sozialübliche Handlungen ohne rechtfertigende Grundlage umgedeutet werden. Außerdem kann die überschießende Innentendenz der Tatbestände gerade im Hinblick auf den Personenkreis, auf den der Entwurf ausdrücklich zielt, eine unangemessene Entwicklung vom Tatstrafrecht zu einem Täterstrafrecht befördern.«

Ist das denn unbedingt Notwendig?

Das Strafgesetzbuch lässt in seiner derzeitigen Form die Verurteilung von terroristischen Handlungen und Organisationen zu. Es existieren bereits zahlreiche Verordnungen und Gesetze, welche den Waffen, und Sprengstoffbesitz sowie -handel reglementieren. Auch die Vorbereitung derartiger Handlungen ist bereits gemäß existierender Paragraphen strafbar. Auch die Aufforderung und der Aufruf zu derartigen Handlungen sind derzeit bereits… strafbar.

Des Weiteren scheint es durchaus fraglich, ob ideologisch oder religiös motivierte AttentäterInnen sich durch ein neues Gesetz mit höheren Strafen und weiteren Grenzen beeindrucken lassen. Wer bereit ist, sein Leben für eine Idee zu opfern, wird sich nicht über mögliche rechtliche Konsequenzen informieren.

Nach dem angedachten § 89a muss kein konkreter Anschlagsplan mehr bestehen, um sich strafbar in Sinne dieses Paragraphen zu machen. Weder Zeitpunkt, Ort noch ein konkreter Entwurf muss feststehen.

Das Grundgesetz sagt in § 103 Absatz II: »Eine Tat kann nur bestraft werden, wenn die Strafbarkeit gesetzlich bestimmt war, bevor die Tat begangen wurde.«

Womit wir wieder bei der Frage nach strafbaren Gedanken und »Präventivschlägen« sowie Beweislastumkehrung angekommen sind. Denn wenn keine Tat, auch nicht deren konkrete Vorbereitung, sondern nur die Absicht stattgefunden hat, bleibt ja nichts außer den Gedanken, die strafbar sind.

Laut § 91-E StGB soll auch die Anleitung und Aufnahme von Beziehungen zur Begehung einer schweren Straftat unter Strafe stehen. Für das Verbreiten oder Verherrlichen von terroristischen Anleitungen oder Aufrufen gibt es nun bis zu drei Jahre Haft, wenn die Anleitung in der »Art und der Weise ihrer Verbreitung« dazu taugt, die Bereitschaft oder das Interesse an terroristischen Anschlägen zu wecken. Diese Voraussetzung erfüllen laut Entwurf Internetpräsenzen innerhalb eines »bestimmten radikalen« Umfeldes. Die Aufnahme von Beziehungen zu einer terroristischen Vereinigung zwecks Ausbildung in einem »Terrorcamp« sollen laut § 91-E StGB bald auch unter Strafe stehen. Die Veröffentlichung von Bauanleitungen für Sprengsätze oder potentielle Sprengsätze im Internet soll unter Strafe gestellt werden.

Kommen wir einmal mehr zu unseren ErasmusstudentInnen zurück…

Wieder nach Deutschland zurückgekehrt, schreibt einer von ihnen nun fleißig an seiner Diplomarbeit. Das kann durchaus dröge und mühsam sein. Insbesondere, wenn alles selbst nachgekocht und synthetisiert werden muss. Um die Zeit zwischen Versuchsbeginn und Auswertung effektiv überbrücken zu können, wird erst einmal im Internet gesurft. Und wenn die Synthese in einer Sackgasse zu versanden scheint, kann in Internetforen nach der Lösung des Problems gesucht werden. So wie das moderne Studierende im digitalen Zeitalter halt machen. Denn nicht alle Probleme sind mit copy-paste lösbar. Manchmal kann gemeinschaftliches Knobeln und Brüten innerhalb von Fachforen die Haus-/Fach-/Diplom-/Magisterarbeit auch noch aus mutmaßlichen Sackgassensituationen retten. Und wenn nicht, so lassen sich doch zumindest hilfreiche Hinweise ausfindig machen.

Dabei kann es auch mal zu merkwürdigen Überschneidungen von Wissenschaft und Interessengruppen kommen, wenn man beispielsweise zufällig an der Synthetisierung eines Stoffes arbeitet, welcher auch anderweitig verwendet werden kann.

Die betreffende Studierende landete bei der Eingabe der Zauberformel in das Scroogle-Fenster[1] nicht etwa im Chemiker-Fachforum, sondern im Forum zur Eigenherstellung von Amphetaminen. Die Ergebnisse waren trotzdem durchaus brauchbar. Dies heißt jedoch noch lange nicht, dass im Universitätslabor des Professors eine Drogenküche eingerichtet worden ist. Derartige Rückschlüsse wären fatal und meist unangebracht.

Der »Feind« scheint schwer zu fassen und auch nicht gerade einfach erkennbar zu sein.

Frage: Was ist, wenn der libanesische Austauschstudent nun an einem Vorprodukt zu einer der unzähligen Sprengstoffarten gebastelt hätte? Wie beweisen, dass seine Diplomarbeit nicht eine dumme Ausrede ist? Ganz davon abgesehen, dass er Chemie doch bestimmt nur belegt hat, um genau an diesen Punkt zu kommen, an dem er nun in der Lage ist eigenständig Sprengstoff herzustellen. Wer würde ihm glauben, dass er nach Deutschland gekommen ist weil er gehört hat, dass hier ein akuter Ingenieursmangel herrsche und er sich daher gute Arbeitsplatzchancen erhoffte…

Die Gedanken sind frei?

Die Berliner Justizsenatorin Gisela von der Aue sieht kein Verbesserungspotential der Strafverfolgung durch die geplanten neuen Anti-Terror-Paragraphen[2].

»Stattdessen würden in Zukunft eine Menge Menschen überwacht, nur weil sie sich irgendwelche physikalischen Abhandlungen aus dem Internet heruntergeladen haben – und zwar mit dem ganzen Arsenal, das die Strafprozessordnung bereithält: Onlinedurchsuchung, Telefonüberwachung, Großer Lauschangriff. Das halte ich bei so geringen Hinweisen für nicht vertretbar.«

Problematisch mag auch die Einordnung eines Inhaltes in ein »radikales Umfeld« sein. Weder enthält der Gesetzesentwurf Anhaltspunkte dafür, noch konkretisiert er die strafbaren Inhalte. Dies kann zu einer höchst subjektiven Rechtsprechungspraxis führen, was nicht gerade das Ziel eines Rechtsstaates sein sollte, in welchem jedem Menschen ein gleichwertiges und gerechtes Verfahren garantiert werden sollte.

Hinzu kommt noch, dass die Bürgerinnen und Bürger unter Androhung von Strafe dazu bewegt werden sollen Verdächtige zu melden. Die Bundesrechtsanwaltskammer sieht das ganze in etwa so:

»Im Wege der Androhung eines Bußgeldes sollen Unternehmer und Private dazu angehalten werden, einen Verdacht zu melden, sofern Vermögenswerte zur Vorbereitung schwerer Gewalttaten eingesetzt werden sollen. Die geplanten Änderungen sind angesichts der Unbestimmtheit der in § 89a StGB-E verwendeten Begrifflichkeiten sowie der nicht erklärlichen Herleitung einer Mitteilungspflicht Privater bei nur abstrakten Gefahren abzulehnen.«

Die Gedanken sind also frei… So so.

Mitglied des AK-Vorrat Münster

Literatur

Bundesanwältekammer: www.brak.de/seiten/pdf/Stellungnahmen/2008/Stn46.pdf

heise über die Ablehnung des Entwurfs durch den Bundesrat: www.heise.de/newsticker/Bundesrat-gegen-deutliche-Verschaerfung-der-geplanten-Anti-Terror-Paragraphen--/meldung/134235

1 Anonym mit Google suchen: www.scroogle.org/

2 Spiegel-Online im Gespräch mit Gisela von der Aue: www.spiegel.de/politik/deutschland/0,1518,611613,00.html

Anonym im Netz

Bei der Kommunikation im Internet hinterlassen wir stetig Spuren. Dies betrifft nicht nur Bereiche wie Online-Shops, in denen wir dies bewusst tun, sondern alle Formen der Internetnutzung. Die Aus- und Verwertung dieser Spuren durch Dritte hat in den letzten Jahren stark zugenommen[1]. Dabei ist es mit Hilfe relativ einfacher Maßnahmen möglich, die eigenen Spuren zu verwischen. Einige Grundlagen (anonymer) Kommunikation im Internet werden in diesem Text vorgestellt.

Da glücklicherweise umfangreiche und leicht verständliche Anleitungen zu allen hier genannten Anonymisierungsprinzipien und -programmen existieren, wird an dieser Stelle auf allzu technische Erklärungen verzichtet und stattdessen auf entsprechende Artikel oder Webseiten verwiesen. Technisch versierte Personen mögen uns die Vereinfachungen und Verkürzungen in diesem Artikel verzeihen.

Was technisch unbedingt notwendig ist, birgt auch umfangreiche Möglichkeiten zur Überwachung.

Das Chaos besiegt die Ordnung, weil es besser organisiert ist – die Struktur des Internet

Was uns als klar strukturierter Raum mit eindeutigen und einfach zu merkenden Adressen erscheint, entpuppt sich bei Betrachtung der zu Grunde liegenden Technik als ziemliches Chaos. Das Internet wurde als dezentrales Netzwerk konzipiert, um auch bei einem Ausfall von Teilen des Netzes weiter kommunizieren zu können. Dieser Ansatz prägte und prägt die Architektur und Struktur des Netzwerks stark. Die in diesem vorhandenen Knoten lassen sich vereinfacht in drei verschiedene Kategorien einteilen: Dienstanbieter, reine Verkehrsknoten und Dienstnutzer.

In die erste Kategorie fallen alle Computer, Server, private Rechner und so weiter, die im Internet Dienste anbieten. Dies fängt bei der Sammlung und Zustellung von E-Mails an und geht über Videoportale bis hin zu einfachen Webseiten. Im einfachsten Fall sind diese Computer einzelne Rechner, die – meistens in großen Rechenzentren, sogenannten Serverfarmen, zusammengefasst – bei einem entsprechenden Unternehmen (Hoster) stehen. Es können aber auch ganze Netzwerke hinter einem einzelnen Dienst stehen. Ein Beispiele hierfür ist die Informationsplattform Wikipedia. So steht für den deutschen Part der Wikipedia nicht nur ein einzelner Server bereit, sondern ein ganzes, wiederum kontrolliertes Netzwerk, in dem die Rechenlasten und Daten verteilt werden.

Verkehrsknoten bilden die Infrastruktur des Internets. Sie leiten die versendeten Nachrichten weiter, stellen sie entsprechend dem angegebenen Ziel zu oder verändern sie derart, dass sie für die weitere Zustellung geeignet sind. Das bekannteste Beispiel für die Bereitstellung und den Betrieb von Verkehrsknoten sind die Internet Service Provider (ISPs). Sie stellen unter anderem die Infrastruktur für private Internetzugänge bereit und leiten die von den angeschlossenen Computern versendeten Nachrichten über spezielle Verkehrsknoten in das gesamte Netzwerk.

Dienstnutzer sind prinzipiell alle mit dem Internet verbundenen Geräte, sei es der eigene Computer, das Mobiltelefon oder der »intelligente«, Lebensmittel bestellende Kühlschrank. Sie zeichnen sich dadurch aus, dass sie anderen Knoten im Netzwerk keine Dienste anbieten, sondern diese lediglich selber nutzen. Es ist möglich und durchaus üblich, dass ein Knoten im Netzwerk in mehrere der Kategorien fällt. So nutzen viele Webserver die Dienste anderer Webserver oder leiten Nachrichten an diese weiter. Auch private Computer fungieren oft als Dienstanbieter, zum Beispiel in Filesharing-Netzwerken wie Bittorrent.

Eine Adresse, sie alle zu finden – der Nachrichtenaustausch

Um Nachrichten zuverlässig austauschen zu können, müssen beide kommunizierenden Knoten ihren Kommunikationspartner im Internet ausfindig machen können. Dies wird über die Vergabe von weltweit eindeutigen Adressen, den sogenannten IP-Adressen gewährleistet. Beim Anschluss an das Internet wird jedem Knoten eine dieser Adressen zugewiesen und an jede versendete Nachricht als Rücksendeadresse angehängt. Adresszuweisungen können dauerhaft sein, zum Beispiel für Webserver, die ständig erreichbar sein müssen (die von uns im Browser eingegebenen Adressen haben eine reine Komfortfunktion). Für viele Knoten ist es jedoch ausreichend, wenn die Adresse lediglich für die Dauer des »Aufenthalts« im Netz gleich bleibt. Dies ist in der Regel auch bei privaten Internetanschlüssen der Fall. Dabei ist zu beachten, dass pro Anschluss lediglich eine IP-Adresse vergeben wird, auch wenn

dieser von mehreren Rechnern genutzt wird. So agieren vier in einer WG an das Internet angeschlossene Rechner von einer IP-Adresse aus (die Nachrichten werden innerhalb der WG dann von einem privaten Router an die einzelnen Knoten verteilt).

Was technisch unbedingt notwendig ist, birgt auch umfangreiche Möglichkeiten zur Überwachung. Da IP-Adressen wie oben beschrieben offen kommuniziert werden (müssen), kann bei der Kommunikation im Internet neben dem Zielknoten jeder Verkehrsknoten, über den eine Nachricht weitergeleitet wird, Absender- und Zieladresse sowie gegebenenfalls auch den Inhalt der Nachricht mitlesen. Konkret bedeutet dies zum Beispiel, dass sowohl der eigene Internetprovider als auch viele Infrastruktur-Provider detaillierte Informationen über die von uns aufgerufenen Webseiten oder empfangenen E-Mails besitzen. Da zumindest der Internetprovider weiß, welche IP-Adresse zu welchem Zeitpunkt einem Anschluss zugeordnet war, ist an dieser Stelle ein Rückschluss auf die AnschlussinhaberIn möglich. Dies wird bereits aktiv genutzt, um beispielsweise Menschen, die Musik oder Filme im Internet tauschen, rechtlich zu verfolgen.

Anonyme Kommunikation im Internet funktioniert jedoch nur mit einer ausreichend hohen Anzahl an NutzerInnen.

Eine Verschlüsselung verbirgt zwar die Inhalte einer Nachricht, nicht jedoch die Tatsache, dass kommuniziert wurde.

Seit dem 01. Januar 2009 sind die Internetprovider in Deutschland (nach aktueller Rechtslage) unter anderem dazu verpflichtet, die Zuordnung der IP-Adresse zu ihren Kunden für mindestens sechs Monate zu speichern und Behörden gegebenenfalls Zugriff auf diese Daten zu gewähren (➳ Artikel Wer wann mit wem kommuniziert, S. 46 ff). Auch die Analyse der Kommunikationsinhalte wird bereits durchgeführt, zum Beispiel um NutzerInnen personalisierte Werbung zukommen zu lassen[2,3].

Reclaim your Anonymity – in der Theorie...

Dennoch kann durch die Verwendung einiger (einfacher) Maßnahmen eine ausreichende Anonymität und Vertraulichkeit der eigenen Kommunikation sichergestellt werden. Hier einige Ansätze:

Verschlüsselung

Damit Nachrichten nur noch von denjenigen gelesen werden können, für welche sie auch bestimmt sind, kann der eigentliche Inhalt der Nachrichten mit Hilfe von Verschlüsselungstechniken für Außenstehende unleserlich gemacht werden. Zu diesem Zweck werden je nach gewählter Verschlüsselungsmethode ein oder mehrere geheime Schlüssel ausgetauscht, die während der Kommunikation zur Ver- beziehungsweise Entschlüsselung der Nachrichten genutzt werden. Genauere Erläuterungen finden sich hier [4,5,11].

Verschleierung

Eine Verschlüsselung verbirgt zwar die Inhalte einer Nachricht, nicht jedoch die Tatsache, dass kommuniziert wurde. Aus diesen Informationen, den Verbindungsdaten, lassen sich jedoch so viele Informationen, zum Beispiel über persönliche Bekanntschaften und Interessen gewinnen, dass eine Kenntnis der Nachrichteninhalte zum Erstellen von Profilen hinfällig wird[6]. Deshalb ist es im Rahmen einer anonymen Kommunikation notwendig, die benutzten Verbindungen vor neugierigen Dritten zu verbergen.

Eine einfache Möglichkeit, dies zu erreichen, ist das massive Erzeugen zufälliger Verbindungsdaten, zum Beispiel mit Hilfe von Programmen, die beliebige Adressen von Webseiten generieren und aufrufen. Somit wird der Aufwand für die Erstellung korrekter Profile erschwert, da eine größere Menge nicht zu den eigentlichen Interessen passende Datenmenge verarbeitet werden muss. Jedoch ist diese Methode in ihrer Wirkung limitiert. Sie bietet keinen Schutz gegen eine gezielte Suche nach bestimmten Verbindungen oder die Protokollierung der Verbindungsdaten durch die aufgerufene Webseite.

Stellvertreter

Um die eigene Identität zu verbergen, kann die eigene Kommunikation über einen anderen Knoten, auch Proxy genannt, geleitet werden. Dieser tritt dann beim Versenden von Nachrichten mit den KommunikationspartnerInnen an Stelle des eigenen Rechners in Erscheinung. Von außen ist somit nur die direkte Kommunikation zwischen dem eigenen Rechner und dem Proxy sowie zwischen dem Proxy und dem Zielknoten sichtbar. Allein der Proxy weiß, welche Knoten miteinander kommunizieren und an welche Adressen eine konkrete Nachricht weitergeleitet werden muss.

Der Vorteil dieser Lösung ist jedoch auch gleichzeitig ihr Nachteil. Der Proxy besitzt alle Informationen zu Deanonymisierung der Kommunikation und kann aufgrund der Position in der Mitte der Kommunikationskette auch Verschlüsselungen angreifen, da der Austausch der benötigten Schlüssel gegebenenfalls ebenfalls über den Proxy läuft. Somit wird das Vertrauensproblem nicht gelöst, sondern lediglich auf den Proxy übertragen. Prinzipiell gilt: Findet sich ein vertrauenswürdiger Proxy, gewährleistet dieser einen hohen Grad an Sicherheit und Anonymität. Jedoch stellen sichere und frei verfügbare Proxy-Server derzeit eine Ausnahme dar.

Eigene Netzwerke

Im Internet existiert eine Reihe von Kommunikationsprotokollen, die es ermöglichen, eigene Netze im großen Netzwerk aufzubauen. Solche dynamischen Netzwerke nutzen weiterhin die »normale« Infrastruktur des Internets, bauen auf dieser jedoch eine softwarebasierte zusätzliche Schicht auf. Nachrichten innerhalb des Netzwerkes werden dann nur noch über ebenfalls im Netz vorhandene Knoten weitergeleitet. Auf diese Weise kann sichergestellt werden, dass Nachrichten nur über vertrauenswürdige Knoten und mit entsprechenden im Protokoll festgelegten Sicherheitsvorkehrungen gesendet werden.

Reclaim your Anonymity – in der Praxis...
Da sich in der Praxis gezeigt hat, dass ein alleiniger Einsatz einer Methode die Anonymität der eigenen Kommunikation nicht sicherstellen kann, wurden in den letzten Jahren Methoden entwickelt, die mehrere der grundlegenden Ansätze kombinieren, erweitern oder zu neuen Methoden zusammenführen.

So nutzen Programme wie TOR[7] oder I2P[9] neben dem Aufbau eigener Netzwerke auch Verschlüsselungstechniken und verschiedene Stellvertretermodelle zur Verschleierung der benutzten Verbindungen. In den letzten Jahren wurden solche Methoden in mehreren Projekten konzipiert, umgesetzt und den NutzerInnen frei zur Verfügung gestellt. Zwei der populärsten und derzeit auch am weitesten entwickelten Programme sind die bereits genannten TOR und I2P.

The Onion Router (TOR)
TOR arbeitet nach dem Zwiebelprinzip. Dabei wird die eigene Kommunikation über ein Netzwerk aus mindestens drei zusätzlichen Verkehrsknoten, den Onion Routern, geleitet. Der letzte Onion Router, auch Exit Node genannt, leitet die Nachricht dann an das eigentliche Ziel weiter und agiert somit als eine Art Stellvertreter. Jede Nachricht wird mehrfach verschlüsselt, so dass außer dem Exit Node kein Router den Inhalt oder das wirkliche Nachrichtenziel kennt. Im Gegensatz zu normalen Stellvertreter-Modellen weiß der Exit Node nicht, von wem die Nachricht wirklich kam – lediglich der vorherige Onion Router ist ihm bekannt. Somit wird das oben beschriebene Vertrauensproblem an dieser Stelle entschärft. Jedoch sollten sensible Daten immer nur über verschlüsselte Verbindungen wie https gesendet werden, um die Inhalte vor einem bösartig agierenden Exit Node zu schützen. Für TOR existieren bereits viele in normale Webbrowser integrierbare Tools, die den eigenen Internetverkehr anonymisieren. Entsprechende Anleitungen finden sich im Internet[8].

Invisible Internet Project (I2P)
I2P anonymisiert Kommunikation ebenfalls über den Aufbau eines eigenen Netzes im Netz. Jedoch liegt hier der Fokus nicht auf der Verwendung des neuen Netzes als Mittel zum Zweck, sondern auf der Schaffung eines komplett eigenständigen, dynamisch aufgebauten Netzwerkes. Jeder Rechner im I2P-Netz übernimmt demzufolge auch Funktionen eines Verkehrsknotens, das heißt er leitet Nachrichten an andere Knoten weiter. Die Anonymisierung der Kommunikation wird über konstante Verschlüsselung sowie eine zufällige Nachrichtenverteilung hergestellt. I2P wird derzeit schwerpunktmäßig zum Betrieb anonymer Webseiten – nur erreichbar für I2P-NutzerInnen – und in Filesharing-Netzwerken eingesetzt. Eine Nutzung zum Surfen im Internet ist ebenfalls möglich, jedoch kann dies analog zu TOR zu Problemen führen, wenn ein Exit Node bösartig agiert. Auch hier sollten sensible Inhalte unbedingt verschlüsselt werden. I2P kann im Internet[9] heruntergeladen werden und bietet dann direkten Zugriff auf verschiedene Features wie anonyme Blogs und E-Mails innerhalb des Netzes. Eine Anleitung findet sich ebenfalls dort[10].

Reclaim your Anonymity – der aktuelle Stand...
Beide Projekte befinden sich derzeit in einem noch recht frühen Entwicklungsstadium und werden von ihren EntwicklerInnen als nicht sicher betrachtet. Dies sollte jedoch nicht überbewertet werden: Zum einen erfordert ein Abhören von per TOR oder I2P geschützter Kommunikation immer noch einen relativ hohen Aufwand. Zum anderen ist die Sicherheit einer durch die Tools geschützten Kommunikation definitiv höher als beim Verzicht auf diese Maßnahmen. Eine Kombination mit bekannt sicheren Konzepten wie PGP oder https bringt hier bereits jetzt einen wirksamen Schutz der eigenen Kommunikation.

TOR und I2P sind – wie auch der Großteil der restlichen Entwicklungen – frei verfügbar und einsehbar. Somit werden ein Test und eine Weiterentwicklung der Systeme durch unabhängige ExpertInnen ermöglicht.

Anonyme Kommunikation im Internet, die ja ein von der Norm abweichendes Verhalten darstellt, funktioniert jedoch nur mit einer ausreichend hohen Anzahl an NutzerInnen. Wird diese Zahl nicht erreicht, ist es auch ohne Kenntnis der Inhalte möglich, Menschen, die anonyme Kommunikation nutzen, zu identifizieren und gegebenenfalls in anderer Form zu überwachen. Somit ist es wichtig, Projekte wie TOR oder I2P durch eine eigene Nutzung oder Teilnahme, zum Beispiel durch den Betrieb von Routern oder dem Testen neuer Versionen, zu unterstützen.

durito, AK-Vorrat Münster

1 Das Ende der Anonymität? Datenspuren in modernen Netzen, Bundesamt für Sicherheit in der Informationstechnik, www.bsi.de/literat/anonym/index.htm

2 BT starte freiwillige Internet-Vollüberwachung, heise security, 30.09.2008, www.heise.de/security/BT-startet-freiwillige-Internet-Vollueberwachung--/news/meldung/116753

3 EU-Kommission geht wegen Phorm gegen Großbritannien vor, heise security, 14.04.2009, www.heise.de/security/EU-Kommission-geht-wegen-Phorm-gegen-Grossbritannien-vor--/news/meldung/136167

4 Das CrypTool-Skript: Kryptographie, Mathematik und mehr, B. Esslinger, 2008, cryptool.de/download/CrypToolScript-de.pdf

5 HTTPS, Chaos Computer Club, www.ccc.de/https/

6 Die Punkte verbinden, Wolfgang Stieler, Technology Review, 05/2006, www.heise.de/tr/Die-Punkte-verbinden--/artikel/73145

7 TOR – Anonymität online, www.torproject.org/index.html.de

8 Privacy Handbuch der German Privacy Foundation, German Privacy Foundation, https://www.awxcnx.de/handbuch.htm

9 I2P Anonymous Network, www.i2p2.de/

10 Das deutsche I2P-Handbuch, planetpeer.de/wiki/index.php/Das_deutsche_I2P-Handbuch

11 Website der Computergruppe H48 mit vielen Anleitungen zur Computersicherheit, computergruppe.h48.de/

Datenschutzorganisationen

Der Chaos Computer Club e.V.
Die Informationsgesellschaft unserer Tage ist ohne Computer nicht mehr denkbar. Die Einsatzmöglichkeiten der automatisierten Datenverarbeitung und Datenübermittlung bergen Chancen, aber auch Gefahren für den Einzelnen und für die Gesellschaft. Informations- und Kommunikationstechnologien verändern das Verhältnis Mensch-Maschine und der Menschen untereinander.

Die Entwicklung zur Informationsgesellschaft erfordert ein neues Menschenrecht auf weltweite, ungehinderte Kommunikation. Der Chaos Computer Club ist eine galaktische Gemeinschaft von Lebewesen, unabhängig von Alter, Geschlecht und Abstammung sowie gesellschaftlicher Stellung, die sich grenzüberschreitend für Informationsfreiheit einsetzt und mit den Auswirkungen von Technologien auf die Gesellschaft sowie das einzelne Lebewesen beschäftigt und das Wissen um diese Entwicklung fördert.

www.ccc.de

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.
Wir sind… etwa 700 engagierte Männer und Frauen aus Wissenschaft und Praxis. Wir sind Fachleute der Informatik und Informationstechnik. Wir denken bei unserer Arbeit auch über deren Konsequenzen nach. Wir wissen, dass nicht alle Probleme technisch lösbar sind. Wir heißen alle willkommen, die Informationstechnik verwenden oder sich Gedanken über ihre gesellschaftliche Rolle machen.

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

Unsere Arbeit wird vom FIFF-Vorstand koordiniert. In wissenschaftlichen Fragen unterstützt uns der Beirat des FIFF. Wir kooperieren mit zahlreichen in- und ausländischen Initiativen und Organisationen. In zahlreichen Veröffentlichungen dokumentieren wir unsere Arbeit. Die kritische Computerzeitung FIFF-Kommunikation erscheint vierteljährlich. Aktuelle Informationen und Diskussionen gibt es in der FifF-Mailing-Liste.

www.fiff.de

Der FoeBuD e.V.
Der FoeBuD e.V. setzt sich seit 1987 mit medienwirksamen Aktionen und anerkannter Kompetenz für Bürgerrechte und Datenschutz, freie Kommunikation und eine lebenswerte Welt im digitalen Zeitalter ein. Der FoeBuD ist seither ein Kristallisationspunkt für technikaffine und politisch interessierte Menschen.

Seit 2000 organisiert der FoeBuD den jährlichen Datenschutz-Negativpreis BigBrotherAwards, der Datenschutzsünder ins Licht der Öffentlichkeit bringt. Seit 2003 hat der FoeBuD mit seiner StopRFID-Kampagne bewirkt, dass die RFID-Funktechnologie (»Schnüffelchips«) wegen ihres Überwachungspotenzials inzwischen allgemein kritisch beurteilt wird. In den letzten drei Jahren hat der FoeBuD sich insbesondere gegen die Vorratsdatenspeicherung engagiert und hat an der Organisation der Großdemonstrationen gegen Überwachung unter dem Motto »Freiheit statt Angst« führend mitgewirkt. Vertreter des FoeBuD werden von Verbänden, Bundestagsfraktionen, Ministerien und der EU-Kommission als ExpertInnen eingeladen. Der FoeBuD hat seinen Sitz in Bielefeld, ist aber deutschlandweit tätig und kooperiert mit anderen Bürgerrechtsorganisationen international.

Der FoeBuD ist unabhängig und lebt durch die Arbeit vieler Freiwilliger. Der FoeBuD ist gemeinnützig und finanziert sich durch private Spenden, Mitgliedsbeiträge und durch Einnahmen des FoeBuD-eigenen Online-Shops.

Für sein Engagement für Bürgerrechte wurde der FoeBuD 2008 mit der Theodor-Heuss-Medaille ausgezeichnet.

www.foebud.org

www.bigbrotherawards.de

DVD

Die Deutsche Vereinigung für Datenschutz e.V.
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, Verbraucherdatenschutz und Datenschutz im Internet – um nur einige zu nennen.

www.datenschutzverein.de

Die Humanistische Union
Die Humanistische Union ist eine unabhängige Bürgerrechtsorganisation. Seit unserer Gründung 1961 setzen wir uns für den Schutz und die Durchsetzung der Menschen- und Bürgerrechte ein. Wir engagieren uns für das Recht auf freie Entfaltung der Persönlichkeit und wenden uns gegen jede unverhältnismäßige Einschränkung dieses Rechts durch Staat, Wirtschaft oder Kirchen.

Die Informationelle Selbstbestimmung und die Achtung des Kommunikationsgeheimnisses bekommen im digitalen Zeitalter eine immer größere Bedeutung. Datensparsamkeit und Zweckbindung schützen nicht nur den Einzelnen, sie sichern auch die Offenheit unserer Demokratie. In einer pluralistischen Gesellschaft müssen radikale Meinungsäußerungen möglich sein.

Humanistische Union

Die Humanistische Union gehört zu den konsequenten Verfechtern des Datenschutzes, 1983 gegen die Volkszählung genauso wie heute gegen die Vorratsdatenspeicherung. Immer wieder ringen wir vor Gerichten um datenschutzrechtliche Mindeststandards für staatliche Stellen: gegen Große Lauschangriffe, IMSI-Catcher, Online-Durchsuchungen oder die Steuer- ID.

www.humanistische-union.de

Der Arbeitskreis Vorratsdatenspeicherung
Der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) ist ein bundesweiter Zusammenschluss, der sich gegen die ausufernde Überwachung im allgemeinen und gegen die Vollprotokollierung der Telekommunikation und anderer Verhaltensdaten im Besonderen einsetzt.

Mitglieder des Arbeitskreises sind einzelne Bürgerrechtler, Datenschützer und Internetnutzer, aber auch Verbände, Organisationen und Initiativen. Sie engagieren sich gegen die anlasslose Speicherung persönlicher Daten, für mehr Datenschutz, für das Recht auf Privatheit, für unbeobachtete Kommunikation und für den Respekt vor der Menschenwürde, besonders für das Recht auf Informationelle Selbstbestimmung.

Sie informieren unter anderem bei verschiedensten Veranstaltungen durch Vorträge, Informationsmaterial und Kunstaktionen, organisieren friedliche Proteste und Lobby-Arbeit, und legen wenn nötig auch Verfassungsbeschwerde ein. Der Arbeitskreis arbeitet international mit vergleichbaren Initiativen und Vereinigungen zusammen. Der Arbeitskreis Vorratsdatenspeicherung ist politisch unabhängig und überparteilich.

www.vorratsdatenspeicherung.de

Ortsgruppe Münster
http://wiki.vorratsdatenspeicherung.de/Ortsgruppen/Muenster

Der Republikanische Anwältinnen- und Anwälteverein (RAV)
Der RAV ist eine politische Anwaltsorganisation. Wir verstehen uns als Teil der Bürgerrechtsbewegung und arbeiten auf nationaler wie auf internationaler Ebene mit zahlreichen Verbänden sowie mit Gruppen der Neuen Sozialen Bewegungen zusammen. Themenschwerpunkt des RAV sind unter anderem die Verschärfungen des Straf- und des Strafprozessrechts, Polizeigewalt und die ständige Ausweitung polizeilicher Befugnisse sowie der Kampf gegen ein diskriminierendes Ausländer- und Asylrecht.

RAV

Der RAV nimmt Einfluss auf rechtspolitische Entwicklungen unter anderem durch Beteiligung an der öffentlichen und fachöffentlichen Diskussion oder Stellungnahmen gegenüber der Legislative und dem Bundesverfassungsgericht. Bei demonstrativen Großereignissen unterstützt der Verein den Aufbau und die Arbeit von »Legal Teams«. Außerdem betreibt der RAV anwaltliche Fortbildung durch Fachanwaltskurse und sonstige berufliche Fortbildungsveranstaltungen.

Gemeinsam mit anderen Bürger- und Menschenrechtsorganisationen gibt der RAV jährlich den Grundrechtereport zur Lage der Bürger- und Menschenrechte in Deutschland heraus. Hintergrundberichte und Diskussionsbeiträge zu aktuellen rechtlichen Entwicklungen und Auseinandersetzungen publiziert der RAV außerdem in regelmäßig erscheinenden Infobriefen.

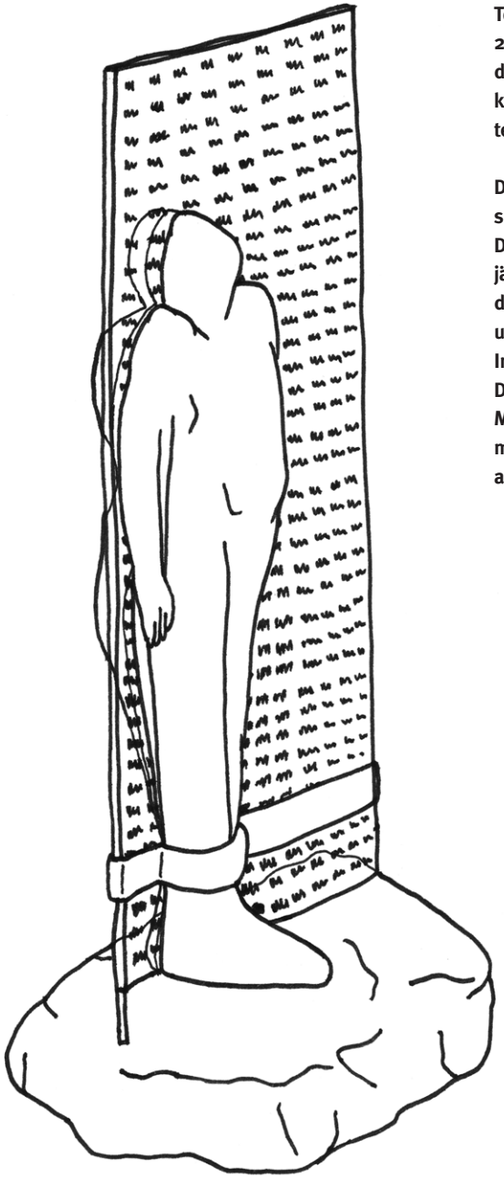
www.rav.de

Die Datenschutzgruppe der Roten Hilfe
Die Datenschutzgruppe der Roten Hilfe beschäftigt sich vorrangig mit dem Einsatz von EDV (und anderer Hi-Tech) durch Repressionsbehörden von Staatsanwaltschaften über Polizeien bis hin zu Geheimdiensten.

Dabei versuchen wir auf unserem Wiki (datenschmutz.de) einen Überblick über die bestehenden Ge- und Missbräuche zu schaffen (und zu gewinnen). Von dort ist auch ein Generator für Auskunftsersuchen an die verschiedenen Behörden zu finden. Physisch sind wir vor allem um Heidelberg konzentriert, was aber niemanden von einer Mitarbeit abhalten muss.

www. datenschmutz.de

Oscar für Datenkraken und ÜberwacherInnen



Topfavorit Telekom hat jüngst beim Big Brother Award 2008 abgeräumt. Aber auch der Europäische Ministerrat, der Bundestag, ein Stromversorger und eine Krankenkasse waren erfolgreich, wenn es darum ging, mit privaten Daten grob fahrlässig umzugehen.

Die Deutsche Telekom AG schickte sogar ihren Datenschutzbeauftragten, um den Preis entgegen zu nehmen. Der an den Roman »1984« angelehnte Award wird jährlich in verschiedenen Kategorien durch den Bielefelder Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBuD e.V.) verliehen. Im Oktober 2008 war es nun endlich wieder so weit. Die größten Datenkraken Deutschlands wurden für ihre Mühen belohnt. Doch Freude wollte unter den derart mit ungewollter Publicity überhäuften nicht recht aufkommen.

Die Preisträger

Kategorie »Europa«

In der Kategorie »Europa« war in diesem Jahr der Ministerrat der Europäischen Union siegreich, der sich durch die Einführung der »EU-Terrorliste« und die hierdurch entstandene Stigmatisierung sowie Diskriminierung einzelner Personen sowie Organisationen erfolgreich für den Big Brother Award qualifiziert hat. Diese undemokratisch und in einem unter Geheimhaltung tagenden Gremium erstellte Liste potentieller Terroristen ist in viele Fällen weder durch ausreichende Beweise begründet noch hinreichend überprüft worden. Alle Institutionen und Bürger innerhalb der Europäischen Union sind verpflichtet, die mit dieser Liste verbundenen Sanktionen auf die Terrorverdächtigen anzuwenden. Ihre Kreditkarten werden gesperrt, der Zugang zu ihrem Vermögen unterbunden, ihre Löhne zurückgehalten, Sozialleistungen jeglicher Art verweigert sowie der Pass entzogen.

Die Betroffenen erleiden durch diese Vorgehensweise wirtschaftliche, politische sowie soziale Ausgrenzung und werden über den bestehenden Verdacht nicht informiert. Für diese ausgesprochen drakonischen Maßnahmen und Grundrechtsverletzungen wurden Ratspräsident Bernard Kouchner zusammen mit Generalsekretär Javier Solana durch den diesjährigen Preis in der Kategorie »Europa« belohnt.

»Gesundheit und Soziales«

In der Kategorie »Gesundheit und Soziales« konnte sich in diesem Jahr die Deutsche Angestellten-Krankenkasse (DAK) erfolgreich gegen die Konkurrenz durchsetzen. Die DAK hat die persönlichen Daten von 200.000 chronisch kranken Patienten an eine Privatfirma weitergegeben, ohne die Betroffenen darüber zu informieren oder überhaupt erst deren Einverständnis einzuholen. Ein privater Dienstleister sollte durch telefonische Beratung chronisch kranker Patienten zu Kosteneinsparungen bei der DAK beitragen. Daten dieser Art unterliegen jedoch dem Sozialgeheimnis nach § 35 SGB I. Somit hat sich die DAK grob fahrlässig im Umgang mit ihren Kundendaten verhalten. Gratulation.

»Verbraucher«

Der Deutsche Bundestag konnte sich den Preis in der Kategorie »Verbraucher« durch sein tatkräftiges Engagement im Bereich der Verschärfung der Gesetzte zur Reisekontrolle sichern. Durch das Gesetz zur Änderung seeverkehrsrechtlicher, verkehrsrechtlicher und anderer Vorschriften mit Bezug zum Seerecht erfahren nun nicht nur die Schifffahrtsbehörden von Kreuzfahrten und Ozeanüberquerungen, sondern auch die Bundespolizei. Des weiteren ist die Weitergabe der persönlichen Daten auch an ausländische Behörden sowie private Unternehmen ohne die Einwilligung der Betroffenen möglich. Wir sind dem Bundestag für diese ausführliche Protokollierung der Reisedaten von jährlich ca. 29 Millionen Bürgern nachdrücklich zu Dank verpflichtet.

Außerdem werden durch ein neues Abkommen mit den USA nun die Daten von Flugpassagieren mit dem dortigen Ministerium für Heimatschutz abgeglichen. Das Wort

Generalverdacht scheint im Deutschen Bundestag demnach noch nicht angekommen zu sein.

Ein weiterer Preisträger in dieser stark umkämpften Kategorie war der Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. (ADM), welcher Telefoninterviews ohne das Einverständnis und Wissen der Betroffenen von Dritten mithören ließ. Die Richtlinie für telefonische Befragungen des ADM empfiehlt diese rechtswidrige Praxis ausdrücklich, wodurch er sich neben den Deutschen Bundestag als würdiger Preisträger des Big Brother Awards in der Kategorie »Verbraucher« qualifiziert hat.

»Arbeitswelt und Telekommunikation«
Der unumstrittene diesjährige Favorit, die Deutsche Telekom AG, hat sich durch ihr herausragendes Engagement im weiten Feld der Datenschlamperei sowie Verstößen gegen den Datenschutz in der Kategorie »Arbeitswelt und Telekommunikation« durchsetzen können. Durch den illegalen Zugriff auf Telefonverbindungsdaten war die Telekom nicht nur in der Lage, Journalisten, sondern auch den eigenen Aufsichtsrat effizient zu überwachen. Damit hat sie sich gleich mehrerer Gesetzesverstöße schuldig gemacht und gezeigt, wie wenig ihr das hohe Gut der Pressefreiheit sowie die Privatsphäre der Betroffenen wert ist.

BIG BROTHER AWARDS.de

Hierdurch versuchte das Unternehmen den Grundsatz des Quellenschutzes der journalistischen Arbeit zu unterwandern. Dies zeugt von ausgesprochener Geringschätzung der bestehenden Gesetze durch die Unternehmensleitung. Die Deutsche Telekom AG hat somit keine Kosten und Mühen gescheut, um dieses Jahr durch ihren Datenschutzbeauftragten den Big Brother Award entgegennehmen zu können.

»Technik«
Durch ihre maßgebliche Rolle bei der Einführung und Entwicklung des Digitalstrom-Prinzips hat sich die Yello Strom GmbH ihre Trophäe in der Kategorie »Technik« sichern können. Durch digitalen Strom soll es in naher Zukunft möglich sein, den Stromverbrauch durch den Einbau spezieller Mikrochips auf die einzelnen Haushaltsgeräte zurückzuführen. Durch die Digitalstrom-ID kann jedes Gerät nun exakt samt Verbrauchsintensität und Zeitpunkt des Gebrauchs erfasst werden. Somit wären Stromanbieter in der Lage, den Tagesablauf ihrer Kunden anhand ihrer Nutzungsprofile genauestens zu rekonstruieren.

Angesichts der bestehenden Begehrlichkeiten von Seiten des Staates, aber auch der Wirtschaft stellt sich natürlich die Frage, was mit diesen Daten geschieht, da ein angemessenes Datenschutzkonzept bisher fehlt. Man darf gespannt sein, was die zukünftigen Entwicklungen im Bereich des digitalen Stroms bringen werden. Vorerst Gratulation für die Entwicklung dieser neuen Überwachungsmöglichkeit.

»Politik«
In der Kategorie »Politik« konnte das Bundesministerium für Wirtschaft und Technologie den Preis für sich beanspruchen. Durch ihre Zustimmung zum ELENA-Verfahren, welches in Zukunft eine elektronische Signatur verpflichtend machen wird, hat sich das Bundesministerium gegen die anderen Nominierungen erfolgreich durchsetzen können. ELENA steht für den elektronischen Einkommensnachweis, der die zentrale Speicherung der Einkommensdaten durch Informationen der Arbeitgeber ermöglichen soll.

Des weiteren soll in Zukunft nur noch mit einer so genannten Job Card der Zugang zu Sozialleistungen gewährt werden. Auch die digitale Geschäftsabwicklung soll durch eine persönliche digitale Signatur ermöglicht werden. Datenschützer sehen auf Grund dieser langfristig angelegten zentralisierten Datensammlung ein hohes Missbrauchspotential, da die Zugriffskompetenzen unter Umständen auch auf weitere Behörden ausgeweitet werden können. Ein kleiner Schritt für Michael Glos, ein großer Schritt in Richtung des gläsernen Bürgers für jeden Bundesbürger.

Mehr Informationen zum Thema Big Brother Awards finden sich auf der Homepage (www.bigbrotherawards.de). Die Veranstalter freuen sich natürlich über Einsendungen und Nominierungsvorschläge.

Katharina Maria Nocun

Grundgesetz – das steht dir zu…

Allgemeines Persönlichkeitsrecht
Das Persönlichkeitsrecht betont das Recht auf Achtung und Entfaltung der Persönlichkeit. Es stützt sich auf Artikel 1 (1) und Artikel 2(2).

Informationelle Selbstbestimmung (Abgeleitet aus dem Volkszählungsurteil von 1983)
»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 Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.«

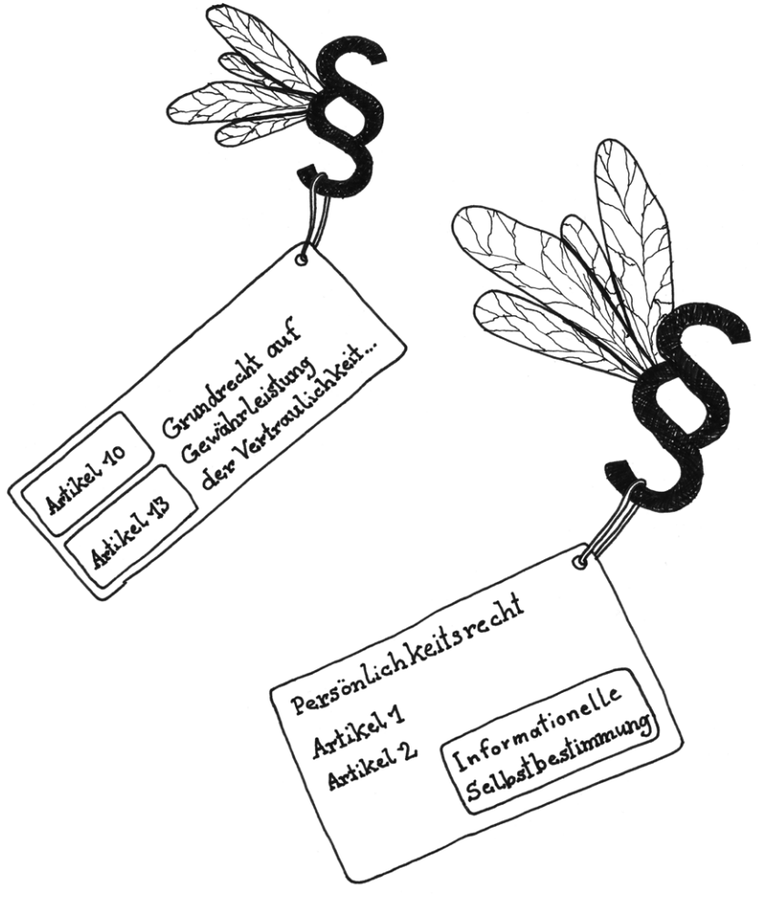
Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
Das neue Grundrecht wurde abgeleitet aus dem Urteil des Bundesverfassungsverichts zur Verfassungsbeschwerde bezüglich der Online-Durchsuchung in Nordrhein-Westfalen und soll durch technische Neuerungen entstehenden Lücken zwischen Artikel 10 (1) und 13 (1) schließen.

Das allgemeine Persönlichkeitsrecht, welches sich aus Artikel 2 (1) in Verbindung mit Artikel 1 (1) des Grundgesetz ergibt, beinhaltet somit auch ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. In der Praxis bedeutet dies den Schutz der BürgerInnen vor Zugriffen auf Computer, Netzwerke und vergleichbare Systeme, wenn diese ihre Persönlichkeitsrechte einschränken.

Artikel 1
(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Artikel 2
(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

Artikel 3
(3) Niemand darf wegen seines Geschlechtes, seiner Abstammung, seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner religiösen oder politischen



Anschauungen benachteiligt oder bevorzugt werden. Niemand darf wegen seiner Behinderung benachteiligt werden.

Artikel 5
(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.

Artikel 8
(1) Alle Deutschen haben das Recht, sich ohne Anmeldung oder Erlaubnis friedlich und ohne Waffen zu versammeln.

Artikel 10
(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

Artikel 13
(1) Die Wohnung ist unverletzlich.

Artikel 17
Jedermann hat das Recht, sich einzeln oder in Gemeinschaft mit anderen schriftlich mit Bitten oder Beschwerden an die zuständigen Stellen und an die Volksvertretung zu wenden.

Artikel 19
(2) In keinem Falle darf ein Grundrecht in seinem Wesensgehalt angetastet werden.

Auskunftsersuchen

Das Grundrecht auf Informationelle Selbstbestimmung ermöglicht uns, frei über die Preisgabe und Verwendung unserer persönlichen Daten zu bestimmen. Das gilt auch nach der Herausgabe der Daten an staatliche Stellen oder private Dritte, zum Beispiel beim Abschluss eines Mobilfunkvertrags. Auskunftsersuchen stellen ein einfaches Mittel dar, Transparenz bezüglich der Verbreitung und Verwendung der eigenen Daten herzustellen, und so eine Basis für weitere Schritte zur Wahrnehmung unseres Grundrechts zu schaffen.

Rechtliche Grundlagen

Die aus dem Grundrecht auf Informationelle Selbstbestimmung abgeleiteten Auskunftsansprüche sind derzeit (Mai 2009) im Bundesdatenschutzgesetz (BDSG) und den jeweiligen Landesdatenschutzgesetzen verankert – zur Vereinfachung wird hier nur das BDSG betrachtet.

§ 19 regelt die Auskunftspflichten staatlicher Institutionen bei Eingang eines Ersuchens. § 34 beinhaltet die Regelungen zur Auskunft von Unternehmen gegenüber Auskunft ersuchenden Personen. Beide Paragraphen verpflichten die Datensammler, Auskunft über die Art, den Umfang, die Herkunft (§ 34 Absatz I, Satz 1), den Zweck (§ 34 Absatz I, Satz 3) und gegebenenfalls weitere EmpfängerInnen der Daten (§ 34 Absatz I, Satz 2) zu geben.

Diese Ansprüche unterliegen jedoch gewissen Einschränkungen. So kann zum Beispiel die Auskunft über Herkunft und Weitergabe der Daten verweigert werden, weil sie das Geschäftsgeheimnis eines Unternehmens gefährden würde (§ 34 Absatz I Satz 3, Absatz II Satz 2) oder die Erfüllung der Aufgaben einer staatlichen Stelle, zum Beispiel bei laufenden Ermittlungen, verhindern würde (§ 19 Absatz IV, Satz 1).

Wird eine Auskunft verweigert, besteht zumindest bei der Speicherung durch staatliche Stellen die Möglichkeit, die Herausgabe der Daten an die jeweilige Datenschutzbeauftragte zur Prüfung des Sachverhaltes zu veranlassen (§ 19 Absatz VI).

Wirkung

Auf Basis der erlangten Informationen können dann weitere Schritte wie die Löschung der eigenen Daten oder auch eine Beschwerde bei der zuständigen Beauftragten für Datenschutz eingeleitet werden. Neben der Ermöglichung dieser direkt spürbaren Aktionen erfüllen Auskunftsersuchen noch zwei weitere Funktionen:

Zum einen können sie eine Prüfung der datenschutzrelevanten Praktiken von Unternehmen und Behörden erwirken, die Druck auf Einzelne oder auch Gruppen von Datensammlern aufbaut oder verstärkt. Zum anderen erzeugen sie insbesondere im Falle von an Behörden gerichteten Ersuchen einen nicht unerheblichen Aufwand, welcher diese gegebenenfalls von der Auswertung bestehender oder Ausführung neuer Datensammlungen abhält.

Dem Risiko, durch das Versenden eines Auskunftsersuchens eigene Daten preiszugeben, kann im Falle von Unternehmen durch ein bewusstes Stellen der Ersuchen an Unternehmen, die die eigenen Daten bereits haben, begegnet werden. Im Falle staatlicher Institutionen wird ein Auskunftsersuchen bei Vorliegen von Daten keinen größeren Ausschlag mehr produzieren. Weitere Details und Erfahrungen zum Umgang solcher Institutionen mit Auskunftsersuchen finden sich bei »Datenschmutz«[1]. Auskunftsersuchen ziehen in der Regel keine Kosten auf Seiten der Anfragenden nach sich.

Zusätzlich kann der Stigmatisierung einzelner Personen über die Nutzung der Auskunftsansprüche durch möglichst viele Menschen begegnet werden. Zu diesem Zweck existiert bereits eine kleine Anzahl an Webseiten, die entsprechende Musterbriefe und Tips bereitstellen[2,3]. Hervorzuheben sind hier die Reclaim your data-Kampagne[4] sowie der Generator für Auskunftsersuchen der Datenschutzgruppe der Roten Hilfe[5], welcher automatisch Ersuchen für sämtliche Polizeibehörden in Deutschland generieren kann.

AK-Vorrat Münster

1 Auskunftsersuchen, Datenschutzgruppe der Roten Hilfe https://www.datenschmutz.de/cgi-bin/moin.cgi/AuskunftErsuchen

2 Deine Daten gehören Dir! Hol Sie Dir zurück!, Datenschutz ist Bürgerrecht, https://www.datenschutz-ist-buergerrecht.de/deine-daten-gehoeren-dir

3 Datenscheckheft, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, https://www.ldi.nrw.de/mainmenu_Service/submenu_Informationsmaterial/Inhalt/Datenscheckheft/Datenscheckheft.php

4 Reclaim your data from the European police authorities!, http://euro-data.noblogs.org

5 Generator für Auskunftsersuchen, Datenschutzgruppe der Roten Hilfe, https://www.datenschmutz.de/cgi-bin/auskunft

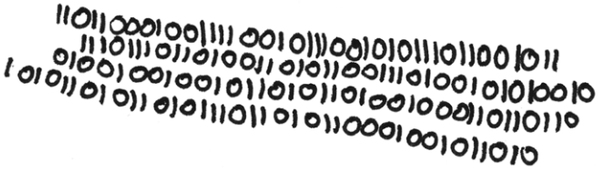
Glossar

Anonyme Mailer Programme, die es erlauben, E-Mails anonym zu versenden. Zu diesem Zweck werden verschiedene Verschleierungstechniken wie Verschlüsselung, Verzögerung und Umleitung eingesetzt. E-Mails benötigen allerdings mehr Zeit, bis sie bei der EmpfängerIn ankommen. Das am weitesten verbreitete Tool ist Mixmaster, welches auch über verschiedene Webseiten als einfach zu bedienender Dienst angeboten wird.

Anonyme Suchmaschine Eine Internet-Suchmaschine, die im Gegensatz zu den üblichen Anbietern darauf verzichtet, Suchanfragen zu speichern, den anfragenden Computer eindeutig zu identifizieren und auf dieser Basis Profile von den NutzerInnen zu erstellen. Kommen daher meistens auch ohne lästige Werbung aus. Die Ergebnisse sind dank des Anzapfens der kommerziellen Anbieter absolut konkurrenzfähig. Zwei bekannte anonyme Suchmaschinen können unter scroogle.org/ und ixquick.com/ genutzt werden.

Bilderkennungsprogramm Eine Software zur automatischen Identifizierung von Objekten in Bildern. Dies reicht von einfacher Geometrie (bei der Stauanalyse) bis hin zu ausgefeilten Sicherheits- und Überwachungssystemen (Gesichtserkennung in Flughäfen). RFID (Radio Frequency Identification) – Eine Technik zum kontaktlosen Austausch von Daten. ➳ Artikel RFID, S. 16 ff

Biometrie Alle Arten von automatischen Erkennungsverfahren, die auf biologischen Merkmalen von Personen basieren. Dies können unter anderem Fingerabdrücke, Fotos oder Informationen über das Erbgut eines Menschen sein. In den letzten Jahren erfolgte eine zunehmende Erfassung biometrischer Informationen, zum Beispiel auf Pässen, sowie die stetige Verbesserung automatischer Erkennungssysteme. ➳ Bilderkennungsprogramm



Bit, Byte, kB, MB, GB,... Maßeinheiten zur Angabe der Größe elektronisch gespeicherter Daten. Ein Bit stellt dabei die (derzeit) kleinstmögliche Einheit dar. 1024 Byte = 1 Kb, 1024 kB = 1 MB, und so weiter.

BMI (Bundesministerium des Innern) Dazu müssen wir wohl nichts mehr schreiben…

Bonusprogramme (Payback, etc.) Bonusprogramme sind eine gängige Strategie von Privatunternehmen, an die Daten ihrer Kunden zu gelangen. Dank ausgeklügelter Rabattsysteme entsteht somit ein Anreiz für den Kunden in den an dem Bonussystem beteiligten Unternehmen einzukaufen und dabei sein Konsumverhalten hemmungslos Preis zu geben, so dass man ihn noch wirkungsvoller mit personalisierter Werbung belästigen kann.

BSI (Bundesamt für Sicherheit in der Informationstechnik) Der zentrale IT-Sicherheitsdienstleister des Bundes. Zuständig unter anderem für die elektronische Sicherheit von Verwaltungen der Kommunen und die Beratung von Unternehmen.

Data Mining Das Suchen von Mustern (Klassen von Personen oder Objekten, Verhaltensweisen,…) in zumeist großen Datenbeständen. Wird sowohl in der Wirtschaft (Warenkorbanalysen, Bewegungsmuster von KundInnen) als auch auf staatlicher Seite (Rasterfahnung) eingesetzt.

Digitale Identifikation Die eindeutige Identifizierung einer Person oder eines Objektes mit elektronischen Mitteln, zum Beispiel EPA oder ePass.

Datenbank Eine Software zur dauerhaften Speicherung großer Mengen von Informationen. Diese können anderen Programmen oder NutzerInnen, je nach Anwendungsfall der aufbereiteten Formen, zur Verfügung gestellt werden. Ein Datensatz ist die kleinste Einheit von in einer Datenbank gespeicherten Informationen, zum Beispiel eine Adresse in einem Telefonbuch. Datenbanken werden in verschiedensten Bereichen eingesetzt, vom persönlichen Adressbuch im Handy bis hin zu Internet-Suchmaschinen.

e-Government Die Abwicklung von Behördengängen und Verwaltungsprozessen in elektronischer Form. Oftmals werden die Dienste den Bürgern online angeboten. Prominentes Beispiel hierfür ist die elektronische Steuererklärung (ELSTER).

Elektronische Gesundheitskarte oder auch eCard/ eGK Soll die bisher in Deutschland verwendete Krankenversicherungskarte zukünftig ersetzen. ➳ Artikel, S. 26 ff

Filesharing Das Tauschen von Dateien (Dokumente, Fotos, Musik, Videos, Software) zwischen zwei oder mehr Menschen. Filesharing geschieht zumeist in dezentralen und offenen Netzwerken, in denen NutzerInnen ihre Dateien anderen zur Verfügung stellen. Entgegen der vor allem von der Musik- und Softwareindustrie vertretenen Meinung ist der Großteil des Verkehrs in Filesharing-Netzwerken auf legale Transaktionen, zum Beispiel zur Verteilung freier Software oder von den KünstlerInnen frei zur Verfügung gestellter Musik, zurückzuführen.

Filtersoftware Programme, die bestimmte Inhalte oder ganze Klassen von Inhalten aus Daten extrahiert. Dies können Teile aus dem Verkehr in einem Netzwerk wie dem Internet sein oder auch bestimmte Farbwerte bei Bildbearbeitungsprogrammen. Der Einsatz von Filtersoftware ist nicht prinzipiell abzulehnen, so werden zum Beispiel Firewalls eingesetzt, um Computer vor Angriffen zu schützen, jedoch kann mit ihnen auch

beträchtlicher Schaden angerichtet werden, wenn zum Beispiel die Pressefreiheit mit solcher Software eingeschränkt wird.

Gesinnungstests Ein für aus 26 – zumeist islamischen – Ländern stammende und in NRW lebende Studierende verpflichtender Fragebogen. Dieser enthält unter anderem detaillierte Fragen zur Herkunft, Religionszugehörigkeit, politischer Einstellung und dem Kontakt zu terroristischen Gruppen.

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme Ein im Rahmen der Urteile zu den Verfassungsbeschwerden gegen die Online-Durchsuchung von Computern vom Bundesverfassungsgericht am 27.02.2008 neu formuliertes Grundrecht. Es ergänzt die die Grundrechte des Telekommunikationsgeheimnisses (Art. 10 Abs. 1 GG) und der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) sowie das Recht auf Informationelle Selbstbestimmung und schützt die privaten informationstechnischen Systeme, zum Beispiel PCs und Mobiltelefone vor staatlichen Eingriffen. Eine Aufhebung dieses Schutzes ist jedoch unter bestimmten Voraussetzungen möglich.

I2P (Invisible Internet Project) Eine Software, die unter ihren Nutzern ein eigenes, dezentrales Netzwerk im Internet aufbaut. Es kann wie Tor zum anonymen Surfen genutzt werden. Weiterhin können anonym Websites eingestellt/betrieben werden, die allerdings nur von anderen Nuztern des I2P-Netzwerks eingesehen werden können. Befindet sich aktuell in der Entwicklung und steht frei zum Download unter: www.i2p2.de/ Eine Anleitung gibt es bei: www.planetpeer.de/wiki/index.php/Das_deutsche_I2P-Handbuch

Informationelle Selbstbestimmung Dieses Datenschutz-Grundrecht ist eine Ausprägung des allgemeinen Persönlichkeitsrechts. Es bezeichnet das Recht jeder Einzelnen/jedes Einzelnen, über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen.

Internetausdrucker Bezeichnung für Menschen, die Computer als moderne Schreibmaschinen und das Internet für eine sehr bunte Zeitung, aber kein eigenständiges Kommunikationsmedium halten. Dieser eher geringe Wissensstand hält Internetausdrucker allerdings nicht davon ab, Gesetze zur verstärkten Kontrolle des unbekannten Wesens Internet zu fordern oder zu verabschieden.

Karlsruhe-Touristen Laut R. Wendt, dem Vorsitzenden der Polizeigewerkschaft, die angemessene Bezeichnung für Menschen, die die Beschneidung oder Abschaffung ihrer Grundrechte nicht gleichgültig hinnehmen, sondern Beschwerden beim Bundesverfas-

sungsgericht einreichen. Gerüchten zu Folge sollen diese Menschen sogar des Öfteren Recht bekommen…

Kategorisierung Die Erstellung von bestimmten Klassen von Objekten. Dies geschieht meistens anhand von mehr oder minder gut trennbaren Eigenschaften wie Größe, Geschlecht oder Form.

Klassifikation Die Zuweisung von Objekten zu bestimmten Klassen anhand ihrer Eigenschaften, zum Beispiel Kundenklassen (normale und VIP-Kunden) oder Subkulturen.

Klickzahlen Die Anzahl der Aufrufe einer einzelnen Website oder Teilen davon. Dabei wird nicht nur der Besuch als Ganzes registriert, sondern jeder Klick auf einzelne Elemente wie zum Beispiel Schaltflächen oder Links. Somit können detaillierte Nutzungsprofile erstellt werden.

Leiterschleifen Geräte, die in der Lage sind, ein magnetisches Feld zu erzeugen und mit diesem RFID-Chips mit Energie zu versorgen. Sie werden in der Regel mit Lesegeräten für die Chips kombiniert. Die bekannteste Variante solcher Geräte sind die Diebstahlsicherungen am Ausgang von Geschäften. Die beachtliche Größe der Geräte ist dabei keineswegs notwendig, sondern dient vielmehr der Abschreckung.

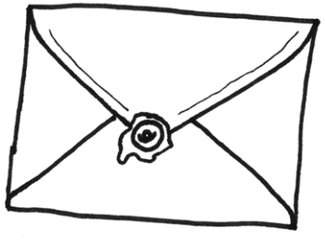
Linux Ein Oberbegriff für eine Familie von frei verfügbaren Betriebssystemen, die ein gemeinsames Basissystem, den Kernel, nutzen. Durch den modularen Aufbau und die Freigabe sämtlicher Quellcodes bieten Linux-Systeme den NutzerInnen ein hohes Maß an Flexibilität, Transparenz und Kontrolle. Es existiert eine Vielzahl von direkt einsetzbaren und professionell weiterentwickelten Linux-Varianten für fast jeden erdenklichen Zweck. Populäre Linux-Distributionen sind unter anderem Debian, Ubuntu, SUSE und Knoppix.

LiveCD Eine CD, die ein Betriebssystem enthält, welches ohne Installation benutzt werden kann. Somit bietet sich die Möglichkeit, ein auf die eigenen Bedürfnisse zugeschnittenes System nahezu unabhängig vom gerade vorhandenen Rechner zu verwenden. Oftmals werden LiveCDs auch für Spezialaufgaben wie Datensicherungen oder Reparaturen eingesetzt. LiveCDs von Linux-Systemen sind besonders weit verbreitet.

Open Source Programme Programme, welche unter Open Source Lizenzen laufen, haben die Eigenschaft offen und frei zu sein. Offen, da der Quellcode (das was hinter der Benutzeroberfläche passiert) im Gegensatz zu proprietärer Software für jeden frei zu-

gänglich ist. Wenn man möchte kann man das Programm also nach Lust und Laune verändern. Frei, da jeder es nutzen darf ohne durch Lizenzen eingeschränkt zu werden. Meistens sind Open Source Programme auch kostenlos.

Opt-In/Out Verfahren zur Zustimmung der Erhebung, Speicherung und Verwendung personenbezogener Daten durch Dritte. Beim Opt-In müssen die NutzerInnen der Verwendung explizit zustimmen, zum Beispiel durch Setzen eines gesonderten Häckchens zur Zustimmung innerhalb der AGB. Opt-Out-Verfahren hingegen erfordern den expliziten Widerspruch zur Verwendung der Daten.



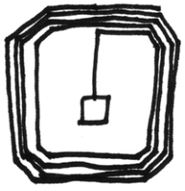
Panoptismus Ein von Michel Foucault eingeführter Begriff, der besagt, dass zunehmende Kontroll- und Überwachungsmechanismen ein einem Staat zwangsläufig auf das Verhalten seiner Bürger Einfluss nimmt und letztlich zu mehr Konformität führt. Unabhängig von einer tatsächlich stattfindenen Beobachtung kommt es zu einer Selbstdisziplinierung eines Individuums. Allein die Vorstellung solch einer potentiellen Überwachung wird die Person veranlassen, ihr Verhalten an gestellte normative Erwartungen anzupassen. Auf längere Sicht führt dies zu einer Verinnerlichung von Normen. An die Stelle eines Fremdzwangs (zum Beispiel von staatlicher Seite), tritt ein Selbstzwang. Diese Formen der indirekt wirkenden Disziplinierung in der Gesellschaft und der repressiven Machttechnik können auch die Auswirkungen von technischen Entwicklungen und Instrumenten wie Videoüberwachung oder Vorratsdatenspeicherung sein.

Personalisierung Die individuelle Gestaltung von Inhalten auf Basis der personenbezogenen Informationen über einen Menschen. Dies reicht von Werbung auf Webseiten bis hin zu speziellen Produktangeboten.

Personenbezogene Daten Datensätze, die detaillierte Informationen über einen Menschen beinhalten. Dies kann beim Namen beginnen und geht über Telefonnummern bis hin zum Konsumverhalten.

PGP (PrettyGoodPrivacy) Die am meisten genutzte Verschlüsselungssoftware. Hauptsächlich wird sie zur Verschlüsselung von E-Mails eingesetzt. Selbstverständlich frei verfügbar, sicher und für (fast) alle E-Mail-Programme geeignet. Eine Anleitung, Erklärung und Links zum Download findet ihr hier: www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/index.htm

Phishing Das bewusste Vortäuschen falscher Tatsachen (»Diese Seite ist die Online-Banking-Webseite der Bank XY«) zum Zweck der eigenen Bereicherung (»Danke für die Eingabe Ihrer Kontonummer und Ihrer PIN…«). Im Gegensatz zu normaler Werbung werden allerdings gar keine Gegenleistungen angeboten und der Preis der »Produkte« ist deutlich höher.



PIN (Persönliche Identifikations-Nummer) Eine (meistens) geheime Kombination aus Zahlen und/oder Buchstaben, mit der sich ein Mensch gegenüber anderen eindeutig ausweisen kann. Das wohl bekannteste Beispiel für eine PIN ist die Geheimnummer einer EC-Karte.

Profiling Das massive Sammeln von detaillierten Daten (Bewegungsmuster, Kommunikationsverahlten, soziale Kontakte, Konsum,…) über eine Person zu einem bestimmten Zweck. Dabei wird im Gegensatz zum Data Mining nicht mit einer großen Menge von Objekten gestartet, sondern eine einzelne Person in den Fokus gestellt. Wird unter anderem in Ermittlungsverfahren eingesetzt.

Qualifizierte Elektronische Signatur Das elektronische Gegenstück zu einer (notariell) beglaubigten Unterschrift.

Quellcode Der für Menschen lesbare, in einer Programmiersprache geschriebene Text einer Software.

Rasterfahndung Die (automatisierte) Suche nach Objekten auf Basis von bestimmten Merkmalen (Raster). Voraussetzung für die Rasterfahndung ist eine umfassende Vernetzung von Datenbanken. Diese werden aufbereitet, um einzelne Datensätze anhand der gewünschten Merkmale finden zu können (Rastern der Daten). Ein mögliches Raster wäre die Suche nach männlichen Studenten in Münster (FH und WWU), die in einer Wohngemeinschaft leben und keine GEZ-Gebühren zahlen. Die Rasterfahndung birgt eine hohe Wahrscheinlichkeit für falsche Verdächtigungen und verstößt oftmals gegen geltende Datenschutzbestimmungen. Deshalb ist sie in den letzten Jahren stark kritisiert und in vielen Fällen von Gerichten für nicht zulässig erklärt worden.

Scoring Scoring ist ein automatisiertes Verfahren, mit welchem Individuen anhand ihrer Merkmale (zum Beispiel Alter, Wohnort, Herkunft) von Unternehmen in bestimmte Kategorien eingeordnet werden. Es kann beispielsweise sein, dass man als Bewohner einer nicht ganz so wohlhabenden Gegend keinen kurzfristigen Kredit eingeräumt bekommt, da das System dies als Anzeichen für eine unzureichende Zahlungsfähigkeit wertet. Die für Scoring verwendeten Verfahren führen somit oftmals zu einer Diskriminierung, ohne das der Betroffene davon erfährt.

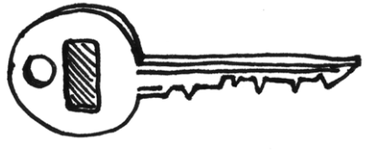
Soziales Netzwerk (im World Wide Web) Eine Website, die es Menschen ermöglicht, im Internet Kontakte untereinander aufzubauen und zu pflegen. In der Regel werden in sozialen Netzwerken von den NutzerInnen eigene Profilseiten erstellt, die oftmals detaillierte Informationen über die eigene Person enthalten und anderen NutzerInnen

zugänglich sind. Soziale Netzwerke sind oft auf eine spezielle Interessengruppe zugeschnitten. Beispiele für soziale Netzwerke sind: StudiVZ (Studierende), Xing (geschäftliche Kontakte), MySpace (Musikinteressierte & Musiker). Webseiten, die soziale Netzwerke anbieten, werden auch als Online-Plattform bezeichnet, da die Nutzer selbst einen Teil des Inhalts beitragen.

SteuerID Die seit 2008 verteilte eindeutige Identifikationsnummer für alle steuerlich relevanten Vorgänge. Diese wird bei der Geburt an jeden Bundesbürger vergeben und bleibt gültig, bis sie nicht mehr benötigt wird (maximal 20 Jahre nach dem Tod).

TOR (The Onion Router) Das derzeit populärste Programm, um anonym im Internet zu surfen. Es ist frei verfügbar, einfach zu nutzen (wirklich) und wird ständig weiterentwickelt. Infos und Download unter https://www.torproject.org/

Überwachungsmaßnahmen Personenbezogene Überwachung ist die gezielte Beobachtung und Informationserhebung seitens staatlicher Dienste (Polizei, Geheimdienst). Außerdem jede Form der Kontrolle von Arbeitnehmern und Unternehmen. Sie laufen unter »Sicherheitsmaßnahmen« oder dienen einer vermeintlichen Gefahrenabwehr. Dazu gehören zum Beispiel Kameraüberwachungen auf öffentlichen Plätzen oder Bahnhöfen; die geforderte Weitergabe von Fluggastdaten; die Audio-Überwachung mittels Abhörgeräte; die Überwachung des Briefverkehrs oder die Telefonüberwachung; die Identifizierung und Lokalisierung von Gegenständen und Personen via RFID-Chips oder verdeckte Zugriffe auf informationstechnische Systeme wie die Online Durchsuchung (Bundestrojaner).



Verschlüsselung / Kryptografie Mechanismen, mit denen ein offen lesbarer Text in einen nicht lesbaren Text umgewandelt werden kann und umgekehrt. Zu diesem Zweck werden Geheimnisse zwischen den KommunikationspartnerInnen, sogenannte Schlüssel ausgetauscht. Die Kryptografie basiert auf komplexen mathematischen Algorithmen, die den Aufwand für ein Erraten der Schlüssel so groß gestalten, dass Angriffe sich nicht lohnen.

Vorratsdatenspeicherung Die verdachtsunabhängige und flächendeckende Speicherung von Verbindungsdaten in der Telekommunikation. Die Vorratsdatenspeicherung wurde in Deutschland zum 01. Januar 2008 eingeführt und verpflichtet Telekommunikationsanbieter, Informationen über sämtliche in Deutschland anfallende Verbindungen (Telefon, Mobiltelefon, E-Mails, SMS,…) für mindestens 6 Monate zu speichern.
➳ Artikel, S. 46 ff

Impressum

V.i.S.d.P.
Frederic Clasmeier

Redaktion
Frederic Clasmeier
Rabea Duscha
Katharina Maria Nocun
AK Vorratsdatenspeicherung Münster

Gestaltung
Luise von Grebe

Auflage
2.000 Stück

Erscheinungsdatum
November 2009

Literaturempfehlung

Kontrollverluste – Interventionen gegen Überwachung Leipziger Kamera. Initiative gegen Überwachung (Hg.)

Das Buch Kontrollverluste versammelt Beiträge zu Fragen einer emanzipatorischen und praktischen Kritik an der aktuellen Überwachungsgesellschaft. Es führt sehr unterschiedliche Strategien und Perspektiven der linken Überwachungskritik zusammen. Kritische WissenschaftlerInnen, AktivistInnen und Initiativen stellen theoretische, aber vor allem strategische und aktionsorientierte Überlegungen an, reflektieren ihre Handlungserfahrungen und beleuchten Probleme und Potenziale von Bewegung(en) gegen immer mehr Überwachung und Kontrolle.

Die »Leipziger Kamera. Initiative gegen Überwachung« ist seit 2003 in der Stadt des bundesdeutschen Pilotprojekts zur Videoüberwachung öffentlicher Plätze aktiv. Zu ihren Projekten zählen überwachungskritische Stadtrundgänge (seit 2004), das Festival »DEL+CTRL« (2006), die Veranstaltungsreihe »Salon Surveillance« (seit 2007) und Aktionen wie die Verleihung des »Erich-Mielke- Gedächtnispreises« (2003/2005) und das »Making Trouble«-Wochenende (2006) zusammen mit den Space Hijackers aus London.

ISBN-13: 978-3-89771-491-5
Ausstattung: brochiert, 256 Seiten
Preis: 18 Euro

Ein Reader über den Datenschutz,
die Informationelle Selbstbestimmung
und den ganzen Rest

asta fh
Allgemeiner Studierendenausschuss
der Fachhochschule Münster

AK VORRAT

asta.ms