

Informationelle Selbstbestimmung

II. Gefährdung

Jeder Mensch ist ein Individuum mit einer vielfältigen Persönlichkeit. Allerdings ist dies für Firmen, Staat und andere Institutionen viel zu kompliziert. Es ist viel einfacher ihm eine Nummer zu geben und an Hand seiner Daten in eine Kategorie einzuordnen. Noch einfacher ist es alle über ihn befindlichen Informationen in einer Datenbank unter einer Identifikationsnummer zu speichern und diese allen Interessenten zur Verfügung zu stellen. Allerdings hat das Bundesverfassungsgericht Ihnen das Recht der informationellen Selbstbestimmung, d.h. das Recht selbst über Ihre Daten zu verfügen, zugesprochen. Daher darf man nicht ohne Ihre Erlaubnis beliebig Daten über Sie sammeln und zu einer virtuellen Identität verdichten.

Allerdings ist diese Recht auf Grund von Sicherheitsbedenken mittlerweile immer mehr ausgehöhlt worden und es wird heute mit allerlei Mitteln versucht an Ihre Daten zu kommen, ohne dass Sie dieses noch merken.

Profiling

Heutzutage ist es für eine Firma wichtig so viele Informationen wie möglich über Sie zu bekommen. Ein Profiler sammelt alle über Sie verfügbaren Daten um ein Profil über Sie anzulegen, welches er dann für Geld verkaufen kann (Weiterführende Informationen unter: [profil]).

Es war noch nie so einfach diese persönlichen Informationen zu bekommen wie im Computerzeitalter. Besonders kritisch ist hierbei, dass Sie nichts davon merken.

Google als Beispiel für das Profiling

Das Profiling wird mittlerweile von vielen Firmen betrieben. Allerdings ist Google wohl das Beispiel, welches diese Technik am meisten perfektioniert hat und es am erfolgreichsten betreibt.

Suchmaschinen

Viele werden jetzt anmerken, dass Google nur eine Suchmaschine ist. Allerdings funktionieren Geschäfte im Internet nicht immer genauso wie in der realen Welt. Hier zahlen Sie meist für ein bestimmtes Produkt oder eine bestimmte Dienstleistung. Im Netz ist es aber oft so, dass Sie selber gar nichts mehr für die Dienste zahlen, allerdings müssen Sie sich dafür Werbung ansehen. Die Firmen, die dort werben, zahlen dann an Google Geld dafür, dass Sie sich auf der Suchmaschine die Werbung ansehen. Dieses System funktioniert deswegen so gut, da die Werbung direkt auf Sie zugeschnitten wird. Nehmen wir als Beispiel eine Produktsuche über die Google-Suchmaschine. Google geht aber noch viel weiter als nur auf Ihre aktuelle Suchanfrage zu reagieren. Wenn Sie beispielsweise am Vortag auf Google Earth einen Weg von Ihrem Wohnort zu einem Ausflugsziel gesucht haben, so kann Ihnen Google gleich passend die Werbung des Ladens genau bei Ihnen um die Ecke anbieten, welches dieses Produkt im Angebot hat.

Sie wundern sich vielleicht wie Google diese Daten bekommt. Dazu werden sogenannte Cookies auf Ihrem Rechner gespeichert. Google versieht diese Cookies noch mit einer Identifikationsnummer um Ihre Cookies jederzeit wieder zu erkennen und Sie damit eindeutig identifizieren zu können. Die Cookies selber speichern dann Uhrzeit, Dauer

und IP-Adresse sowie Ihre Suchbegriffe mit Funktionen und Hilfestellungen und liefern damit genug Daten zum Aufbau Ihres Profils.

Dieses System verwendet nicht nur Google, sondern auch andere Firmen wie die Suchanbieter Yahoo, Lycos etc.

E-Mail

Neben der Suchmaschine kann man bei Google beispielsweise auch einen kostenlosen E-Mail Account bekommen. Auch hier werden Daten vom Kunden abgegriffen. Dieses System gilt wiederum nicht nur für Google, sondern auch für andere kostenlose E-Mail Anbieter wie web.de, Gmx, Hotmail etc.

Zum Versenden von E-Mails muss man wissen, dass diese nicht wie ein Brief unter das Postgeheimnis fallen. Prinzipiell kann eine E-Mail jeder lesen, der bei der Weiterleitung von Ihnen zum Empfänger beteiligt ist.

Wenn Sie die E-Mails über einen Internet Provider versenden, sind die E-Mails also auf dem Transport unsicher. Nach dem Versand werden die E-Mails aber vom Server des Providers auf Ihren Rechner geladen und nur noch für Sie lesbar. Bei Google-Mail hingegen verbleiben die E-Mails auch vor bzw. nach dem Versand auf den Google-Servern. Selbst wenn Sie die E-Mails löschen, können diese noch in Sicherungen, die Google als zusätzliche Sicherheit für seine Kunden anpreist, bestehen bleiben. Dabei sichert Ihnen Google zu, dass keine Person Ihre E-Mails liest. Allerdings durchsucht das System Ihre E-Mails systematisch nach Keywords um Ihr Profil zu schärfen. Warum sollte Google auch Menschen dafür zu bezahlen Ihre E-Mails zu lesen, wenn Sie leistungsstarke Rechner zum Auswerten Ihrer E-Mails besitzt?

Weitere Dienste

Google hat erst kürzlich seinen neuen Internetbrowser **Chrome** fertig gestellt. Jede Eingabe in der Adresszeile des Internetbrowsers wird an die Google-Suchmaschine weitergeleitet um noch mehr Ihrer Daten sammeln zu können.

Des Weiteren bietet Google Ihnen eine News-Seite, auf der die neuesten Nachrichten gesammelt werden. Wenn Sie sich dort für Links interessieren oder eine Suche starten, so werden diese Informationen auch für Ihre Profil verwendet.

Im Google-Kalender können Sie kostenlos Ihre Termine verwalten. Auch diese verwalten Sie nicht auf Ihrem eigenen Rechner, sondern alle Termine werden auf dem Google-Server verwaltet. Wenn Sie nicht bei der Einstellung Ihres Accounts aufpassen, kann Ihre Termine nicht nur Google, sondern jeder andere Nutzer sehen.

In den USA kann man auch sein persönliche Krankenakte auf den Google-Servern anlegen. (Weiterführende Informationen zum Profiling von Google finden sie hier: [google; Seite 1-6])

Konvergenz

Heutzutage ist der eigentliche Rechner ein aussterbendes Medium, vor allem im privatem Bereich. Mittlerweile sind die sogenannten Smartphones angesagt, mit denen man nicht nur Telefonieren und SMS senden, sondern auch bequem surfen und immer mehr Apps (kleine Anwendungen) verwenden kann. Mittlerweile gibt es auch schon Möglichkeiten E-Books (elektronische Bücher) zu lesen oder fern zu sehen. In Zukunft

werden also immer mehr Funktionen in einem Gerät gebündelt. Dadurch wird das Verdichten der Daten noch viel einfacher, da man nicht nur Ihr Surf- und Internetverhalten, sondern auch gleich Ihr Fernsehverhalten protokollieren kann, womit Ihnen gleich noch attraktivere Angebote unterbreitet bzw. Ihren Interessen entsprechende Werbungen angeboten werden können.

Ein weiteres Problem ist, dass bei der Vermischung der Kommunikationswege die bewährten Sicherheitssysteme nicht mehr funktionieren und so ein Missbrauch der übermittelten Daten erleichtert wird. (Detaillierte Informationen zur Konvergenz unter: [konver; Seite 1-5])

Lokalisation

Ein weiteres Problem der Handys ist, dass beim Aufbau einer Verbindung Ihr Standort lokalisiert werden kann. Mit den heutigen Smart Handys fragt man immer mehr Informationen ab, so dass man ständig eine Verbindung zum Server aufbaut und damit seinen Standort auf wenige Meter genau an den Betreiber übermittelt. Dabei gibt es durchaus sinnvolle Anwendungen wie die Ortung von Hilfsbedürftigen und Kindern. Aber jede Ortung ist eine Eingriff in Ihr von der Verfassung garantiertes Recht auf informationelle Selbstbestimmung [local; Seite1-4].

Es ist selten klar, wie viele Daten wo erfasst bzw. gespeichert und vor allem ob Ihre Daten ausreichend vor dem Zugriff Fremder geschützt werden.

Im Belgien war vor kurzem ein Mautsystem in der Diskussion, bei dem jedes einzelne Fahrzeug mit einer GPS-Einheit versehen wird. Auf diese Weise können die Fahrwege der Autos geortet und dementsprechend Abgaben gezahlt werden. Zwar wird beteuert, dass diese Daten nicht einzeln abgefragt werden können, allerdings sind die Daten vorhanden und es wäre ein leichtes die gefahrene Geschwindigkeit mit zu übertragen. Dann könnte man jedem Fahrer, der die Geschwindigkeit übertritt, gleich einen Strafzettel zu schicken. Wenn das Geld in die Gemeinden und Länder fließt, in denen die Vergehen begangen wurden, so hätten die Städte wahrscheinlich keine Geldprobleme mehr. Eigentlich sind dies ehrenwerte Ziele, aber wollen wir unsere Freiheit derart einschränken, dass wir permanent auf Fehlverhalten überprüft werden? Ist der Druck keine Fehler zu machen nicht mittlerweile groß genug?

RFID-Chips

Diese funkenden Chips wurden entwickelt um die Logistik zu vereinfachen und die Waren berührungsfrei verfolgen zu können. In Betrieben werden diese Chips aber auch gerne für die Zeiterfassung oder Zugangskontrolle benutzt. In nicht mehr allzu ferner Zukunft werden auch Einkäufe direkt an der Kasse gescannt und dann gleich von Ihrem Konto abgebucht. Dadurch kann man Ihre Einkäufe jederzeit mit Ihnen in Verbindung bringen. Problematisch ist dabei aber auch, dass die RFID-Chips auch nach Ihrem Einkauf weiter funken und somit immer weiter Ihre Daten auch außerhalb des Ladens an die Umwelt weitergeben.

Auch in Krankenhäusern werden Bänder mit den funkenden Chips verwendet, welche die Daten des Patienten enthalten. In Großbritannien wird darüber diskutiert, dass die Fussfesseln beim Hausarrest durch injizierte RFID-Chips überwacht werden sollen. Weitere Anwendungsfelder für die RFID-Chips sind Fahrkarten(Bahncard100), Tickets

für Großereignisse wie die Fußball Weltmeisterschaft 2006, Bücher der Bibliotheken, Studentenausweise oder Pässe [rfid4, Seite 4]. Diese Einsatzfelder werden meist mit Sicherheit vor Fälschungen begründet. Wie es allerdings um die Sicherheit Ihrer Daten aussieht, wird angesichts der vielen Datenskandale vor allem in Deutschland lieber verschwiegen. Des Weiteren ist es nur noch ein kleiner Schritt von der Sicherheit zur Überwachung jedes einzelnen (Weiterführende Informationen unter [rfid3] , [rfid4] und sehr detailliert in der Studie des BSI unter: [rfid7]).

Soziale Netze

Im Zeitalter des Web 2.0 üben Blogs, Wikis, Foren, Twitter und Netzwerke eine große Faszination auf verschiedenste Personen aus. Allerdings wird auf den Datenschutz in sozialen Netzen meist nicht sehr viel geachtet. Gefährlich sind dabei vor allem die Informationen, welche nicht Sie selber, sondern beispielsweise Freunde über Sie veröffentlichen. Dabei sollten Sie immer daran denken, dass Daten, die erstmal ins Netz gelangt sind, nicht mehr so leicht zu entfernen sind, da Sie in der Zwischenzeit schon längst vervielfältigt und an anderer Stelle platziert werden können.

Bei allen unter Ihrem Namen verbreiteten Daten sollten Sie sich immer klar machen, dass diese Daten Ihr Chef sehen könnte, da mittlerweile Personalabteilungen standardmäßig soziale Netze durchsuchen. Allerdings können Sie den Spieß hier auch mal umdrehen und Ihr Bild für die Personalabteilung etwas besser darstellen als es in Wirklichkeit ist.

Vor allem soziale Netze haben meist einen sehr niedrigen Sicherheitsstandard. Daher sollten Sie sich bewusst sein, dass es für kriminelle Personen nicht sehr schwierig ist an Daten zu gelangen, welche Sie nicht bzw. nur für Freunde freigegeben haben [sozial; Seite3]. Der Identitätsklau wächst in Zeiten des Internets immer mehr. Über die Folgen eines solchen Identitätsklau berichtet Tina Groll in Ihrem Bericht "Meine Identität gehört mir" [ident] sehr anschaulich.

(Detaillierte Informationen unter: [sozial; Seite 1-5])

Ubiquitous Computing (allgegenwärtige Datenverarbeitung)

Dass die heutige Datensammelflut erst der Anfang ist, können wir schon auf Messen wie der CEBIT sehen. Hier gibt es schon Häuser, in denen für Sie einfache alltägliche Vorgänge von kleinen vernetzten Einheiten übernommen werden. In diesen vollautomatischen Häusern löst beispielsweise das Klingeln des Weckers den Start der Kaffeemaschine aus. Das Licht geht automatisch an, wenn Sie sich in ein Zimmer bewegen und der Kühlschrank kauft automatisch über das Internet neue Waren Ihrer Lieblingsmarken ein, wenn diese nicht mehr in ausreichender Menge zur Verfügung stehen. Damit diese vollautomatischen Vorgänge funktionieren, müssen die Geräte Ihre Gewohnheiten und Ihren Alltag bis aufs kleinste Detail kennen (Detaillierte Informationen unter: [ubi]).

Videoüberwachung

Mittlerweile gehören die Kameras schon zum Stadtbild der meisten Städte. Vor allem Leute, die öffentliche Verkehrsmittel benutzen, werden täglich mehrmals gefilmt. Dabei tragen die Kameras subjektiv zum Sicherheitsgefühl der meisten Leute bei. Auch in meinem Bekanntenkreis gibt es viele, die glauben, dass Ihnen mit der

Videoüberwachung nichts mehr passieren kann. Allerdings vergessen viele, dass eine Kamera kein Verbrechen verhindern kann und nach Studien aus Großbritannien, dem Staat der Videoüberwachung schlechthin, dienen die Kameras weder der Abschreckung vor allem bei Gewaltverbrechen noch der Aufklärung von Verbrechen (Von hundert Videokameras hilft eine bei der Ermittlung des Verbrechens). Des Weiteren hat die Videoüberwachung andere gravierende Folgen. Durch die suggerierte Sicherheit der Videokameras sind noch weniger Menschen bereit bei Zwischenfälle einzugreifen. Außerdem verlagern sich Verbrechensschwerpunkte nur an bisher ungefährliche Orte [video; Seite 18].

Allerdings haben sich die Kameras sehr hilfreich dabei erwiesen das Stadtbild von unerwünschten Personen wie Obdachlosenn zu säubern. Das Geld, welches in die ganze Videoüberwachung investiert wird, wäre meiner Meinung nach viel besser in richtige Beamte investiert, welche bei einem Verbrechen auch wirklich helfen können.

III. Existierende Datensammlungen und deren Problem

Bei der elektronischen Gesundheitskarte, dem elektronischen Personalausweis oder dem elektronischen Entgeltausweis fragen die meisten Menschen nach dem Nutzen, da diese vor allem große Probleme und Kosten bei geringem Mehrwert verursachen.

Wie meist sind es vor allem wirtschaftliche Interessen. Auffällig ist dabei die elektronische Signatur, die auf allen drei Karten entweder geplant war oder zum Einsatz kommen wird. Da sich diese elektronischen Unterschriften weder bei normalen Bürgern noch bei Unternehmen großer Beliebtheit erfreuen, sollen diese jetzt offensichtlich von der Regierung per Zwang durchgesetzt werden um eine Vorreiterrolle beim E-Government spielen zu können.

ELENA (elektronischer Entgeltnachweis)

In dieser Datenbank werden Arbeitnehmerdaten gespeichert um über Arbeitslosen-, Wohn- oder Elterngeld zu entscheiden. Dazu werden vom Arbeitgeber seit dem 1.1.2010 die Daten auf elektronischem Wege an die deutsche Rentenversicherung übermittelt. Neben dem Verdienst werden aber auch Krankmeldungen und Abmahnungen gespeichert. Dabei können diese Daten auch heute schon von den Ämtern schriftlich angefordert werden. In diesem Zusammenhang wird häufig vergessen, dass diese Daten von allen Arbeitnehmern erhoben werden und zwar insbesondere von denen, die nie eine der betroffenen Leistungen angenommen haben, sowie von denen, die eine solche Leistung gar nicht in Anspruch nehmen können (beispielsweise Richter und Beamte). So verstößt Elena gegen den Grundsatz der Datensparsamkeit und ist nicht mit dem Recht auf informationelle Selbstbestimmung in Einklang zu bringen.

Davon abgesehen bieten diese Daten auch noch ein sehr großes Missbrauchspotenzial. Denn welcher Arbeitgeber würde nicht gern wissen, ob sein möglicher neuer Arbeitnehmer höhere Fehlzeiten als üblich hat und aus welchem Grund ihm gekündigt wurde. Auch die privaten Krankenkassen oder Versicherungen könnten daran interessiert sein, ob jemand öfters als normal Fehlzeiten bei der Arbeit hat. Des Weiteren werden von mehreren Seiten die von der Bundesregierung angepriesenen hohen Entlastungspotentiale angezweifelt. Die Ignoranz der Bundesregierung

gegenüber Datenschutzbelangen, obwohl von ihren eigenen Datenschutzbeauftragten mehrmal angemahnt, wird auch in diesem Falle wieder sehr deutlich: Das zuständige Ministerium wollte erst nach lautstarken Protesten eine Überprüfung der Notwendigkeit der Datenerfassung und eine Befragung der Betroffenen durchführen. Für all diejenigen, welche ihr Recht auf Auskunft über Ihre Daten wahrnehmen wollen, hier noch der Hinweis, das die Daten zwar ab dem 1.1.2010 gespeichert werden eine Auskunft aber aus technischen Gründen erst ab dem Jahre 2012 erfolgen kann. Weiterführende Informationen zu dem Thema ELENA gibt es auch im Wiki der Piratenpartei [<http://wiki.piratenpartei.de/ELENA-Verfahren>].

Steuerdatenbank (Steuer-ID)

Jeder Deutsche wird ab seiner Geburt mit der neuen Steueridentifikationsnummer versehen und behält diese ein Leben lang. Daher wird die Nummer von Datenschützern auch als Personenkennziffer bezeichnet, welche nach einem Urteil des Bundesverfassungsgerichts aus dem Jahre 1968 nicht mit der Menschenwürde vereinbar wäre.

Ein große Gefahr bildet diese jedem zugeordnete Identifikationsnummer wenn sie auch für andere Behörden genutzt wird. Eine automatischer Abgleich mit den Meldebehörden beispielsweise ist geplant. Daher wurde von der Humanistischen Union eine Musterklage gegen die Steuer-ID eröffnet (Nähere Informationen finden Sie unter [human]).

Auch eine Benutzung der Identifikationsnummer für Unternehmen würde sich anbieten, aber auch ein großes Missbrauchspotential beinhalten. Die Krankenkassen wollen schon mal alle IDs einsammeln. Bei Weigerung wird mit der Streichung der steuerlichen Vergünstigung gedroht (Weiterführende Informationen unter [steuer2]).

Etwas "Positives" zur Steuer-ID: Mit ihr kann man jetzt der Nachwelt noch etwas länger erhalten bleiben, da die Steueridentifikationsnummer bis zu 20 Jahre nach dem Tod erhalten bleibt.

Vorratsdatenspeicherung

Wissenschaftler haben festgestellt, dass mit den Verbindungsdaten von drei Monaten das Bewegungsprofil der betreffenden Person mit 80% Wahrscheinlichkeit, bei Leuten, die wenig reisen, sogar mit 93% Wahrscheinlichkeit vorhergesagt werden kann (Die Veröffentlichung der Studie finden Sie hier: [vorrat2]).

Auch wenn die Ortung der Personen noch nicht exakt möglich ist, so wird das Handynetz in Zukunft immer dichter und die Ortung immer genauer werden. Man könnte jetzt erwidern, dass der Aufenthaltsort nur bei einem Telefonat übermittelt wird. Allerdings gibt es auch sogenannte "stille SMS", die der Angerufene nicht mitbekommt, die allerdings dazu führen, dass die Verbindungsdaten gespeichert und damit der Aufenthaltsort wieder ermittelt werden kann.

Am zweiten März 2010 erklärte das Bundesverfassungsgericht die Umsetzung der Vorratsdatenspeicherung in Deutschland als verfassungswidrig und nichtig. Damit müssen alle bisher gesammelten Daten wieder gelöscht werden.

Allerdings wird in der CDU schon wieder die Forderung nach einer schnellen Neufassung der Vorratsdatenspeicherung gestellt. Daher wird die Vorratsdatenspeicherung wahrscheinlich nur zu verhindern sein, wenn man die

Gesetzeslage auf EU-Ebene ändert.

Weiterführende Informationen zu dem Thema Vorratsdatenspeicherung gibt es auch im Wiki der Piratenpartei [<http://wiki.piratenpartei.de/Vorratsdatenspeicherung>].

INDECT

Indect steht für die ehrgeizigen Überwachungspläne der Europäischen Union (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment). Dabei sollen die technischen Mittel entwickelt werden um alle verfügbaren Informationen auf Bedrohungen und "abnormales Verhalten" zu überprüfen. Speziell für Menschenansammlungen gibt es in der EU noch das Projekt Adabts (Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces), welches ebenfalls "abnormales Verhalten" -diesmal in Gruppen- durch die Auswertung von Suchalgorithmen erkennen will (Weiterführende Informationen finden Sie hier: [adabts]).

Indect beinhaltet nicht nur die Überwachung per Video oder anderer Sensoren, sondern auch Suchmaschinen, welche in "Websites, Diskussionsforen, Usenet-Gruppen, Datenservern, P2P-Netzwerken, sowohl nach der Bedeutung, als auch nach der Stimmung untersuchen". Das bedeutet, dass man nicht nur auf der Straße gefilmt wird, sondern auch die ganze Körperhaltung automatisch analysiert wird.

Nach dem neusten Veröffentlichungen [indect5, Seite 42f.] des Indect Programms sollen nicht nur Videokameras, sondern auch fliegende Drohnen, welche mit Kameras ausgestattet werden (Unmanned Aerial Vehicles), vor allem in den Großstädten eingesetzt werden. Sowohl in Frankreich als auch in Großbritannien soll es schon Pläne geben diese Drohnen mit Tasern zu bewaffnen (Nähere Informationen hierzu finden Sie unter: [indect7], [indect8]).

Die Daten sollen dann auf einem WebPortal zur Verfügung gestellt werden, natürlich unter höchsten Sicherheitsbedingungen. Aber auch den normalen Nutzer soll es in seiner "gewöhnlichen Arbeit " unterstützen und täglich "interessante Inhalte" liefern [indect6, Seite 7].

Elektronische Gesundheitskarte

Die elektronische Gesundheitskarte soll die bisherige Karte ablösen. Dies ist für 2010 geplant, es kann aber zu weiteren Verschiebungen kommen, da nach dem Wechsel der Regierung die elektronische Gesundheitskarte noch einmal auf dem Prüfstand steht um den Datenschutz zu überprüfen. Dabei werden nur die Daten, welche bisher auch gespeichert wurden, verpflichtend gespeichert (Wie bei der Steuernummer bekommen sie auch hier eine Versicherungsnummer, welche Sie lebenslang behalten und Ihnen immer wieder eindeutig zugeordnet werden kann, auch wenn Sie beispielsweise die Krankenkasse wechseln). Alle anderen Leistungen werden nach dem heutigen Kenntnisstand doch freiwillig sein. Dazu gehören das elektronische Rezept, die elektronische Patientenakte, Arztbriefe (für schnelle Kommunikation unter den Ärzten) und die Notfalldaten (für chronische Erkrankungen, Allergien etc.).

Wenn man einverstanden ist, werden die Daten nicht auf der Karte gespeichert, sondern an einen zentralen Server gesendet. Dazu wird neben der elektronischen Gesundheitskarte, die Heilberufskarte des behandelnden Arztes benötigt. Die Daten

werden verschlüsselt auf dem Server abgelegt. Die Entschlüsselung soll nur mit der elektronischen Gesundheitskarte möglich sein.

Flugpassagierdaten

Seit 2007 werden die Daten aller Passagiere bei Flügen in die USA gespeichert, wobei das US-Heimatschutzministerium(DHS) Zugriff auf diese Daten hat[flug3; Seite 5]. Dabei werden neben allen Personen- und Flugdaten auch Daten wie Behinderung und besondere Essenwünsche übergeben [flug3; Seite 11f.]. Die Daten dürfen sowohl an andere US-Behörden als auch an Drittstaaten weitergegeben werden [flug3; Seite 7]. Die Daten werden 15 Jahre gespeichert [flug3; Seite 13]. Dabei hätte laut Vertrag die Datenübergabe 2008 auf ein Push-Verfahren umgestellt werden müssen, so dass die Airlines die Kontrolle über die Datenübermittlung in die USA behalten [flug3; Seite 5 und Seite15].

Ein erstes Abkommen zum Übermitteln der Daten von 2003 wurde durch den Europäischen Gerichtshof gekippt. Hier waren mit dreieinhalb Jahren noch wesentlich kürzere Speicherfristen vorgesehen. Auch die Menge der abgefragten Daten hat sich nur unwesentlich verändert.

Kontodaten

2009 wurden durch das Bundeszentralamt für Steuern im Auftrag der Finanzämter und Sozialbehörden (vor allem Arbeitsämter) 43.066 Kontostammdaten abgerufen. Damit setzt sich die stark steigende Tendenz der letzten Jahre fort [konto1, Daten bei Bundesfinanzministerium suchen Monatsbericht].

Seit einem Urteil des Bundesfinanzhofs im Jahre 2009 benötigen die Steuerbehörden auch keinen konkreten Verdacht auf eine Straftat mehr, sondern es reichen Unregelmäßigkeiten in der Steuererklärung aus um die Bankdaten abzurufen (Pressemitteilung zum Gerichtsurteil unter: [konto2]).

SWIFT-Datenbank

Mit dem Swiftabkommen wollte die EU-Kommission der USA Zugriff auf die Daten der Swiftdatenbanken gewähren. Dieses Abkommen war notwendig, da Swift die Daten nicht mehr auf Servern in den USA speichert, worauf die amerikanischen Behörden sowieso Zugriff hatten, sondern die Daten nach Europa umzieht. Die EU-Kommission wollte die Daten der Swift mit den europäischen Daten noch um die Daten innerhalb der einzelnen Ländern ergänzen. Auch ein Datenschutz, der dem europäischen Standard entspricht, wäre nicht gewährleistet. Selbst eine Weitergabe der Daten an Drittländer wäre möglich gewesen. Selbst der Bundesrat warnte davor, dass die Daten für Wirtschaftsspionage verwendet werden könnten. [swift1].

Diese Bedenken und die mangelnde Aufklärung des Parlaments durch die EU-Kommission haben dazu geführt, dass das EU-Parlament das schon unterzeichnete Abkommen durch eine klare Abstimmung gegen das Abkommen ungültig gemacht hat.

GEZ-Gebühreneinzugszentrale

Um die GEZ-Gebühren von Nutzern, welche sich nicht selber melden, einfordern zu können, versucht die GEZ die Adressen aller Einwohner, die für Zahlungen in Frage

kommen, zu bekommen. Dazu wendet sich die GEZ nicht nur regelmäßig an die Einwohnermeldeämter, sondern kauft auch genau die Adressen, die durch die sogenannten Adresshändler vorher gesammelt wurden. Dies geht aus einer Prüfung einiger Landesdatenschutzbeauftragten im Jahre 2005 hervor [gez1, Seite 71].

Schufa (Schutzgemeinschaft für allgemeine Kreditsicherung)

Die Schufa ist ein privates Unternehmen, das Daten von Bürgern und Unternehmen speichert, welche ihnen von ihren Vertragspartnern zugesendet wird. Zu den Vertragspartnern zählen unter anderem Banken, Versicherungen, Händler, Leasinggesellschaften und Telekommunikationsunternehmen. Die Schufa selber erteilt dann wiederum bestimmte Auskünfte an die Vertragspartner.

Dabei gibt es die B-Auskünfte, bei denen nur Informationen über nicht vertragsgemäßes Verhalten weitergegeben werden. Daneben gibt es noch die A-Auskunft, die sogenannte Vollauskunft, in der alle gespeicherten Daten vor allem an Banken und Versicherungen weitergegeben werden (Nähere Informationen unter: [schufa1, schufa4].

Neben diesen Auskünften ermittelt die Schufa den Scorewert. Dabei wird anhand von Faktoren wie Alter, Wohnort, Wohnungswechsel das Verhalten einer Vergleichsgruppe zu Grunde gelegt um Ihr eigenes Verhalten prognostizieren zu können [schufa4]. Dieser Wert ist umstritten und vom Amtsgericht Hamburg gibt es auch schon ein Einzelfallurteil (Aktenzeichen 9 C 168/01) die Weitergabe dieses Scorewertes zu unterlassen [schufa1]. Aufgrund einer Gesetzesänderung des Bundesdatenschutzgesetzes wird es ab dem 1. April 2010 möglich sein, seine Daten bei der Schufa einmal im Jahr kostenlos zu überprüfen [Bundesdatenschutzgesetz §34 Abs.8]. Dies lohnt sich einer Studie des Bundesverbraucherministeriums zufolge auch, da die Fehlerrate der Eintragungen bei der Schufa sehr hoch ist (Bericht zur Studie und Pressemitteilung zu den Ergebnissen der Studie: [schufa5, schufa6]).

Datenbank mit den biometrischen Daten des Ausweises

2005 wurde ein elektronischer Reisepass eingeführt und Ende 2010 soll der elektronische Personalausweis folgen.

Für den elektronischen Reisepass (epass) werden schon seit 2007 die Daten aus Fingerabdrücken gespeichert. Für den neuen elektronischen Personalausweis wird die Abgabe der Fingerabdrücke optional sein. Die biometrischen Daten aus dem Foto werden in beiden Fällen auf einem sogenannten RFID-Chip (Funkchip gespeichert). Da die Daten auf dem Chip so gespeichert sind, dass das Clonen von Daten (eins-zu-eins-Kopie) nicht ausgeschlossen werden kann, ist theoretisch das Auslesen der Daten möglich (Ergebnisse von Versuchen dazu können Sie hier finden [bio2, bio4]). Nach einem Bericht der Sendung WISO vom 9.2.2009 ist auch die Erfassung der Fingerabdrücke eine mögliche Schwachstelle, da durch Angriffe auf die Rechner der Meldebehörde die Fingerabdrücke entwendet und somit falsche Fingerabdrücke auf Pässe gelangen können. Das dies nicht so abwegig ist, unterstreicht auch der Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, in welchem bei einer Stichprobe in "keiner der geprüften Passbehörden ein vollständiges IT-Sicherheitskonzept vorgelegen konnte" [bio5; 4.4.2 Prüfung des Verfahrens zur Beantragung von Reisepässen; Erstellung von IT-Sicherheitskonzepten]. Des Weiteren werden auf Grund von täglichen

Datensicherungen Fingerabdrücke länger als erlaubt gespeichert [bio5; 4.4.2 Prüfung des Verfahrens zur Beantragung von Reisepässen; Unzulässige Speicherung der Fingerabdrücke]. Dass unberechtigte Zugriffe auf die Online-Melderegisterauskunft möglich sind, wird im nächsten Kapitel des Tätigkeitsberichts des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg ausgeführt [bio5; 4.4.2 Prüfung des Verfahrens zur Beantragung von Reisepässen; Unberechtigte Zugriffe auf die Online-Melderegisterauskunft].

Daten aus dem Mautsystem

Es wurde immer wieder gefordert die Daten des Mautsystems für die Verfolgung von Verbrechern zu öffnen. Dadurch wird aber die vom Bundegerichtshof geforderte Zweckbindung ausgehebelt. Technisch werden schon jetzt alle an den Mautbrücken vorbeifahrenden Fahrzeuge fotografiert. Daher ist es technisch einfach umzusetzen alle Fahrzeuge zu speichern oder mit Datenbanken abzugleichen, was auch schon in einigen Bundesländern durchgeführt wird. Es wäre technisch auch möglich mit diesem System Geschwindigkeiten zu überwachen und bei Übertretungen automatisch einen Strafzettel zu verschicken.

Melderegister

2008 wollte das Innenministerium unter Wolfgang Schäuble ein bundesweites Melderegister aufbauen. Dieses Vorhaben ist aber nie über die Planungsphase hinausgekommen.

Trotzdem sollte man der Weitergabe der Daten durch das Melderegister unbedingt widersprechen, da die Daten nicht selten bei Adresshändlern landen (lesen Sie dazu die Pressemitteilung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein [melde1]).

Handelsregister

Im Handelsregister sind alle Daten, die in der Handelsregisterverordnung §40 und §43 gefordert sind, gespeichert. Die Daten sind über die Homepage des Handelsregisters [<https://www.handelsregister.de>] abrufbar.

Elektronisches Grundbuch

Elektronisch geführte Grundbücher können über das Internet eingesehen werden.

Datenschutzskandale

Tabelle mit aktuellen Datenschutzskandalen finden Sie unter: http://wiki.piratenpartei.de/AG_Datenschutz/Datenschutzskandale

IV. Aktuelle Schutzmöglichkeiten

Technische Schutzmöglichkeiten

Bei vielen Diensten gibt es wenig oder keine Möglichkeiten sich vor dem Speichern der Daten zu schützen, da man auf diese Dienste angewiesen bzw. aus Bequemlichkeit nicht mehr missen möchte. Allerdings sollte man diese Dienste sparsam verwenden. Vor Beginn eines Dienstes sollte man die Datenschutzerklärung verlangen. Da diese meist

schwer zu verstehen sind, sollten Sie sich nicht scheuen bei Unklarheiten auch nachzufragen. Des Weiteren sollten Sie die Weitergabe der Daten an Dritte untersagen [local, Seite4]. Wenn Ihnen dies nicht angeboten wird, sollten Sie es aktiv einfordern, es ist Ihr gutes Recht.

Es gibt unter www.robinson-listen.de eine Liste, in die Sie Ihre Daten eintragen können, die für den Datenhandel blockiert werden sollen. Allerdings sollten Sie wissen, dass nicht alle Datenhändler und Werbende die Daten aus dieser Liste abrufen [robin].

Sicherheitssystem und Verschlüsselung

Um Ihre Daten vor unbefugtem Zugriff zu schützen, sollten Sie darauf achten Firewalls und Virens Scanner sowie auch die installierten Programme immer auf den neusten Stand zu halten. Wenn Sie ein WLAN verwenden, sollten Sie darauf achten, dass die Übertragung verschlüsselt wird. Sie können Ihr Passwort durch Verwendung von Groß- und Kleinschreibung, sowie die Verwendung von Zahlen und Sonderzeichen sicherer machen.

Wenn Sie oft mit Ihrem Laptop bzw. USB-Stick unterwegs sind, sollten Sie die ganze Festplatte bzw. den USB-Stick oder zumindest den Teil mit den sensiblen Daten verschlüsseln, damit im Fall eines Diebstahls der Dieb nichts mit den Daten anfangen kann.

Bei Eingabe von persönlichen Daten in ein elektronisches Formular sollten Sie immer überprüfen, dass diese Seite auch über eine SSL-Verbindung verfügt. Dies können sie meist leicht überprüfen: Immer wenn Sie Daten eingeben, sollte die Adresse dieser Seite mit https: statt http: anfangen (Nähere Informationen zu SSL finden Sie hier: [ssl]).

E-Mails

Um den Transport von E-Mails zu sichern, sollten die E-Mails verschlüsselt und mit einer digitalen Signatur versehen werden. Mit digitale Signaturen kann man die Identität des Absenders zweifelsfrei feststellen und Fälschungen in der E-Mail erkennen (Weitergehende Informationen unter [schlüssel]).

Cookies

Um zu vermeiden, das Cookies permanent auf Ihrem Rechner gespeichert werden um Ihr Internetverhalten immer wieder mitzuprotokollieren, sollten Sie Ihren Browser so einstellen, dass zwar Cookies akzeptieren werden, diese aber nach dem Schließen Ihres Browsers wieder von Ihrem Rechner gelöscht werden (Detaillierte Informationen zu Cookies finden unter: [cookie]).

Lokalisation

Falls Sie nicht wollen, dass man permanent Ihren Aufenthaltsort bestimmen kann, sollten Sie Ihr Handy nur dann einschalten, wenn Sie dieses benötigen, da Sie bei ständig laufenden Geräten jederzeit Daten übertragen. Bei Navigationsgeräten sollten Sie keine Onlinesysteme mit Rückkanal verwenden, sondern nur solche Geräte, die Ihnen die gewünschten Daten liefern, aber keine Daten zurück an den Server senden. Wenn sich dies nicht vermeiden lässt, sollten Sie zumindest nicht Ihre direkte Wohnadresse angeben, sondern beispielsweise einen zentralen Ort in Ihrer

unmittelbaren Nähe [lokal; Seite4]. Oft kann man auch auf altmodische Dienste zurückgreifen wie beispielsweise die Münzen in einer Parkuhr anstatt das Handy mit BezahlDienst um seine Daten zu schützen.

Anonymisierungsdienste

Um seine Identität im Netz zu verschleiern, gibt es sogenannte Anonymisierungsdienste. Der wohl bekannteste und dazu kostenlose Dienst ist das Tor-System. Dabei wird die eigene Anfrage über mehrere Tor Server geführt. Dabei weiss ein Tor immer nur von wem er die Anfrage bekommen hat und an welches Tor er diese dann weitergeleitet hat. Dies bedeutet, dass die Anfrage über so viele Server geführt wird, dass nicht mehr nachvollzogen werden kann von wem die Anfrage ursprünglich stammt. Dabei sollte man aber immer bedenken, dass das Weiterleiten der Daten über viele Server seine Zeit benötigt und sich deutlich in der Geschwindigkeit widerspiegelt. Daher ist dieses System keine Lösung fürs tägliche Surfen, aber eine gute Alternative, wenn man eine erhöhte Anonymität benötigt. Des Weiteren sollte man auch über dieses System so wenig wie möglich eigene Daten leiten, da prinzipiell jeder ein Tor betreiben kann, was wiederum bedeutet, dass auch ein Tor von einem Datenspion betrieben werden kann, der Ihnen Ihre Daten stehlen will.

VPN (Virtuelle Private Netze)

Wenn man eine sichereres Netz als das Internet zu einem bestimmten System benötigt, kann man sogenannte Virtuelle Private Netze verwenden. Mit einem VPN wird innerhalb eines Netzes (meist Internet) ein eigenes Netz aufgebaut, welches allerdings logisch vom anderen Netz getrennt wird. Dies kann beispielsweise durch eine Verschlüsselung geschehen (Secure VPN). Daher kann man in einem VPN auch über ein öffentliches Netzwerk Daten relativ sicher transportieren. Es gibt auch die sogenannten Trusted VPNs, bei denen mit Hilfe eines dritten Anbieters der VPN-Datenverkehr vom übrigen Internetverkehr abgetrennt wird. Dabei sollte man aber beachten, dass die transportierten Daten vom Anbieter des Dienstes ausspioniert werden können (Detaillierte Informationen zu vpn finden Sie hier: [VPN; Seite 24]).

Rechtliche und Persönliche Schutzmöglichkeiten

Informieren Sie sich über die Datenschutz-Richtlinien der Dienste, die Sie nutzen. Wenn Sie etwas nicht verstehen, scheuen Sie sich nicht nachzufragen. Wenn Ihnen der Schutz Ihrer Daten dabei nicht ausreichend erscheint, sollten Sie überlegen, ob Sie diesen Dienst bzw. dieses Produkt wirklich nutzen wollen oder ob Sie nicht vielleicht doch lieber darauf verzichten sollten.

Wenn Sie Probleme mit Verstößen gegen den Datenschutz haben, können Sie sich an die Datenschutzbehörden wenden.

RFID

Sie sind der Kunde und zahlen meist viel Geld für Ihre Produkte, da sollten Sie auch Forderungen stellen. Zum ersten, dass Sie informiert werden, dass angebotene Produkte mit RFID-Chips ausgestattet sind. Außerdem sollten die Chips sichtbar

angebracht sein und ohne Folge für die Garantie entfernt bzw. unbrauchbar gemacht werden können. Des Weiteren sollten die Chips nur so gestaltet werden, dass Sie nur durch berechnete Systeme ausgelesen werden können. Datendiebstahl muss mit allen technischen Mitteln verhindert werden, auch wenn es die Firmen mehr Geld kostet. Die Firmen setzen diese Chips ja nicht für Ihre Bequemlichkeit ein, sondern weil Sie hoffen damit mehr Geld durch weniger Personal oder weniger Missbrauch einzunehmen. Daher sollten die Firmen zumindest ein Teil des Geldes wieder in die Sicherheit Ihrer Daten investieren. Des Weiteren sollten Sie die Unternehmen daran erinnern, dass Sie zur Auskunft und Löschung der von Ihnen gewonnen Daten verpflichtet sind. [rfid4; Seite 6]

Als aktiven Zugriffsschutz auf die Daten von RFID-Chips in Karten und Personalausweisen gibt es mittlerweile auch Schutzhüllen im Handel, durch die der Chip von seiner Umgebung abgeschirmt wird. Für technisch Versierte gibt es auch schon Software zum Deaktivieren der Chips (Nähere Informationen unter:[rfid2]).

Soziale Netze

Bei Veröffentlichungen in Foren und Blogs sollten Sie ein Synonym verwenden (mit eigener E-Mail-Adresse sowie eigenem Login und Passwort). Unter Umständen kann es auch sinnvoll sein - je nachdem, welche Ziele Sie mit dem sozialen Netzwerk verfolgen - mehrere Scheinidentitäten aufzubauen (privat und geschäftlich). Wenn Sie schon echte Bilder oder Daten in sozialen Netzwerken einstellen, so sollten Sie den Zugriff soweit wie möglich einschränken. Vergessen Sie dabei nicht zunächst die Einschränkungen einzugeben und erst dann die Daten freizugeben. Achten Sie bei allem was Sie im Internet schreiben darauf die Geheimhaltungsverpflichtungen, die Sie gegenüber Ihrem Arbeitgeber haben, einzuhalten [sozial; Seite 5].

V. Verbesserungsmöglichkeiten

Umkehr bei Erlaubnis für Datenweitergabe

Die Daten sollten nur noch gespeichert und weitergegeben werden dürfen, wenn man das Einverständnis des Dateneigentümers hat. Der momentane Einspruchszwang ist im Informationszeitalter zu unpraktikabel, da man gar nicht mehr weiß, wer welche Daten von einem hat. Dies ist vor allem dann der Fall, wenn man gar nicht mehr mitbekommt, wenn Daten über einen erhoben werden.

Datenbrief

Eine andere Möglichkeit ist der sogenannte Datenbrief, mit dem der Kunde einen jährlichen Überblick über die Daten bekommt, welche bei Unternehmen über ihn gespeichert sind.

RFID CHIPS entwerten

Bei Chips für den Endbenutzer sollten die Chips nach dem Einkauf automatisch beim Verlassen des Ladens funktionsuntüchtig gemacht werden, damit eine weitere Verfolgung nicht mehr möglich ist. Des Weiteren sollte der Kunde das Recht haben, die Chips zu zerstören ohne dadurch negative Folgen fürchten zu müssen. Es sollten keine versteckten Schnüffelchips in Geräten mehr angebracht werden dürfen und die

Entfernung der Chips sollte nicht zum Verlust der Garantie führen [rfid6, Seite2].

Fazit

Viele werden wahrscheinlich anführen, dass in Zeiten von Terroranschlägen der Datenschutz nicht mehr zeitgemäß ist. Allerdings sollten man bedenken, dass man für mehr Sicherheit immer auch ein Stück seiner Freiheit einbüßt. Sich selber in ein Gefängnis einzusperren ist auch keine -zugegeben sichere- Lösung.

Jeder muss für sich selber entscheiden, inwieweit er seine Daten schützen will. Aber wenn man dies will, so sollte man auch in der heutigen Zeit sein Recht auf informationelle Selbstbestimmung wahrnehmen können.

Literatur:

[ababts] HIDE – Homeland Security, Biometric Identification & Personal Detection Ethics; URL:http://www.hideproject.org/references/fp7_projects/ADABTS

[bfdi1] Schaar: Datenschutzrechtliche Verbesserungen beim elektronischen Entgeltnachweis (ELENA) – verfassungsrechtliche Probleme bestehen aber weiterhin; 22.01.2009; URL:http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2009/PM_02_09_DatenschutzrechtlicheVerbesserungenELENA.html?nn=409950

[bio1] CCC; Biometrie; URL:<http://www.ccc.de/de/biometrie>

[bio2] Kim Zetter; Hackers Clone E-Passports; 08.03.2006; URL:<http://www.wired.com/science/discoveries/news/2006/08/71521>

[bio3] Christiane Rütten; ePass-Hack im niederländischen TV demonstriert; 02.02.2006; URL:<http://www.heise.de/newsticker/meldung/ePass-Hack-im-niederlaendischen-TV-demonstriert-171541.html>

[bio4] Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg; 15. Tätigkeitsbericht 2008/2009; URL:http://www.lda.brandenburg.de/sixcms/detail.php?gsid=bb1.c.194872.de&template=allgemeintb15_lda

[cookie] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein; Cookies; URL:<https://www.datenschutzzentrum.de/selbstdatenschutz/internet/cookies/cookies.htm>

[elena] Deutschen Rentenversicherung Bund; ELENA für Teilnehmer; URL:<http://www.das-elena-verfahren.de/teilnehmer>

[flug1] European Union; United States Of America; 2007 PNR (passenger name record) AGREEMENT; 18.07.2007; URL:<http://register.consilium.europa.eu/pdf/en/07/st11/st11595.en07.pdf>

[gez1] Landesdatenschutzbeauftragte Brandenburg; Tätigkeitsbericht 2004/2005;

31.12.2005; URL:http://www.lda.brandenburg.de/media/1666/tb_2005.pdf

[google] Die Landesbeauftragte für Datenschutz und Informationsfreiheit für Bremen; Sie schon – oder sind Sie noch Sie selbst?; November 2008; URL:<http://www.datenschutz-bremen.de/google0.php>

[human] Humanistische Union; Informationen zur Steueridentifikationsnummer; URL:http://www.humanistische-union.de/themen/datenschutz/steuer_id

[ident] Tina Groll; Meine Identität gehört mir!; 11.02.2010; URL:<http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung?page=all>

[indect1] <http://www.indect-project.eu>

[indect2] Andrzej Ciarkowski, Jacek Dajda, José A. Hernández, Paweł Korus, Petr Machník, Gema Maestro, María J. Martínez, Marcin Niemiec, Ralph Roche, Nikolai Stoianov, Pavel Svoboda, Manuel Urueña, Plamen Vichev; Specification of Requirements for Security and Confidentiality of the System; 23.12.2009; URL:http://www.indect-project.eu/files/deliverables/public/INDECT_Deliverable_D8.1_v20091223.pdf/at_download/file

[indect3] Czesław Jędrzejek, Pavel Nevlud, Gema Maestro, María José Martínez Gil; Intelligent Portal for Crisis Management – Functional Specification and Conceptual Architecture; 31.12.2009; URL:http://www.indect-project.eu/files/deliverables/public/INDECT_Deliverable_D6.2_v20091230.pdf/at_download/file

[indect4] David Hambling; Future police: Meet the UK's armed robot drone; 10.02.2010; URL:<http://www.wired.co.uk/news/archive/2010-02/10/future-police-meet-the-uk%27s-armed-robot-drones.aspx>

[indect5] Sharon Weinberger; French Reveal Plans for Taser Flying Saucer; 27.11.2007; URL:<http://www.wired.com/dangerroom/2007/11/french-reveal-p>

[konto1] Bundesministerium der Finanzen; Monatsbericht des BMF September 2009; URL:http://www.bundesfinanzministerium.de/nr_53848/DE/BMF_Startseite/Aktuelles/Monatsbericht_des_BMF/2009/09/inhalt/Monatsbericht-September-2009.property=publicationFile.pdf

[konto2] Bundesfinanzhof; Bankgeheimnis steht nicht generell Kontrollmitteilungen anlässlich einer Bankprüfung im Wege; Urteil vom 9. Dezember 2008 VII R 47/07 URL:http://www.bundesfinanzhof.de/www/presse/pr2009/PM_24.2009.pdf

[konver] Die Landesbeauftragte für Datenschutz und Informationsfreiheit für Bremen; wächst zusammen, was nicht zusammen gehört/e; Dezember 2009; URL:<http://www.datenschutz-bremen.de/konverg0.php>

[local] Die Landesbeauftragte für Datenschutz und Informationsfreiheit für Bremen; 1, 2, 3, 4, Eckstein – niemand soll versteckt sein!; November 2009;

URL:<http://www.datenschutz-bremen.de/locbase0.php>

[maut1] Bayerische Landesbeauftragte für den Datenschutz; Punkt 6.3.1 Mautdaten - Keine Verwendung zu Strafverfolgungszwecken; 1.2.2007; URL:<http://www.datenschutz-bayern.de/tbs/tb22/k6.html>

[maut2] Toll Collect; Nutzerinformationen; Stand: 11/2008; URL:http://www.toll-collect.de/pdf/benutzerinformation/web_einfuehrungstex_dt.pdf;jsessionid=A2C3F3882D33EA25FB32F51E035844FE

[melde1] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein; Speicherung von Meldedaten durch Adresshändler ist unzulässig; Pressemitteilung vom 26.08.2008; URL:<https://www.datenschutzzentrum.de/presse/20080826-adresshandel.html>

[profil] Die Landesbeauftragte für Datenschutz und Informationsfreiheit für Bremen; "... (nur) in Krimis ist der Profiler der Gute!"; November 2008; <http://www.datenschutz-bremen.de/profiler.php>

[rfid1] Christian Rentrop; Geld sparen durch RFID-Manipulation; 30.07.04; URL:<http://www.netzwelt.de/news/66812-geld-sparen-rfid-manipulation.html>

[rfid2] Bastian Ballmann; RFID - Radio Frequency Identification; 29. Februar 2004; URL:<http://dasalte.ccc.de/cards/rfid>

[rfid3] Die Landesbeauftragte für Datenschutz und Informationsfreiheit für Bremen; Ich seh' etwas, was Sie nicht sehen: Ihre Daten; November 2008; URL:<http://www.datenschutz-bremen.de/rfid0.php>

[rfid4] Berliner Beauftragter für Datenschutz und Informationsfreiheit; Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg; RFID-Technologie - Funkchips im Alltag; Januar 2010; URL:http://www.lda.brandenburg.de/sixcms/media.php/2232/fa_rfid.pdf

[rfid5] Bundesamt für Sicherheit in der Informationstechnik; **Risiken und Chancen des Einsatzes von RFID-Systemen**; 2005; URL:https://www.bsi.bund.de/cae/servlet/contentblob/482266/publicationFile/30574/RIKCHA_barrierefrei_pdf.pdf

[robin] Die Landesbeauftragte für Datenschutz und Informationsfreiheit für Bremen; Robinsonliste; URL:<http://www.datenschutz-bremen.de/tipps/robinsonliste.php>

[schlüssel] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein; Verschlüsselte Kommunikation mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein; URL:<https://www.datenschutzzentrum.de/material/themen/pgp>

[schufa1] Verbraucherzentrale Bremen; 15 Fragen und Antworten zur SCHUFA mit einem Musterbrief: „Wie wehre ich mich gegen falsche Einträge bei der SCHUFA“; 09.08.2007; URL:http://www.verbraucherzentrale-bremen.de/beratung/verbraucherrecht/probleme_schufa.html#s1

[schufa2] Verbraucherzentrale Bayern; Häufige Fragen zur Schufa - FAQ's; 10.02.2005; URL:http://www.vis.bayern.de/finanzen_versicherungen/finanzierung/schufa.htm

[schufa3] Dieter Korczak & Michael Wilken; Bericht Verbraucherinformation Scoring; 06.2009; URL:http://www.bmelv.de/cae/servlet/contentblob/638114/publicationFile/36111/Scoring.pdf?bcsi_scan_05DE6D444A73ACDA=ICcwv0tMrB7WcUYpIvdx6ZK6UEcHAAAApIekAQ==&bcsi_scan_filename=Scoring.pdf

[schufa4] Bundesverbraucherministerium; Pressemitteilung 178; 19.08.2009; URL:http://www.bmelv.de/cln_093/SharedDocs/Pressemitteilungen/2009/178-Verbraucherinformation-Scoring.htm

[sozial] Die Landesbeauftragte für Datenschutz und Informationsfreiheit für Bremen; Sie auch schon auf Ihre Privatsphäre?; Dezember 2008; URL:<http://www.datenschutz-bremen.de/socnet0.php>

[ssl] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein; Webzugriffe mit SSL; URL:<https://www.datenschutzzentrum.de/selbstdatenschutz/internet/SSL/index.htm>

[steuer1] Clemens Brandt, Andreas Hinnerichs, Jörn Hoffmann, Michael Wilz; Lohnsteuerliches Ordnungsmerkmal, steuerliche Identifikationsmerkmale und „informationelle Selbstbestimmung“; 09.02.2004; URL:<http://ig.cs.tu-berlin.de/oldstatic/w2003/ir1/uebref/BrandtEtAl-Gutachten-G1-022004.pdf>

[swift1] Bundesrat; Beschluss des Bundesrates 788/09; 27.11.09; URL:[http://www.bundesrat.de/cln_090/SharedDocs/Drucksachen/2009/0701-800/788-09_28B_29.templateId=raw.property=publicationFile.pdf/788-09\(B\).pdf](http://www.bundesrat.de/cln_090/SharedDocs/Drucksachen/2009/0701-800/788-09_28B_29.templateId=raw.property=publicationFile.pdf/788-09(B).pdf)

[ubi] Die Landesbeauftragte für Datenschutz und Informationsfreiheit für Bremen; nur Fische sollten sich vor Netzen hüten; Dezember 2008; URL:<http://www.datenschutz-bremen.de/ubic0.php>

[video] Deutsche Hochschule für Verwaltungswissenschaften in Speyer; Kolloquium zum Thema "Datenschutz und e-government"; 4. Referat: "Videoüberwachung: Geschichte – Rechtsvorschriften - Beispiele"; Sommersemester 2008; URL:http://www.datenschutz.rlp.de/de/service/reden/20080611_lfd_-_Videoueberwachung.pdf

[vorrat] Chaoming Song, Zehui Qu, Nicholas Blumm, Albert-László Barabási; Limits of Predictability in Human Mobility ; 19.02.2010; URL:<http://www.sciencemag.org/cgi/content/abstract/sci.327/5968/1018?maxtoshow=&hits=10&RESULTFORMAT=&fulltext=Mobility&searchid=1&FIRSTINDEX=0&issue=5968&resourcetype=HWCIT>

[vpn] „Technik“ und „Medien“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ; Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet; November 2008; URL:<http://www.lfd.m->

v.de/dschutz/informat/internet/oh-internet.pdf