Eigen(daten)schutz in der Informationsgesellschaft

Dr. Dieter Klumpp

Abendvortrag auf der Tagung
„Überwachung überall? Steht die Privatsphäre vor einer grundsätzlichen Neubewertung?“
Evangelische Akademie Tutzing
Tutzing
27. Juli 2002

Der unverzichtbare Eigenschutz in der Informationsgesellschaft ist unterentwickelt und bedarf dringend der nachhaltigen Impulse aus der Rechtswissenschaft, der Organisationswissenschaft, der Informationswissenschaften, der Jetztzustand zeigt nicht zuletzt großen Handlungsbedarf aller drei staatlichen Gewalten auf.

Zunächst soll die Begriffswahl „Eigendatenschutz“ erklärt sein, obwohl es doch eingeführt den Begriff des „Selbstdatenschutzes“ gibt, der damit keineswegs verdrängt werden soll[1]. Aber der „Selbstschutz“ wird überwiegend in Zusammenhang mit einem „Angreifer“ verwendet, in unseren Netzwelten also ganz unterschiedliche Gruppen wie der schlimme Spammer, der böse Hacker, der ganz böse Cracker, der menschenverachtende Netzterrorist und nicht zuletzt der gute fürsorgliche Rechtsstaat. Nicht vergessen werden soll in diesem Zusammenhang auch der „gemeine Datenvoyeur“, der fremde Daten ganz ohne aggressive Absichten zu seinem eigenen Vergnügen sammelt. Alexander Roßnagel erläutert den Selbstdatenschutz, der „(...) durch technische Möglichkeiten der digitalen Signatur, des anonymen und pseudonymen Handelns, der Verschlüsselung, Steganographie und viele weitere technische Hilfsmittel verbessert werden kann“. Er sieht im Selbstdatenschutz „zwei Vorteile: Der Bürger oder das Unternehmen sind aus *Eigeninteresse* ebenfalls ständig lernende und sehr rasch reagierende Systeme. Daher ist es – wo dies möglich erscheint – sinnvoller, sie in die Lage zu versetzen, den ihnen jeweils wichtig erscheinenden Selbstschutz jederzeit realisieren zu können, als sie durch flächendeckende Vorgaben zwangsweise zu beglücken“[2].

Die Konnotationen der deutschen Sprache zu Begriffen wie „Eigeninteresse“ sind nicht durchweg empirisch nachvollziehbar. Oft handelt es sich um ein unterstelltes oder gar konstruiertes „Eigeninteresse“. Das Zitat von Roßnagel zu den „rasch reagierenden Bürgern und Unternehmen“ interpretiere ich als eine „self-fulfilling prophecy“, die andere als dieser äußerst feinsinnige Mensch[3] exklamativ mit „die dürfen doch nicht gegen ihr eigenes Interesse sein?“ ausdrücken würden. Bei Stefan Dokters Web-Kanzlei steht unter „Eigenschutz“ ebenfalls nur der „technische Selbstschutz“[4] etwa gegen frame-linking und derlei.

Die deutsche Sprache ist bekanntlich nicht systematisch, sondern radikaldemokratisch. Es heißt eben Eigenarbeit, nicht Selbstarbeit, und Eigenheim, nicht Selbstheim. Aber es gibt auch die „Selbstbedienung“, nicht die Eigen-Bedienung, einerseits die Selbstbestimmung und andererseits die Eigenverantwortlichkeit. Und aktuell wird ja nicht von einer Eigen-AG oder einer Selbst-AG gesprochen, sondern unmissverständlich zeitgeistig sogar von einer „Ich-AG“.

Ich benutze den Ausdruck „Eigendatenschutz“ zunächst eher in der Konnotation von „Eigenarbeit“ bzw. „Eigenbau“, und meine damit den mühsamen Prozess, die eigenen Daten und die anderer vor dem eigenen inneren Schweinehund zu schützen, der seit Menschengedenken

---

[1] Vgl. hierzu Roßnagel/Wedde/Hammer/Pordesch, Digitalisierung der Grundrechte, 1990, S.220
[2] Roßnagel, Allianz von Recht und Technik, Stiftung 2001
[3] schon mehrfach hatte ich das Vergnügen, Roßnagel simultan für Entscheider übersetzen zu dürfen. So bedeutet bei ihm „nicht optimal“ in etwa „völlig falsch“, „nicht recht nachvollziehbar“ ziemlich exakt „Bockmist“.
[4] Vgl. Dokters, www.web-kanzlei.de, Haftung für Hyperlinks, IV

bekanntlich faul, träge und nachlässig ist. Dies bezieht auch die datenschutz-ergonomisch schlechten Tools ein, die der Softwaremarkt bietet. Aber auch die unmittelbare Gefahrenabwehr soll natürlich nicht zu kurz kommen. Das Polizei- und Ordnungsrecht kennt den „Eigenschutz“ im Zusammenhang mit der Inanspruchnahme unbeteiligter Dritter: „Nur wenn die Beseitigung der Gefahr weder durch Inanspruchnahme eines Verantwortlichen, noch durch Eigenabwehr der Behörde möglich ist, ist es zulässig, den unbeteiligten Dritten als Notstandspflichtigen zur Gefahrenabwehr heranzuziehen“.

Es könnte - wenn man das heutige Tagungsthema rund um die bedrohte Privatheit zuspitzt - durchaus sein, dass ein solcher „Notstand“ beim Datenschutz entsteht, dass man die Netzbürger zu „Notstandspflichtigen“ machen, und sie sogar unter Sanktionsdrohung zum Eigendatenschutz auffordern muss. Mit einer einfachen Anweisung oder einem Gesetz wäre es aber nicht getan, der Staat müsste zunächst seine Ohnmacht eingestehen. Roßnagel sagt: „Wenn der demokratische Rechtsstaat seine Bürger...nicht mehr zuverlässig schützen kann, muss er sie zum Ausgleich zum Selbstschutz befähigen. Es muss sie stark machen, eigene Instrumente zu ihrem Schutz selbstbestimmt einzusetzen (...). Der Staat reduziert seine Verantwortung von einer Erfüllungsverantwortung zu einer Strukturverantwortung“. Den vielen Paradoxien steht also eine voran, dass nämlich der Staat zuallererst eine allgemeine und gesamtgesellschaftliche Schutzverantwortung hat, aber aus dieser übergeordneten Schutzverantwortung heraus die spezielle Schutzverantwortung, zum Beispiel den Eigendatenschutz, nicht aktiv fördert.

Die zum Teil recht unsachlichen Diskussionen um den Datenschutz aufgrund der Terrorismusbedrohung haben erneut als neue Spitze des Eisbergs alles unter Wasser gedrängt, was dort schon seit Jahrzehnten heranwächst. Deswegen soll anhand möglichst konkreter und aktueller Beispiele betrachtet werden, welche Hürden allein für einen eigenverantwortlichen selbstverantwortlichen und rechtsgemäßen Umgang mit moderner Informations- und Kommunikationstechnik dem schlappen Wanderer in seinen Weg zur Informationsgesellschaft stellen.

Eigendatenschutz auch ohne Angreifer

In der ausdifferenzierten Datenschutzdiskussion spielt der Schutz der eigenen Daten vor einem selbst oder der Schutz vor Datenverlust aus gutem Grund eine eher untergeordnete Rolle. Denn das hat auch Tradition in der Papierwelt. Die historisch gewachsene Fixierung auf „angreifende Dritte“ hat das Briefgeheimnis sogar ins Grundgesetz gebracht. Vor allem wird dabei überwacht, dass der *Transport* der Briefe auf einem vertrauenswürdigen Kanal erfolgt. Nach erfolgreichem Transport liegen die bis dato sorgsam gehüteten Briefe dann ebenso geöffnet wie unsortiert in den berüchtigten Schubladen zuhause und - von der Unverletzlichkeit der Wohnung nicht geschützt - in den Papierstapeln auf Büroschreibtischen. Als junger Praktikant musste ich einmal einen luftdicht versiegelten und „wirklich ganz vertraulichen“ Brief meinem Chef überbringen. Nach eingehender Prüfung des Siegels las er ihn vor sich auf dem Schreibtisch, ich las ihn als Gegenüber „verkehrt herum“ aus Neugier sogar schneller als er (es war eben vor meiner Lesebrillenzeit). Später lag der Brief tagelang im Vorzimmer im Ablagekorb und wurde mindestens von einem halben Dutzend Unbefugter gelesen. Schlussfolgerung: Nicht der Brief, sondern wohl das Siegel war vertraulich.

Der gedankenlose und schlampige Umgang mit den eigenen Daten und Informationen ist also keine Entwicklung der Netzzeit. Nach einem Jahrzehnt Speicherung und mindestens fünf PC-Generationen sieht es auf den Festplatten der PCs und der Server aus wie bei Hempels unter dem Dach. Der einzige Unterschied zu den Papierhaufen ist dadurch gegeben, dass die ganz hartnäckigen Anhänger des Data Mining glauben, man könne mithilfe von Browsern aus diesem ganzen Informationsschrott noch „Wissen“, gar „corporate knowledge“ generieren,

das nachfolgenden Generationen das Leben leichter macht[1]. Auch Ordnung hilft übrigens nicht entscheidend weiter, wie Notare und Nachlassverwalter wissen: Während Bücher noch immerhin einen Kilowert (und schlimmstenfalls einen Kilowattwert) haben, fliegt Opas säuberlich geordnete Diasammlung („Berchtesgaden 1963“) nach einer gewissen Schamfrist auf den Müll. Den Festplatten droht dasselbe Schicksal als Grabbeigabe der DV-Dynastien des 21. Jahrhunderts. Ausscheidende Büromitarbeiter kopieren die ganze Festplatte noch einmal, nicht um wie weiland Señor Lopez einen neuen Berufsstart zu erleichtern, sondern in der vergeblichen Hoffnung, sie würden noch einmal von der alten Firma angerufen und könnten dann Auskunft geben.

Die Hoffnung aller willensschwachen Benutzer, auf Festplatten mit Computerhilfe besser Ordnung halten zu können, ist von den dominanten Office-Suite-Herstellern überall enttäuscht worden. Die aus der DOS-Zeit stammenden Ordnungssysteme, etwa Filenamen wie „BR270702.doc“, was einen Brief von heute bedeutet, helfen überhaupt nicht weiter, wenn man ein Jahr später einen Brief im Zusammenhang mit einer Tagung in Tutzing sucht, deren Datum man sich nicht gemerkt hat. Nach zwanzig Jahren intensivster Forschung über Expertensysteme geben die Office-Textverarbeitungen als Default immerhin als Trost schon einmal einen langen Dateinamen vor, der häufigste Dateinamenvorschlag im Bürobereich lautet bekanntlich „Sehr geehrte Damen und Herren.doc“, der zweithäufigste ist [Ort] [Datumsfeld].doc. Die überall immer wieder aufs neue entdeckten Praktiken, die Ordner- oder Dateinamen mit Präfixen wie „WICHTIG“ zu versehen, scheitern trotz Volltextindexierung entweder an der schieren Masse oder am Informationsparadox zweiten Grades. Das Informationsparadox ist bekanntlich die Tatsache, dass man den Wert einer Information erst dann bestimmen kann, wenn man sie vollständig hat. Bei den Eigeninformationen (nicht: Selbstinformationen), die man ja plausibler Weise vollständig hat, bemerkt man den Wert erst dann, wenn man sie sucht und nicht mehr findet.

Es gibt dennoch eine signifikante qualitative Änderung in der Informationsgesellschaft. Sensitive personenbezogene Daten wurden in der Papierzeit überwiegend Briefen und Tagebüchern anvertraut, die meist schon einen Wohnungsumzug nicht überstanden. Die entsprechende Katharsis-Funktion im Büro für die Aktennotizen oder Hausbriefe hat der gnädige Reißwolf oder der angeblich "„sicher entsorgte Papiercontainer" der örtlich zuständigen Müllmafia übernommen. In einer Welt der Knopfdruckkommunikation hingegen werden personenbezogene Daten wild herumgemailt, kopiert und weitergemailt, zwischendurch auch noch zur Sicherheit mehrfach ausgedruckt[2]. „Zur Sicherheit“ werden auch Dutzende (meist unbeschrifteter) „Backup-CDs“ gebrannt, die entlang der Entwicklung der Staubschicht in den Abfall wandern. Irgendwann landen diese Informationen im richtigen Kontext, also elektronisch bei einem Interessierten von der Kategorie Adressenhändler oder als Print-Output beim Zeitungsvolontär, der auf der Müllhalde einen karrierestützenden aufsehenerregenden Fund macht. Der seit 25 Jahren erschallende Appell der Datenschützer zur „Datensparsamkeit“ im Zuge eines Selbstdatenschutzes erscheint in diesem Zusammenhang als nostalgische Reminiszenz ohne relevanten Aufforderungscharakter. Selbst wer wenige Daten erzeugt, kopiert sie unverdrossen „zur Sicherheit“, womit er - paradoxerweise - das Sicherheitsproblem erhöht.

Eigendatenschutz als Kompetenzproblem

Man könnte meinen, dass hinreichende Kompetenz der Benutzer solche alltäglichen Schlampereien und Unbedachtheiten der „Klick-Kommunikation“ verhindert. Hier ist deutli-

---

[1] eine Spekulation, die nur beim akademischen Nachwuchs aufzugehen scheint: der „Dr. c. p.“ (copy and paste) ist schon längst Wirklichkeit.

[2] Vgl. vom Verfasser: Ethik, Bildung und Wissen in Netzwelten, Stiftungsreihe 45, Alcatel SEL Stiftung 2001

che Skepsis angebracht. Die Simulationsstudie von provet[1] mit dem Signatureinsatz im juridischen Bereich zeigte recht deutlich, dass viele Anwälte trotz nachgewiesener Nutzerkompetenz ihre Passwörter aus ganz praktischen Gründen an die Sekretärin weitergaben. Selbst die relativ hohen Anforderungen der CEPIS Skill Card[2] zum Selbstdatenschutz sind bei genauem Hinsehen zu großen Teilen der Kategorie „gute Vorsätze" zuzuordnen, die bekanntlich nie lange genug halten. Bei hinreichend erfahrenen und hochqualifizierten Benutzern wie etwa Vollprofis in Rechenzentren taucht unvermeidbar und regelmäßig auch das Vigilanzproblem auf, wonach Auffälligkeiten in der Masse der Routinearbeit routinemäßig übersehen werden.

Um es ein erstes Mal zu sagen: Eine nachhaltige Lösung kann nur darin bestehen, dem Nutzer Automatismen in der Dateiverwaltung und spezielle Software-Agenten zu bieten, die ihm helfen, seinen Eigendatenschutz regelmäßig zu überprüfen. Mit einem - abschaltbaren - Büroklammermännchen ist es aber nicht getan, hier muss das Leitbild eher der „Eigen-Server" sein, der auch den einzelnen PC wie ein virtuelles Helpdesk unter einem vorgegebenen Qualitätszwang verwaltet. Ein konkretes Vorbild könnte die Anzeige des Autobordcomputers sein, die auf notwendige Wartungsarbeiten hinweist. Voraussetzung für solche technischen Hilfen ist allerdings ein Leidensdruck, der sich weder bei Benutzern noch bei den Herstellern von Hardware und Software einstellen will.

Ein manifester Leidensdruck „von unten" wird wohl niemals entstehen. Es hat auch nie eine Autofahrerdemonstration mit dem Ziel stattgefunden, man möge rasch den Anschnallgurt und den Airbag erfinden und auf den Markt bringen, ganz im Gegenteil, es gab und gibt Widerstände, weil das Gurtanlegen lästig ist. Und beim Airbag weiß man ja nicht einmal, ob er im Bedarfsfall funktioniert. Ganz genau so (wenngleich ohne lautstarke Begleitmusik durch PC-Clubs, wenn man vom Threat bei Heise Online absieht) würde es auch einem „Databag" gehen, der zum Schutz des Benutzers den Eigendatenschutz verbessert.

Ein „Databag" ist - soweit der allwissende Google das weiß - bisher lediglich als Ausdruck für kommerziell angebotene Tools bei Festplattencrash, als Datensicherung im Flash-ROM oder auch für eine praktische Tasche („MultiSmart bag") für den Laptop aus Polyester in Benutzung. Im Zusammenhang mit Selbstdatenschutz oder Eigendatenschutz wird eine derartige Funktionalität nicht einmal erwähnt. Niemand macht sich dafür stark, also werden weder Markt noch Staat auf den Plan gerufen. Es wird ceteris paribus keinen „Databag" im umfassenden Sinn geben. Hingegen könnten und sollten einige notwendige Funktionalitäten mit mehr Nachdruck in der Expertenzirkeln bis hin zu den Normungsgremien diskutiert und vorangetrieben werden. Interessierte an einem Arbeitskreis von ITG und GI dürfen mir übrigens gerne ihre persönlichen Daten weitergeben.

Eigendatenschutz als Wiederentdeckung von Ort und Zeit

Tagtäglich werden über das Instrument PC Prozesse angestoßen oder Verabredungen getroffen, die der gemeine Benutzer gar nicht als „Vertrag" ansieht und deswegen auch keine Veranlassung hat, eine Unterschrift zu leisten oder gar eine „Signatur" zu verwenden. Für die Ablage solcher alltäglicher Vorgänge auf dem Festplattenspeicher ist die Spalte „Uhrzeit" sehr hilfreich, weil man zum Beispiel verschiedene (natürlich mit demselben Filenamen versehene) Versionen eines Schriftstücks in einer Zeitreihe zur Verfügung hat. Immer wieder kommt es dabei aber zu den hässlichen kleinen Büropannen, weil man doch die falsche Version druckt oder gar verschickt. Erklärung ist dabei oft die PC-Uhr, die aus unerfindlichen Gründen keine „Funkuhr" oder „Netzuhr" ist, sondern von jedem PC aufgrund der Nutzereinstellung erzeugt wird. Viele Nutzer fragen, warum ausgerechnet die PC-Uhren immer wieder nachgehen, eine Nachprüfung bei 10 PCs in meiner Umgebung brachte Zeitabweichungen in einer Spanne von fast 25 Minuten. Der Grund ist rund achtzig Jahre alt und liegt in der Tatsa-

[1] Simulationsstudie Gesundheitswesen bei Dr. Otto entliehen!?
[2] Siehe www.ecdl.de, www.cepis.org

che, dass sich die USA nach einer vorangegangenen ebenso langen Diskussion auf einen Wechselspannung mit einer 60-Hertz-Frequenz geeinigt hatten. Der US-normierte Quarz für die PC-Uhr wundert sich in Europa millionenfach, dass er hier nur 50 Hertz Wechselspannung bekommt. Die daraus resultierenden Probleme bei der Dateiablage sind leicht vorstellbar. Aber auch gravierendere Dinge („meine Mail an Sie hat offensichtlich drei Stunden gedauert, das muss am Provider liegen") muss man nicht explizieren. Und was man im Alltagsleben mit einem rückdatierten Dokument anrichten kann, weiß auch jeder mit ein wenig Phantasie. Erwähnt seien nur die harten Bestimmungen des Deutschen Patentrechts in Bezug auf Veröffentlichungen.

Das Netz - zumindest aber die professionelle Seite der Netznutzung - braucht eine global synchronisierte Netzzeit. Es wäre sehr hilfreich, wenn das Fernmeldenetz, das übrigens zur Synchronisierung der Datenpakete ohnehin auf die Atomzeit zurückgreift, auf jedes Dokument automatisch einen codierten Zeitstempel aufbrächte, dessen Entschlüsselung im Streitfall notwendige, wenngleich nicht hinreichende Anhaltspunkte oder gar Evidenzen erbringt. Es ist jedem klar, dass auch ein verschlüsselter „time stamp" kopiert werden kann, deswegen sei nochmals gesagt, dass dies für die Dokumente, die aus dem alltäglichen Prozess heraus unversehens doch gebraucht werden, bestimmt ist. Er ersetzt nicht die akkreditierte Digitale Signatur, sondern trägt dazu bei, dass diese nicht den einzigen Halt im digitalen Nirwana darstellt.

Ebenso wichtig für die Alltagskommunikation über das Netz, aber auch für jedes an einem PC erzeugte Routinedokument wäre ein zu schaffender „location stamp". Gekoppelt mit dem Zeitstempel würde ein Ortsstempel automatisch und verschlüsselt aufgebracht. Ein solcher Stempel kann technisch sowohl über Mobilfunk-Basisstationen als auch per Satellit über GPS oder Galileo generiert werden. Bei Firmen würde dies im Server implementiert werden, ebenso bei Intranets, aber auch Einzelplatzlösungen für den PC wären machbar. Diese Kombination aus Zeit- und Ortsangabe wäre ein wichtiger Beitrag für den Eigendatenschutz auf Feldern wie E-Commerce oder besonders Electronic Government. Im Electronic Government halte ich ohnehin ein geographisch exakt fixiertes Intranet für eine wichtige Voraussetzung, im globalisierten Netz wieder eindeutige Rechtsräume zu schaffen.

Mit dem Zeit-Orts-Stempel wäre es möglich, strittige Punkte wie den gültigen Rechtsraum - Deutschland - EU - USA etc. - besser meistern zu können. Perspektivisch ließe sich sogar in jeder beliebigen Applikation ein „Ankerwert" für den Rechtsanspruch festlegen, ganz vordergründig könnte man für das Verfassen einer E-Mail genauso Zeugen beibringen wie für das Verfassen eines Briefes. Die Wiederentdeckung des Ortes im globalen Netz wäre eine zweite Bedingung, die infrastrukturell für einen hinreichenden Eigendatenschutz erfüllt werden muss. In diesem Leitbild eines technisch-infrastrukturellen Eigendatenschutzes lassen sich Elemente eines „Daten-Airbags" bereits festmachen. Gewiss: Eine gründliche Abwägung ist erforderlich, ob die evidenten Vorteile eines „Time-Location-Stamp" die Nachteile ausgleichen, die unter anderem darin bestehen, dass autorisierte Stellen oder nichtautorisierte Angreifer in relativ kurzer Zeit oder gar „online" den geographischen Aufenthaltsort eines E-Mail-Schreibers feststellen könnten. Wie so vieles in der Informationsgesellschaft ist auch die Mächtigkeit eines solchen Instruments letztlich von einem großen Unbekannten abhängig, den wir ja mit der Bezeichnung „Vertrauenswürdiger Dritter" seit Jahrzehnten kennen, dem wir aber leider immer noch nicht begegnet sind. Ich habe schon früher darauf verwiesen, dass etwa im Bereich Electronic Government die „öffentlichen" (also staatlichen) Stellen von allzu vielen Menschen offensichtlich eher als „para-polizeiliche" Stellen im Sinne einer ständigen Kontrolle empfunden werden[1]. Ich halte es aber schon seit langem für denkbar, dass man den

[1] Vgl. Klumpp, D., Electronic Government - in zwei oder in zwanzig Jahren? Eröffnungsvortrag auf der Fachtagung für Führungskräfte des Städtetages Baden-Württemberg, veranstaltet von der Evangelischen Akademie Bad Boll und dem Städtetag Baden-Württemberg, Bad Boll, 24. 09. 2001, in: Modernisierungschance Electronic Government, Stiftungsreihe der Alcatel SEL Stiftung, Stuttgart 2002, S.18 ff

„vertrauenswürdigen Dritten“ sogar privat organisieren und akzeptabel machen kann, wenn denn die richterliche Kontrolle gewährleistet ist. Inzwischen gehe ich so weit, dass dieser vertrauenswürdige Dritte - gestalterischen Willen vorausgesetzt - sogar ein „verplombter“ Computer sein könnte, dessen Plombe nur vom Richter geöffnet werden darf. Andererseits darf solch ein Computer oder Speicher als „Dritter“ nicht automatisch den Nutzer zum Eigendatenschutz zwingen, es droht unweigerlich das „fiat justitia pereat mundus“, also ein noch schlimmerer HAL als der aus Odyssee 2000.

Im Sinne eines Eigendatenschutzes wäre es natürlich eleganter, den Zeit-Ort-Stempel bei einem vertrauenswürdigen Dritten temporär zu hinterlegen, aber man bekäme wieder das Problem, dass der Nutzer einen „sehr bewussten“ Akt der Datensicherung zu machen hätte, was sich im Alltag als illusionär herausstellt. Noch einmal: Der notwendige Kompromiss ist bei einem vom Benutzer kontrollierten Software-Agenten in einem Assistenzleitbild zu suchen.

Insgesamt müssen jedoch auf allen Gebieten temporäre Eigenschutzmechanismen weiter forciert werden, nicht nur bei der Datenkommunikation, sondern auch beim Mobiltelefon der heutigen und künftigen Generationen.

Eigendatenschutz durch Alias-Infrastruktur

Gemäß Verwaltungsgericht Karlsruhe vom Frühjahr 2002[1] darf ein falsch geparktes Fahrzeug nicht abgeschleppt werden, wenn die Mobiltelefonnummer des Fahrers sichtbar im Fahrzeug hinterlegt ist, und dieser innerhalb von fünf Minuten sein Fahrzeug entfernt. Dies ist eine bereits viel geübte Praxis im Alltag, es ist auch ein direkt erlebbarer Nutzen des Mobiltelefons. Andererseits ist dies natürlich auch eine Gelegenheit für Dritte, die Mobilnummer (erkenntlich an der Struktur der Vorwahl) auszuspähen und diese zusammen mit weiteren Angaben (etwa Automarke, Kennzeichen und ggf. sogar Namen) für eine unsachgemäße Verwertung, etwa für Spam-Zwecke, Werbung, Unfug oder sogar Delikte zu benutzen. Mit jeder weiteren zusätzlichen Information wird auf diese Weise aus einer 5-Cent-Adresse eine 5-Euro-Adresse für den Adressenhandel. Dieses Einzelbeispiel ist verallgemeinerbar. Generell wird nach dem Handyboom den Nutzern erst jetzt allmählich deutlich, dass schon allein die Mobiltelefonnummer einen sensiblen personenbezogenen Datensatz darstellt, der in bestimmten Situationen und/oder Lebenslagen äußerst schutzwürdig ist.

Die sich zunächst anbietende Lösung des „Selbstdatenschutzes“ (möglichst sparsame Weitergabe der Nummer) widerspricht der Funktionalität des Telefons an sich. Auch dieses Verhalten ist letztlich erfolglos, weil Nummern Dritter unbedacht weitergegeben werden. Außerdem will man ja auch selbst in bestimmten Situationen angerufen werden können. Zusätzlich ist selbst bei angeblich ergonomisch gestalteten Displayführungen das Umschalten von „Rufnummer anzeigen“ zu „nicht anzeigen“ unter vier Tastendrucken nicht zu haben. Der regelmäßige Wechsel der Telefonnummer ist für Nutzer wie Betreiber aufwändig und kann nur als ultima ratio angesehen werden. Es gibt sogar Angebote, „lebenslange“ Nummern zu erhalten bzw. unter dem Stichwort „Nummernportabilität“ die Nummern von Prepaid-SIM-Karten beim Betreiberwechsel zu erhalten.

Eine Problemlösung könnte ein neuer infrastruktureller Telekommunikationsdienst „Verfügungsnummer“ sein, mithilfe dessen der Nutzer mit dem Bedarf für eine „temporäre“ Telefonnummer seinen Provider unter einer bestimmten Servicenummer anruft, vom Provider eine auf den Anruf bei der Servicenummer automatisch (zufalls-)generierte Verfügungsnummer für einen bestimmten Zeitraum (z.B. 24 Stunden, eine Woche, ein Monat etc.) als kostenpflichtige Dienstleistung zugewiesen bekommt. Die Verfügungsnummer ist fest mit der eigentlichen Nummer verkoppelt und damit konform mit dem Telekommunikationsgesetz. Die-

[1] AZ: 8 K 3615/00

ser offizielle, aber eben temporärer Alias wäre ein äußerst praktischer Eigendatenschutz nicht nur für Mobiltelefone, sondern auch für das Festnetz. Gegen professionelle Spammer, die mithilfe von Wählcomputern „brute force“ alle denkbaren Telefonnummern anrufen oder eine SPAM-SMS schicken, hilft die Verfügungsnummer nichts, aber dieser Fall kommt wegen der nicht klassifizierbaren Zielgruppe gar nicht so häufig vor.

An einer solchen Alias-Struktur als ein Hauptelement eines Eigendatenschutzes geht wohl kein Weg vorbei. Jede systematische Nummern- oder Adressvergabe ist inzwischen strukturell anfällig für Angriffe bzw. Missbrauch. Hans Mustermann hat mit immer höherer Gewissheit eine Adresse nach dem Muster Hans-Punkt-Mustermann@provider.de, wenn der ISDN-Anschluss 4711 auf einen Anrufbeantworter stößt, helfen 4712 fortfolgende weiter. Zu den Passwörtern mit den wenigen Geburtstagsvarianten braucht man erst gar keine Worte zu verlieren. Es wird eine vornehmliche Aufgabe der Netzarchitekten sein, entsprechende Sicherheitsarchitekturen selbst in das gute alte Telefon einzubringen. Denn es steht zu erwarten, dass sich das Problem mit der Durchdringung weiterer Mobilfunkgenerationen vor allem wegen der Bewegtbild-Kommunikation) verschärft.

Eigendatenschutz durch Bildquellenfilterung

Während die Verwirklichung einer Alias-Infrastruktur etwa mit temporären Verfügungsnummern vor allem an der durch ein rein ökonomisches Regulierungsregime erzwungenen Konkurrenz der Betreiber scheitert, die von der technischen Entwicklung ausschließlich exklusive Leistungsmerkmale erwarten, sind die absehbaren Probleme der Breiteneinführung eines Videofons, also des Bildfernsprechers, noch nicht einmal in der technischen Forschung und Entwicklung angekommen. Überraschend ist dies nicht, weil es eine interdisziplinäre Forschung im Wesentlichen nur auf dem Papier gibt - zugegeben: viel Papier. Juristen kennen das Problem des Persönlichkeitsschutzes und des Rechts am eigenen Bild, sie können aber daraus höchstens die Forderung ableiten, den Bildausschnitt der Kameras doch so zu wählen, dass unbeteiligte Dritte nicht erfasst werden. Ingenieure erkennen dieses Problem nicht einmal als existent an, wenn man es ihnen erklärt. Zum einen rührt das aus der Überzeugung der Ingenieure und Naturwissenschaftler, dass alles außerhalb der physikalischen Gesetze nicht nur grundsätzlich änderbar ist, sondern auch bei Bedarf geändert werden sollte. Zum anderen haben sie bei der Ablehnung der „Kamera mit begrenztem Ausschnitt“ die Ökonomen und Psychologen samt der Kommunikationsforscher auf ihrer Seite. Denn die Konsequenz wäre ein nicht akzeptabler Close-Up, eine Nahaufnahme des Gesichts und damit eine völlig unnatürliche Kommunikationsform, insgesamt ein vorprogrammierter Marktflop. Schließlich will man per Bewegtbild auch Konferenzen übertragen, Gruppen ins Bild bringen und auch öffentliche „Bildfernsprechstellen“ einrichten, in die der Anrufer nicht geradezu den Kopf in einen schwarzen Kasten hineinstecken muss. Es erübrigt sich zu sagen, dass es dem Benutzer eines Videofons völlig gleichgültig ist, ob die Persönlichkeitsrechte von zufällig hinter ihm Stehenden verletzt werden könnten. Es gibt also keine Lösung, die Amtsgerichte dürfen sich schon auf die entsprechenden Klagen vorbereiten.

Wahrhaft interdisziplinäre Forschung kann jedoch Lösungen erbringen. In unserem Beispiel des Videofons ist es eine elektronische Kamera, die das Persönlichkeitsschutzproblem herauszufiltern imstande ist. Eine solche Blue-Screen-Kamera ist dadurch gekennzeichnet, dass die elektronische Kamera die über einem bestimmten manuell einstellbaren Abstand (z.B. 2 Meter) festgestellten Bildinhalte in ein gleichmäßiges, international genormtes Blue-Screen-Signal umwandelt. Es werden also lediglich die innerhalb des Schärfebereichs sichtbaren Objekte dargestellt, es kann eine „Discretion Line“ festgelegt werden, wie wir sie aus dem Bankbereich (und demnächst auch aus dem Apothekenbereich) kennen. Im „Videofonat“ (Bildtelefonat) erscheinen also nur die beiden kommunizierenden Seiten, alles dahinterliegen-

de ist völlig neutral blau. „Blau“ hat bekanntlich kein Recht auf das eigene Bild. Amtsgerichte können aufatmen.

Dieses Verfahren lässt sich auch auf viele Arten von Überwachungskameras übertragen. So kann mit der Blue-Screen-Kamera zum Beispiel ferngesteuert ein bestimmter Schärfebereich (z.B. 5m) eingestellt werden, innerhalb dessen sich kein bewegtes Objekt befindet. Zur Überwachungs-Zentrale wird normalerweise nur der Blue-Screen übermittelt. Erst wenn ein Objekt oder eine Person in den Überwachungs-Bereich kommt, wird ein Bild sichtbar; dies entschärft das bekannte Vigilanzproblem durch den Wechsel von „gar kein Bild zu einem Bild“ beim Überwachungspersonal erheblich und kann dadurch auch beim computerkontrollierten automatisierten Einsatz viel Aufwand für Mustererkennung (z.B. ein sich auf das gesicherte Terrain hin bewegender Busch) einsparen.

Dieses Beispiel ist nicht unrealistisch, weil es die Kamera prinzipiell gibt, nur wird sie noch nirgends entwickelt und gebaut, weil sie nirgends nachgefragt wird. Es gibt bis heute keine Nachfrage nach technischen Werkzeugen zur Erzeugung von Eigendatenschutz, also gibt es auch kein Angebot. Mir ist nur ein einziges BMBF-Projekt[1] bekannt, in dem Juristen und Ingenieure explizit die interdisziplinäre Technikgestaltung in Form von Software-Agenten angehen, aber auch von solchen Leitprojekten können dringend für den Eigendatenschutz benötigte innovative Produkte nicht einfach „abgerufen“ oder „bestellt“ werden. Das staatliche System der Forschungsförderung ist strukturell nicht auf innovatorische Zukünfte ausgerichtet, sondern auf die administrative Absicherung von vorzeigbaren Projekterfolgen, die vor allem nicht der ökonomischen Richtlinienkompetenz der EU zum Opfer fallen dürfen. Aus interdisziplinären Forschungsprojekten würden ja ohne diese ideologischen Hemmnisse direkt Produkte für den Eigendatenschutz entstehen. Produkte aber sind Sache der Wirtschaft und dürfen nicht subventioniert werden. Die Wirtschaft entwickelt die Produkte aber nicht, weil keine Nachfrage vorhanden ist. Der Staat hat angesichts seiner stetig wachsenden Finanzierungsprobleme auch kein Interesse daran, an die Stelle der Marktnachfrage - nach dem Muster der kalifornischen Abgasbestimmungen für Motoren - substitutiv eine Vorschrift zu setzen, zumal sich ja niemand für den Eigendatenschutz stark macht und er sich auch nicht als Wahlgeschenk eignet.

Hingegen gibt es eine sehr dynamische Nachfrage des Staates nach datenschutztranszendierenden Instrumenten und Verfahren, dies wird auch gestützt vom „gesunden Menschenverstand“ in Redaktionsstuben und an Stammtischen. Damit löst sich das zu Beginn dargestellte Paradox auf, dass der Staat aus dem Grundrecht der informationellen Selbstbestimmung heraus seine Bürger zu Eigendatenschutz befähigen und zugleich aus seiner Verpflichtung zum Schutz seiner Bürger genau das verhindern muss.

Eigendatenschutz - ein ewiges Auf-der-Stelle treten?

So schließt sich denn der Kreis des erforderlichen Eigendatenschutzes mit der resignativ-optmistischen Feststellung, dass das „ceteris paribus“ ja nur eine mögliche Annahme unter mehreren ist. Begründeten Optimismus ziehe ich aus der Belastbarkeit von Expertenzirkeln, die sich teilweise bis in den späten Samstagabend hinziehen, obwohl doch solches gesellschaftspolitisches Engagement gewiss nicht gerade als „zeitgeistgemäß“ bezeichnet werden kann.

Anstelle einer feuilletonistischen Zusammenfassung soll daher noch ein Szenario als Beispiel dienen, wie man durch rechtzeitige Analyse und Spezifikation zu hochinnovativen Lösungen auch für den Eigendatenschutz kommt, die den Weg zu einer Informationsgesellschaft beschleunigen und nicht bremsen. Das Beispiel ist der Chipkartenausweis, wie er von der EU gefordert und den nationalen Instanzen betrieben wird. Wenn nichts dramatisch Innovatives

[1] Leitprojekt MAP (Mobiler Arbeitsplatz)

geschieht, wird es über kurz oder lang einen Chipkartenausweis geben, mithilfe dessen jeder Ausweisinhaber bei Bedarf identifiziert werden kann. Besonders in Deutschland herrscht dabei ein Leitbild vor, das man mit „Universallösung“ ganz treffend bezeichnen kann. Ein Ausweis soll in Fortführung nicht nur die Identifikationsmöglichkeiten bieten, sondern möglichst auch noch als Authentisierungsinstrument dienen, vielleicht gar als Zahlungsmittel und als Hausschlüssel. Weil für die Identifikation das Passfoto bekanntlich nicht ausreicht, werden nun derzeit alle denkbaren biometrischen Merkmale als „unsicher“ verworfen und nichtsdestotrotz Zug um Zug implementiert. Als wahre Zielstellung entpuppt sich beim genauen Hinsehen ein Wunsch der staatlichen Autoritäten nach 80 Millionen computerlesbaren Bürgern samt der Millionen Besuchern und Durchreisenden. Das wird ceteris paribus kommen.

Bei genauerem Hinsehen zeigt es sich jedoch, dass der alte Ausweis nicht die Identifikation, sondern vor allem die *Gültigkeit* als Hauptfunktion hat. Vor ein paar Wochen wollte ich mit meiner Frau von der sächsischen Schweiz ungeplant über das tschechische Karlsbad zurück nach Stuttgart fahren. Leider war ihr Ausweis vier Wochen abgelaufen, was der deutsche Grenzbeamte bemerkte und die Ausreise nicht gestattete. Alle Versuche, ihm mit Dutzenden von amtlichen Dokumenten, Kreditkarten, Unterschriftsproben und dergleichen zu einer Ausnahme zu bewegen, schlugen fehl. Denn er hatte keinerlei Zweifel an der Identität meiner Ehefrau, zumal sie mir glaubhaft (weil lautstark) Vorwürfe machte, warum ich denn unbedingt über Tschechien nach Hause fahren wolle und was das bitte mit Goethe zu tun habe. Es ging also um die Gültigkeit eines Papiers. Überraschender Nebenkriegsschauplatz war, dass ein deutscher Tagesausweis gemäß Anordnung des Grenzschutzkommandos Ost nicht mit einem Passfoto versehen werden darf, während dieses Passfoto zwei Meter weiter beim tschechischen Grenzbeamten unabdingbar ist. Auch die tschechische Seite hatte keinerlei Zweifel an der Identität meiner Frau, zumal ich einen Gentest vorschlug, aber ein Tagesausweis ohne Foto sei nun mal nicht gültig.

Ich habe mich nach der Erholung von einem über dreistündigen Umweg kundig gemacht und feststellen dürfen: Hauptprobleme mit Ausweisen sind tatsächlich die 1) Fälschbarkeit, das 2) Verlieren und das 3) Verlegen, also alles Dinge, die nur wenig mit der Identifikation zu tun haben. Dies führt zu einer völlig anderen Spezifikation eines denkbaren Chipkarten-Ausweises.

- Auf dem neuen Chipkartenausweis (wie Bahncard mit Foto) wird von der ausgebenden Stelle eine (unendlich) hoch verschlüsselte Randomzahl (o.ä.) gespeichert, deren Algorithmus ausschließlich der ausgebenden Stelle bekannt ist. Wenn ein gültig aussehender Ausweis ohne diese gültigkeitsgarantierende Randomzahl geprüft wird, zeigt das Terminal „ungültig“ an und setzt eine Meldung an eine zentrale Datenbank ab. Eine Fälschung von Ausweisen ist nicht mehr möglich.
- Ein Ausweis mit Chipkarte lässt sich durch den Ausweisinhaber mithilfe autorisierter Stellen über eine zentrale Rufnummer wie „114“ mit sofortiger Wirkung elektronisch als ungültig „sperren“. Bis zur Aktivierung des neuen Ausweises benutzt der Bürger einen nur elektronisch verwendbaren Chipkartenausweis, dessen Einsatz grundsätzlich mit Zeit- und Ortsangabe an eine zentrale Datenbank gemeldet wird. Ein solcher nur elektronisch verwendbarer Chipkartenausweis ist für einen Dritten ohne Wert, weil bei jedem Einsatz sowohl die Datenbank kontaktiert als auch eine weitere Personenidentifikation erforderlich wird.
- Ein verlegter Ausweis lässt sich durch den Ausweisinhaber mithilfe autorisierter Stellen für eine bestimmte Zeit (etwa 1-4 Wochen) in der zentralen Datenbank als „verlegt“ markieren. Der Ausweisinhaber wird per SMS (o.ä.) telekommunikativ in bestimmten Abständen aufgefordert, den Ausweis als „wiedergefunden“ zu melden oder ihn endgültig sperren zu lassen. So lange benutzt er den Notfallausweis.

Ein auf diese Weise spezifizierter Ausweis wäre zugleich ein Beitrag für den Eigendatenschutz, aber auch eine Erleichterung von notwendigen Identifizierungsvorgängen.

Und das macht mich denn doch optimistisch: Gäbe es solche Vorschläge von Fachleuten so rechtzeitig, dass verantwortliche Entscheider darüber einen Konsens herstellen können, dann wäre mir nicht bange um den Weg zur Informationsgesellschaft.

Ich danke für Ihre Aufmerksamkeit.