"Zwar weiß ich viel,
doch möcht' ich alles wissen"
Goethe, Faust

Wer hört mit? (II)

Auf dem Weg zum gläsernen Bürger

Wenn ECHELON und PROMIS die (vermeintliche) Ohnmacht des Einzelnen gegenüber einem Goliath-ähnlichen, staatlichen Überwachungssystem illustrieren, dann ist das Verschlüsselungsprogramm „Pretty Good Privacy" (PGP) der Stein in der Schleuder Davids. Die Bürger, die sich in der schönen neuen Welt der Telekommunikation bewegen, haben allen Grund um ihre Privatsphäre zu fürchten.

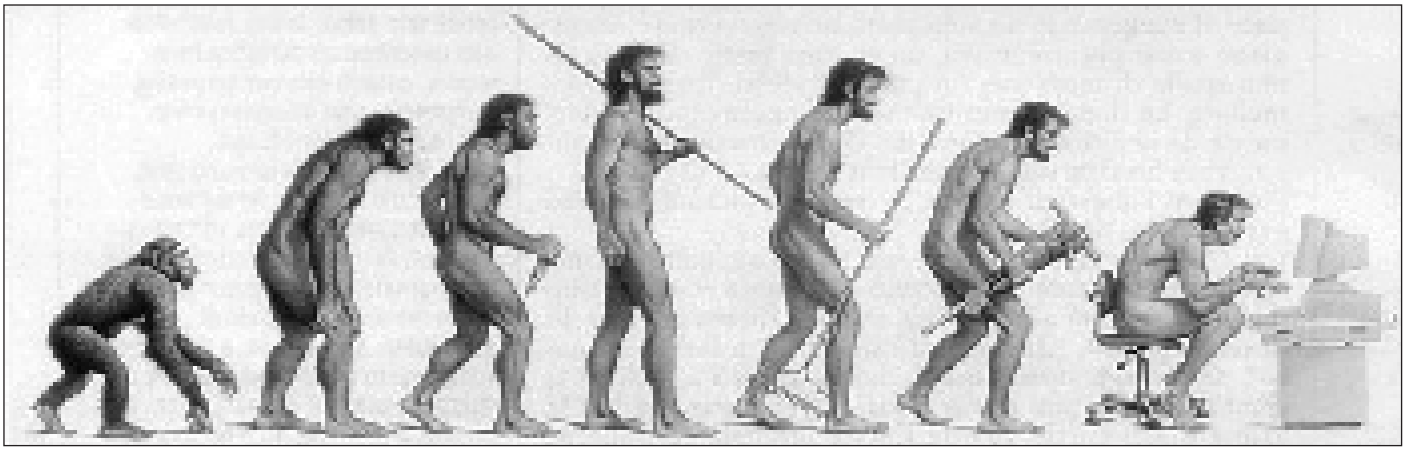
E-mails sind im Prinzip für jeden Teilnehmer im Internet lesbar – fast wie eine Postkarte. Will man ein e-mail verschlüsseln, interveniert der Staat: das Lesbare wird unlesbar und deshalb suspekt. Der Staat aber erlaubt dem Briefeschreiber, seinen Brief in einen Umschlag zu stecken – im Prinzip für keinen außer dem Adressaten lesbar. Was wäre also die Verschlüsselung eines e-mails anderes als ein elektronischer Briefumschlag? Ausgehend von dieser Überlegung entwickelte der Amerikaner Philipp Zimmerman ab 1991 das Verschlüsselungsprogramm PGP. 1993 meldete sich bei ihm die US-Zollbehörde, um Informationen zu PGP einzuziehen. Kurz darauf folgte eine Klage wegen Umgehung der amerikanischen Exportbestimmungen für „Dual-use" Güter: laut amerikanischer Gesetzgebung fällt die internationale Vermarktung von Verschlüsselungs- oder Kryptographiesoftware unter die Bestimmungen über den Export von zivil- und militärisch nutzbaren Gütern. Zimmerman stellte daraufhin kurzerhand PGP im Internet jedem zum Herunterladen gratis zur Verfügung. Es scheint, als sei bis heute der Algorithmus, der PGP zugrunde liegt, noch nicht geknackt. Hauptnutzer von PGP sind nach Aussage Zimmermans Menschenrechtsorganisationen in Drittweltländern, die kaum frei kommunizieren können. In diesen Ländern gäbe es ohne PGP keine Menschenrechte: Verschlüsselung als Garant der Ausdrucksfreiheit.

Die großen Softwarehersteller halten sich mit Aussagen hinsichtlich der Sicherheit ihrer eigenen Verschlüsselungssysteme äußerst zurück. Microsoft etwa hat sich nie zum Thema Schlüsselhinterlegung für die Produkte „Outlook" und „Exchange" bei der NSA geäußert. Allein im Rahmen einer Untersuchung des „Subcommittee on Economic and Commercial Law des Repräsentantenhauses zum Thema „backdoors" beklagte sich Microsoft in einem Brief von August 1992, dass die US-Regierung Druck ausübe, damit „backdoors" in international vermarkteten Softwares eingebaut würden…

Die Lotus Corporation gestand vor mehreren Jahren, dass die Freigabe von „Lotus Notes 4" für den weltweiten Verkauf seitens der NSA erst gestattet wurde, als Lotus die Hälfte des zur Verschlüsselung der mit Notes 4 generierten elektronischen Nachrichten benutzten Schlüssels (24 Bit) bei der NSA deponierte hatte. Die National Security Agency las ab dem ersten Tag sämtliche Notes 4 Nachrichten mit.

Das Argument der US-amerikanischen und einiger weiterer Regierungen, Kryptosoftware schütze nur kriminelle Organisationen, ist ein falsches Argument: Selbst bei einem totalen Verbot würden diese Organisationen selbst-

Evolution, Quelle: www.web-art.de



verständlich massiv Verschlüsselungssoftware einsetzen, um sich vor staatlicher Verfolgung zu schützen. Sie wären dann die einzigen, die über die notwendige Technologie verfügten. Statt den Bürger zu schützen, würde der Staat ihn durch derartige Maßnahmen eher noch größeren Gefahren aussetzen.

Übrigens: PGP, das Unternehmen gleichen Namens, wurde von Network Associates übernommen. Und auch hier schließt sich der Kreis: Im Februar 1998 kaufte Network Associates das Unternehmen Trusted Information Systems, ein Unternehmen, das sich wiederum aktiv an der „Key Recovery Alliance", einer Gruppe von Firmen, beteiligt, die die Entwicklung von Softwareprodukten fördern, die Dritten das Lesen verschlüsselter Daten ermöglicht und sehr enge Verbindungen hat zur… NSA!

Auf die Frage, warum man den einzelnen durch absolute Kryptographie schützen soll, meint Phil Zimmerman: „Durch Allwissenheit könnte eine gute Regierung schlecht werden und eine schlechte noch schlechter. Wir sähen dann einer Orwell'schen Zukunft entgegen."

„Little Shop of Horrors" für den privaten Anwender

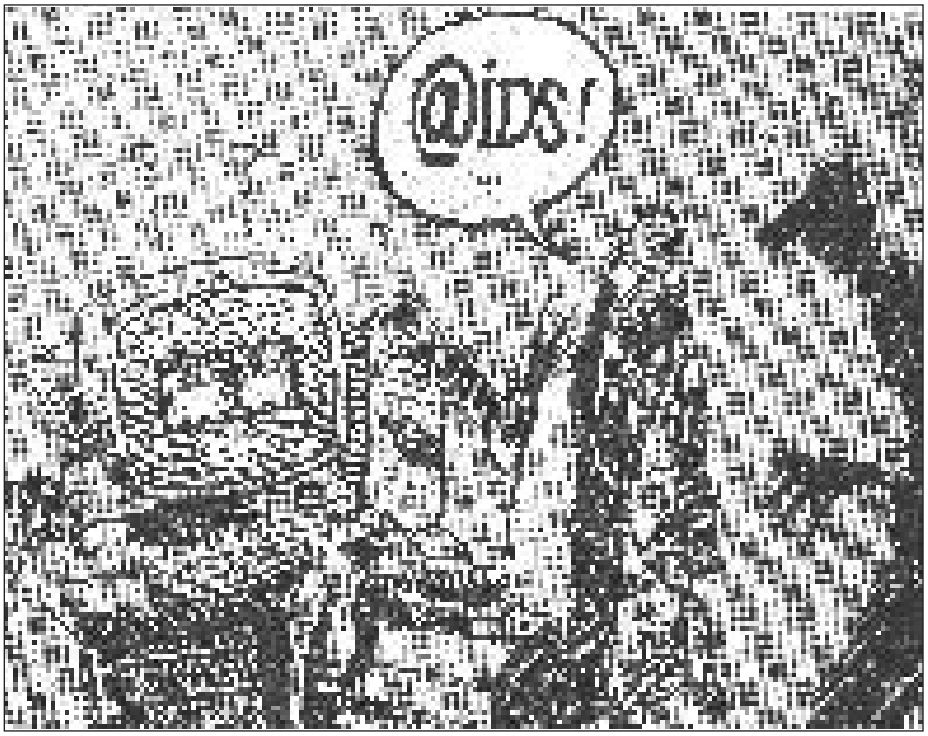
Man kann dem Leser an dieser Stelle nicht verübeln, dass er sich fragt, was ihn das ganze Problem eigentlich angeht. Direkt nichts, außer er ist militanter Verfechter der Bürgerrechte. Oder doch? Einige Beispiele:

Internet ist eine tolle Sache – „mal ein Mausklick hier, mal ein Download da, und niemand weiß, wo ich gewesen war" – bis zu dem Tag, an dem die Spam-Lawine einsetzt (als "Spam" bezeichnet man nicht angeforderte Werbe-e-mails) und man sich gerne einen Aufkleber „Keine Reklamesendungen" auf den Schirm kleben würde. Allein, es hilft nichts. Man hat das kleine Kästchen am untersten Rand des Schirmes übersehen, in dem steht: „Ich bin nicht einverstanden, dass meine Angaben gespeichert und gegebenenfalls Dritten zu Werbezwecken zur Verfügung gestellt werden" und das Kästchen daneben hat man auch nicht angeklickt. Schon ist man ein für Werbetreibende interessantes Profil. Man hat eine Namensangabe, eventuell ein Alter, man weiß woher der Internaut kam und wohin er geht – und dann gibt es ja noch die kleine „Kekse", oder „Cookies", jene Programm-strings die beim Aufrufen einer Home Page auf den Computer des Internauten geladen werden, von diesem oft unbemerkt, und die dem Betreiber der Home Page wichtige Informationen über den Internauten und sein Surf-Verhalten liefern…. Auch aus den Informationen, die ein Cookie liefert, kann man auf Alter, Konsumgewohnheiten, Einkommenslage, geographische Herkunft, etc. des Internauten schließen. Rechtlich geht die Entwicklung, sowohl auf der Ebene der EU, als auf der der Einzelstaaten aber dahin, dass ein Konsument eine explizite Willenserklärung abgeben muss, anhand derer er sich bereit erklärt, Werbemails zu erhalten. Andernfalls steht ihm ein Klagerecht auf Unterlassung zu. Das Pendant des Opt-in Prinzips ist das Opt-out, bei dem Zustimmung unterstellt wird, außer, es liegt eine explizite gegenteilige Willenserklärung vor.

Und ist der e-commerce Surf erst perfekt, zieht der Internaut die Kreditkarte, tippt vertrauensvoll seine Kartennummer ins Nichts des virtuellen Netzes und wundert sich am Monatsende über die astronomischen Abbuchungen: da hat doch glatt jemand die Kreditkarte geclont. Der Franzose Serge Humpich hat vor kuzem mit einer elementaren Grundausstattung bestehend aus einem Computer, einem mechanischen Kartenleser und einem Satz überall erhältlicher Blankokarten die französischen Kartenanbieter das Fürchten gelehrt: die Chip-Kreditkarte ist nicht fälschungssicher! Aber das ist nicht alles: Was macht die Bank mit den Buchungen, die sie von der Kartenclearingstelle erhält, außer sie vom Konto abzubuchen? Ein Kundenprofil erstellen? Warum wohl reiste der Chef einer Luxemburger Großbank systematisch ohne Kreditkarten? Um keine „Spur" zu hinterlassen…

In der Bundesrepublik Deutschland organisiert die SCHUFA, die Schutzgemeinschaft für allgemeine Kreditsicherung, eine Datenbank säumiger Schuldner, deren Informationen an Vertragspartner der SCHUFA auf der Grundlage des Prinzips gegenseitiger Information gegeben werden. Ist Ihr Konto regelmäßig überzogen, wird ebenso regelmäßig mit der SCHUFA gedroht. Wer in welchem Maße

Chappatte, in: Weltwoche, 11.5.2000



Zugang zu den Daten der SCHUFA hat, ist dem Bankkunden nicht ersichtlich. In anderen Ländern als Deutschland, z.B. in Luxemburg läuft dieser Datenaustausch auf informellem Wege, ist dafür aber nicht minder real.

Im Supermarkt zücken Sie nach erfolgtem Einkauf, und nachdem Sie die siebenköpfige Caddie-Schlange an den Kassen überwunden haben, konsumbewusst Ihre Kundenkarte. Ihre Einkäufe werden verbucht und am Ende des Jahres winkt eine Prämie. Was macht der Supermarkt, oder gar die ganze Kette, mit Ihren Daten? Sie sind ein idealer Informationsstock, um Ihnen, Bezug nehmend auf Ihr Einkaufsverhalten, gezielt Direktwerbung zukommen zu lassen.

Unternehmen, wie SOPRES in Belgien zum Beispiel, sind an derartiger Information interessiert. Diese Unternehmen sammeln alle Informationen, die sie über potentielle Kunden erhalten können, aus sämtlichen zugänglichen Quellen: Telefonbücher, Todesanzeigen, Geburts- und Hochzeitsanzeigen, e-mail-Verzeichnisse, etc. Manchmal lässt ein solches Unternehmen Ihnen auch einen Fragebogen zukommen, der Ihr Konsumverhalten analysieren soll. Zweck der ganzen Operation: das Erstellen von Kundenprofilen, zum Zweck des Verkaufs von Datenbanken mit mehr oder weniger gezieltem „targeting" beim Konsumverhalten der aufgelisteten Personen. Handel mit derartigen Datenbanken wird immer schwieriger, bleibt aber ein sehr lukratives Geschäft.

Für die Datensicherheit des Einzelnen bieten Direkt-Marketing Strukturen aber keine wesentliche Bedrohung.

Es bleibt allein als treuer Begleiter das Mobiltelefon, „des Managers Tamagochi". Aber auch ihm ist nicht zu trauen. Es ist heute technisch kein Problem, sowohl ein Mobiltelefon abzuhören, als auch es nur zu lokalisieren, solange es eingeschaltet, aber nicht benutzt wird.

Mann und Frau von Welt seien gewarnt: die Lokalisierung eines Mobiltelefons und die Überschneidung dieses Trackings mit den Spuren, die die Kreditkarte hinterläßt, erlaubt mit ziemlicher Genauigkeit Rückschlüsse darauf, wer wann wo mit wem was erlebt hat…

Im Zusammenhang mit Computerge- und -missbrauch am Arbeitsplatz treffen gleich zwei Überwachungssphären aufeinander: die externe, betrieben durch Hacker und Staatsräson, und die interne, veranlasst durch den Chef, der die Produktivität hoch halten will, und nicht schätzt, dass sein Unternehmen allein für 30% der Hits bei den sites des Portals „Schweinkram.de" den Meritus für sich beansprucht. Totale Überwachung durch den Vorgesetzten wäre sicherlich rechtlich sehr problematisch. Will man eine derartige Überwachung einführen, sollte das Site Monitoring transparent geschehen.

Der alltägliche Angriff auf die Privatsphäre

Beim Wandeln über die Kommerz-Seiten des Internet begegnet einem manchmal bewusst, manchmal unbewusst ein Cookie, jenes kleine Programm, welches der Betreiber der HomePage, die angeklickt wird, auf der Festplatte des Computers des Besuchers installiert. Das Cookie ist, wie gesehen, ein kleiner Spion, der es dem Betreiber der HomePage erlaubt, den Internauten beim nächsten Mal wiederzuerkennen. Informationen, die der Cookie sammelt, können in Verbindung mit den Informationen, die der Computer oder Internet-Server an den besichtigten Site meldet (Name des Servers, Standort des Servers, verwendetes Betriebssystem, etc.), zu einem mehr oder weniger detaillierten Userprofil führen.

Natürlich kann die Annahme von Cookies verweigert werden – doch dafür muss man im Detail die Funktionsweise seines Internetbrowsers (Netscape Navigator oder Microsoft Explorer) kennen, um die Abwehrfunktionen zu aktivieren, oder den Computer von angenommenen Cookies zu reinigen. Bei e-commerce sites wird man den Internauten auch oft dazu auffordern, seine Browsereinstellung zu revidieren, damit Cookies akzeptiert werden – angeblich, weil sie zur Erstellung des gekauften Warenkorbes notwendig sind.

Fraglich ist, wo die so über den Einzelnen gesammelten Informationen letztlich landen, wie sie vernetzt, und verwendet werden. Denn nicht das einfache Sammeln ist wirklich problematisch, sondern die Vernetzung, das Zusammenführen von von einander unabhängig existierenden Datenbeständen – PROMIS winkt aus der Ferne.

Auch der alltägliche Gebrauch des Computers wirft nicht unerhebliche Fragen auf: Beim Installieren einer neuen Software wird der Benutzer aufgefordert, einen Lizenzvertrag, der auf dem Bildschirm erscheint, durchzulesen und die Zustimmung zu den Vertragsbedingungen zu quittieren. Tut man das nicht, ist eine Installation oft nicht möglich. Nimmt man den Vertrag an und clickt z.B. auf „OK", ruft ein kleines Progammanhängsel die Softwarefirma an und meldet den Benutzer als neuen Lizenznehmer. Zusätzlich läuft – unbemerkt von dem Benutzer ein „Agent"-Programm (noch ein kleiner Spion) an und prüft die Art der Programme, welche auf dem Computer installiert sind. Auch diese Information wird an die lizenzgebende Softwarefirma zurückgemeldet – angeblich zum Vorteil des Kunden, u.a. zu dessen Absicherung gegen fehlerhafte Raubkopien. Was sich der „Agent" im Innenleben des Computers wirklich alles anschaut und zurückmeldet, ist nicht ersichtlich. Was mit den gemeldeten Informationen bei der Softwarefirma geschieht auch nicht.

Nun hat der einzelne PC sicher nicht unbedingt strategischen Wert für den Lizenzgeber. Aber die Möglichkeit, mit Hilfe eines Agents zu erfahren, was auf Großrechneranlagen an Software läuft, kann für eine Softwarefirma von entscheidender Bedeutung für ihre Unternehmenspolitik sein. Eine ähnliche Rückmeldungsfunktion existierte zum Beispiel bei Windows95 und wurde von dem Datenschutzbeauftragten der Bundesregierung als „Unding" bezeichnet. Ob nach erfolgter Rückmeldung nicht auch vielleicht noch eine „Hintertür" („backdoor") „offen" bleibt, ist zumindest denkbar …

Es bleibt daher nur anzuraten, das Thema Datensicherheit, auch als Individuum, ernst zu nehmen. Einen Anstoß hierzu gibt die HomePage des französischen Amtes für Datenschutz CNIL (www.cnil.fr). Auf diesem Site kann man spielerisch erforschen, wie gläsern man beim Bummeln im Inter-

net aussieht, wie durchsichtig unsere Verhaltensweisen sind. Auch gibt es dort interessante Tips zum „Sicheren Surfen".

Ein weiterer Site, der sich diesen Fragen widmet, wird von der Firma Anonymizer.com. angeboten. Zu erreichen ist er über *www.anonymizer.com*
Er bietet dem ahnungslosen Internauten, der sich noch unbeobachtet wähnt, ein sehr genaues Röntgenbild über sein elektronisches Wesen und seine Herkunft (vgl. nebenstehenden Kasten).

Anonymizer.com erlaubt dem Internauten, anonym zu surfen und sich auch sonst vor den inquisitorischen Fragen besuchter Websites zu schützen.

Verknüpft man die Informationen, die allein Anonymizer schon feststellen konnte zusammen mit denen, die von Cookies gesammelt werden und schließlich denen, die der Internaut selbst preisgibt, entsteht ein Profil eines Internet-Surfers, eines Konsumenten, eines Marketing-Targets… Unternehmen, wie DoubleClick, einer der größten Vermarkter von Internet-Sites und Ersteller von Werbe-Bannern, haben eine außerordentliche Expertise bei der Verknüpfung von derartigen Informationen entwickelt – was dem Unternehmen kürzlich Probleme mit der Justiz einbrachte. Denn Profile von Internet-Surfern sind wertvoll, sehr wertvoll. Für Handelsunternehmen, Vermarktungsstrategen, Geheimdienste.

Etwas Sci-fi zum Schluss

Die Zukunft aber liegt, angesichts dieser noch relativ harmlos wirkenden Beispiele, woanders.

Das Unternehmen IrisScan vermarktet Soft- und Hardware, die es erlaubt, einen Menschen biometrisch, d.h. auf Grund seiner biologischen Spezifizitäten zu erfassen, u.a. anhand der Form, Farbe und Zeichnung seiner Iris. 100000 Iris-Patterns in der Sekunde kann ein derartiges Programm vergleichen. Diese Entwicklung basiert auf der wissenschaftlichen Erkenntnis, dass die Iris bei jedem Menschen, sogar bei eineiigen Zwillingen, verschieden ist.

Space Imaging ist ein Anbieter von Satellitenphotos, welche bis zu einer Auflösung von 1 Meter in der Lagen ist zu gehen. Space Imaging obliegt einer strikten Privacy Policy – allerdings ist die Policy hinsichtlich der photographierten Objekte weniger offensichtlich – wann ist das Photo die Reproduktion einer mir gehörenden Sache? Was ist mit den Rechten auf Privatsphäre? In „Enemy of the State" wird Personenüberwachung anhand eines Satelliten dargestellt. Hollywood-Phantasie oder Wirklichkeit?

Professor Kevin Warwick, aus dem Fachbereich Kybernetik der Universität Reading in England, hatte sich während 9 Tagen einen Chip einpflanzen lassen, der es ihm erlaubte, mit dem Universitätsgebäude, in welchem sich sein Laboratorium befindet, zu kommunizieren. Anwendungen, wie automatische Türöffnung, sind dabei noch harmlos. Sensoren können aber zu jeder Zeit angeben, wo sich der Chip, und demnach auch der Mensch der ihn trägt,, befindet. Eine mögliche Anwendung ist der Strafvollzug – ein Chip ist kleiner und diskreter, als der zum Beispiel in Amerika gebräuchliche Armreif im Rahmen des offenen Vollzuges. Die Möglichkeiten des Missbrauchs sind ebenso diskret, aber unbegrenzt…. Die viel subtilere Gefahr, die von derartigen Systemen ausgeht, ist die, dass die Schnittstelle zwischen Mensch und Maschine aufgehoben wird. Man wird unwillkürlich an Fritz Lang's „Metropolis" erinnert.

Die Entschlüsselung des menschlichen Gen-Codes, wie sie vor ein paar Tagen angekündigt wurde, ist neuer Hoffnungsträger für alle genetisch bedingten Krankheiten, wirft aber genau so die Frage nach der Auswertung erhaltener genetischer „Fingerabdrücke" auf.

In Island wurde diese Frage in Form eines Gesetzes durch das Parlament gelöst, ausgehend von dem Projekt eines Unternehmens mit dem Namen deCODE Genetics. Das Projekt von deCODE basiert auf der Tatsache, dass die isländische Bevölkerung ethnisch fast isoliert ist, es dementsprechend

Über den Autor, der mit Hilfe eines Proxy-Servers surft und sämtliche Cookies systematisch ablehnt, wußte Anonymizer.com auf einen Mausklick hin das folgende zu berichten:

- die IP Adresse des Servers des Autors
- der Name des Computers des Autors
- der von dem System von Anonymizer.com gesetzte Cookie sowie das Vorhandensein von älteren Cookies
- der Link, von dem aus der Autor auf den Site anonymizer.com kam
- der Browsertyp und das "operating system" des Computers des Autors
- die Auflösung des Computerbildschirms
- die Frage, ob JAVAScript, VBScript oder JAVA installiert sind bzw. laufen
- Informationen zum JAVAScript Monitor
- die Anzahl der Webseiten, die der Autor auf seinem Weg zu Anonymizer.com besuchte
- Zeit-, Datumsanzeige und -format des Computers des Autors
- die Route, von dem Anonymizer.com-Server zum Ursprungsserver des Autors
- die Frage, ob der server die e-mail Adresse des Autors mitteilt
- die Informationen, die der Webbrowser des Autors an den Site von Anonymizer mitteilt
- die Identität des Nutzers, der den Domainnamen des Servers des Autors registriert hat, sowie sämtliche Details zur Registrierung
- die Konfiguration des Domains des Autors
- der Besitzer des Computernetzwerks, von dem der Autor ausging….

Man hat das Gefühl, als begegne man einem sehr guten alten Freund, der viel über einen weiß, über dessen Verschwiegenheit man sich aber nicht ganz sicher sein kann…

kaum Einflüsse von außen, besonders rassischer Natur, gibt und die Genealogie der Isländer in etwa vollständig vorliegt. Dementsprechend könnte eine Erstellung der detaillierten genetischen Datenbank sämtlicher Isländer die Grundlage für die Erforschung genetisch bedingter Krankheiten bieten – eine ganze Nation als Laboratorium. Als conditio sine qua non zu einer erfolgreichen Durchführung des Projektes aber muss deCODE Zugang zu den Krankenakten der erfassten Personen haben. Dieser bevorzugte Zugang wurde deCODE durch Gesetz gewährt, verbunden mit einer Exklusivität der Vermarktung der Forschungsergebnisse für 12 Jahre. deCODE hat parallel einen Vertrag mit dem Schweizer Pharmakonzern Hoffmann-LaRoche über die Erforschung von 12 Pathologien (Wert: 200 Millionen US-Dollar) abgeschlossen. Der Zugang Dritter zu den medizinischen Daten kann nur nach Zustimmung von deCODE erfolgen. Jeder Isländer kann, durch Abgabe einer Erklärung, verhindern, dass seine Akte an deCODE weitergegeben wird – es bedarf also eines expliziten Opt-out – welches den internationalen Empfehlungen in dem Bereich nicht entspricht. Bioethik-Experten und Datenschützer aus Island und dem europäischen Ausland haben diese Initiative stark kritisiert, da sie unter den Gesichtspunkten des Datenschutzes und der Bioethik mit fest etablierten Prinzipien bricht. Nach wachsender Kritik an dem Projekt von deCODE in der Schweiz (wegen des Vertrages mit Hoffman-LaRoche) und in Island, sinkt die soziale Akzeptanz des Projektes in diesem Land. Roche ist vorerst auf Distanz zu dem Projekt gegangen.

In den USA besteht eines der Projekte der National Academy of Justice, ein dem Justizministerium angegliedertes Rechercheinstitut, darin, eine komplette Datenbank der genetischen Fingerabdrücke der Personen zu erstellen, die in den Computern der US-amerikanischen Justiz gespeichert sind. Beifutter für PROMIS.

In Belgien könnte zum Beispiel die Chip-Karte der Sozialversicherung, die jeder bei sich trägt, von heute auf morgen zum Taschenformat des Großen Bruders werden, denn schon heute ist die Sozialversicherungsnummer identisch mit der nationalen Einwohnerregistrierungs- und der Steuernummer. Es würde ausreichen, eine Verbindung zwischen den einzelnen Institutionen, die der Sozialversicherung angeschlossen sind (ca. 2000) und den anderen staatlichen Datenbanken herzustellen und entsprechend auszuwerten.

Die Wahrheit liegt zwischen 0 und 1 oder „Der Nationalstaat als Mottenkugel"

"Ich rechne damit, dass, wie bei einer Mottenkugel, die vom festen in den gasförmigen Zustand übergeht, die Nationalstaaten sich einfach in Luft auflösen und das Zwischenstadium der unangenehmen, schmierigen Masse einfach überspringen werden. Am Ende beherrscht ein weltweiter Cyberstaat die politische Sphäre. Keine Frage: die Rolle des Einzelstaates verändert sich dramatisch und der Nationalismus wird in Zukunft so beliebt sein wie die Pocken." Dies meint Nicholas Negroponte, Begründer und Direktor von Media Lab, des Instituts zur Erforschung zukünftiger Formen der menschlichen Kommunikation am Massachussets Institue of Technology und Mitbegründer der Computerzeitschrift „Wired".

Auch wenn Negroponte diese Mottenkugelperspektive als realistisch und sogar als „erfrischend" ansieht, wird die Wahrheit doch wohl eher irgendwo zwischen 0 und 1 liegen – in der binären Welt – zwischen einzelstaatlichem Übergriff auf die Restfreiheit innerhalb und außerhalb des Internet und ultraliberalem „Laisser-aller". Und obwohl uns heute oft Server näher sind als Staatsgrenzen, sie die geographischen, geometrischen, politischen, rechtlichen, räumlichen und zeitlichen Umrisse der uns bekannten Welt aufheben, wird man wohl kaum verhindern können, dass einzelstaatliche Initiativen versuchen werden, in vermeintlich rechtsfreie Räume vorzudringen, unter dem Vorwand, das was dort passiere könne, man doch nicht geschehen lassen. Zu diesem „löblichen" Zweck werden alle Mittel recht sein, um den Bürger, egal wie mündig er auch sein möge, vor sich selbst und vor anderen zu schützen. Außer vor dem Staat – denn vor dem ist offenbar kein Schutz mehr nötig. Andererseits sind die wirtschaftlichen Interessen an einem begrenzten Schutz der Privatsphäre derart stark, dies um so mehr im Rahmen der allgemeinen Globalisierung, dass die Absichten (national-)staatlicher Regulierung jedesmal auf starke Gegenwehr von Seiten der Wirtschaft treffen.

Der Schutz des Privaten beginnt aber zuerst im Verantwortungsbereich eines jeden, der, selbst mit einem alten Vehikel, die Datenautobahn befährt. Es geht hier nicht um Utopia, sondern darum zu verhindern, dass der Negroponte'sche Cyberstaat sich der Datensicherung des Einzelnen annimmt. Die Mottenkugelstaaten brauchen mündige Bürger und funktionierende Kontrollmechanismen. Sonst wird auch in diesem Bereich die Aussage Edgar Faures wahr werden: „Voilà l'immobilisme qui avance et personne ne sait comment l'arrêter!"

Jean-Philippe Boever
Luxemburg, Juni/Juli 2000

Der Autor ist Jurist und arbeitet für ein international tätiges Medienunternehmen mit Sitz in Luxemburg.