HANSER

Die Überwachungsmafia

Pär Ström

Das gute Geschäft mit unseren Daten

ISBN 3-446-22980-9

Leseprobe

Weitere Informationen oder Bestellungen unter
http://www.hanser.de/3-446-22980-9 sowie im Buchhandel

Einleitung: Digitale „Fingerabdrücke“ und Überwachungsstaat

Wir vertrauen auf Gott – alle anderen überwachen wir.

Redewendung innerhalb der NSA
(National Security Agency) in den USA

Der ärmste Mensch darf in seiner Hütte der gesamten Staatsgewalt trotzen. Sein Haus mag baufällig sein, das Dach mag klappern, der Wind hindurchpfeifen, Sturm und Regen mögen eindringen – der König von England jedoch darf nicht eindringen; seine gesamten Streitkräfte dürfen es nicht wagen, über die Schwelle der zerfallenen Behausung zu treten.

William Pitt, englischer Parlamentsabgeordneter (1763)

Die Erkenntnis kam fast wie ein Schock.
Das Ganze begann damit, dass Robert Rivera auf einer kleinen Pfütze verschütteten Jogurts ausrutschte, als er in einem Laden der Vons-Supermarktkette einkaufte. Unglücklicherweise wurde beim Fall die Kniescheibe zertrümmert. Trotz einer Operation war Robert seitdem unfähig, eine normale Arbeit auszuüben.
Als er den Supermarkt auf Schadenersatz verklagte, erhielt er vom Rechtsanwalt der Vons-Supermarktkette eine unangenehme Mitteilung. Ihm wurde klar gemacht, dass „wir in unserer Datenbank genaue Informationen darüber besitzen, welche Waren Sie gekauft haben, und bei der Menge Alkohol, die Sie eingekauft haben, lag es wohl nicht am Jogurt, dass Sie das Gleichgewicht verloren. Wenn Sie den Prozess weiterverfolgen, werden die Geschworenen

durch diesen Hinweis einen denkbar schlechten Eindruck von Ihnen erhalten. Wir raten Ihnen daher von einem Prozess ab.“

O weh! Als Robert die elektronische Kundenkarte des Supermarktes erwarb, hätte er sich nicht träumen lassen, dass das Unternehmen einmal die über seine Einkäufe gespeicherten Informationen zu einem solchen Zweck verwenden könnte. Er muss sich gedemütigt, frustriert und machtlos gefühlt haben. Der Vorfall weist auf die Risiken hin, die sich aus dem immer umfassenderen Einsammeln und Speichern persönlicher Informationen als Folge der digitalen Revolution ergeben. Diese Entwicklung ist nicht neu, sie hat sich jedoch in den letzten Jahren erheblich beschleunigt.

Während meiner Kindheit gab es überall in den Städten öffentliche Telefonzellen. Man steckte eine Münze in den Schlitz und konnte telefonieren – und zwar völlig anonym und ohne Spuren zu hinterlassen. Heute benutzen die Menschen meist ihr Handy. Das bedeutet, dass Informationen darüber vorliegen, wann und wo eine Person eine bestimmte Telefonnummer gewählt hat. Die Informationen können jahrelang gespeichert werden – z. B. wurde bekannt, dass die irischen Telekomfirmen Eircell und Digifone die Verbindungsdaten sechs Jahre lang gespeichert hatten. In der Tat kann niemand mit Sicherheit sagen, ob diese Informationen überhaupt jemals gelöscht werden.

Der Leser wird jetzt vielleicht einwenden: „Wird da nicht der Teufel an die Wand gemalt? Die Möglichkeit, dass sich wirklich einmal jemand an diese Informationen heranmacht, ist doch höchst unwahrscheinlich – eine rein hypothetische Möglichkeit!“ Dazu ist zu sagen, dass die Möglichkeit durchaus äußerst real ist. Und das Ausgraben solcher Informationen ist ebenfalls keine bloße Möglichkeit mehr – es findet bereits statt.

Nach den Terroranschlägen vom 11. September 2001 in den USA hat sich das Gleichgewicht zwischen staatlicher

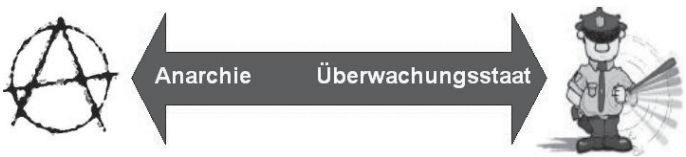
Kontrolle und Schutz der Privatsphäre erheblich verschoben. Ein weiterer Schub zur Störung dieses Gleichgewichts erfolgte nach den Attentaten in Madrid vom 11. März 2004. Eine Welle neuartiger staatlicher Vorgehensweisen und Gesetzesvorlagen geht seitdem um die Welt. So haben Polizei und andere staatliche Organe wesentlich erweiterte Befugnisse erhalten, um auf persönliche Daten zuzugreifen. In den USA war man nahe daran, ein riesiges Kontrollsystem einzuführen, das zuerst Total Information Awareness (TIA – totale Informationskenntnis) genannt, dann in Terrorism Information Awareness (Terror-Informationskenntnis) umgetauft wurde. TIA war als ein System geplant, das die digitalen Fingerabdrücke unschuldiger Bürger in Tausenden von öffentlichen und privaten Datenbanken überwachen sollte, um Verdächtige vorbeugend aufzuspüren. Ein weiteres amerikanisches Kontrollsystem (Secure Flight) soll der „Profilerstellung“ von Flugpassagieren dienen und wird bereits angewandt. Die Europäische Union hegt Pläne, Daten über den Telefon-, Internet- und E-Mail-Verkehr sämtlicher EU-Bürger zu speichern.

Tatsache ist, dass eine neue Überwachungs- und Schnüffelmentalität, wie sie sich in Systemen wie TIA, CAPPS II und Secure Flight darstellt, in breiter Front und in unterschiedlichen Zusammenhängen auf uns zukommt. In Anleitungen der Polizei und anderer Behörden kann man lesen, wie sich digitale Fingerabdrücke am besten nutzen lassen. In seinem 2003 erschienenen Leitfaden *Investigative Data Mining for Security and Criminal Detection* schreibt Jesús Mena z. B. Folgendes:

> In der modernen Gesellschaft ist es praktisch unmöglich, bei digitalen Transaktionen keine Spuren in kommerziellen und privaten Datenbanken sowie in Netzwerken zu hinterlassen. Der Prozess der „Datengewinnung“ wird normalerweise angewandt, um Angaben über das Verhalten von Verbrauchern zu erhalten, jedoch kann die gleiche

> Technologie auch dazu genutzt werden, kriminelle Personen aus Sicherheitsgründen aufzuspüren und zu identifizieren. Die Daten gibt es überall, und damit erhält man Anhaltspunkte, Delikte vorauszusehen, ihnen vorzubeugen und sie zu lösen sowie die allgemeine Sicherheit zu erhöhen und illegale Handlungen zu entdecken (und vor ihnen abzuschrecken). Im 21. Jahrhundert müssen Polizei und Untersuchungsrichter anfangen, sich der neuen Technologie für die Erkennung von Verbrechensmustern zu bedienen, um unsere Gesellschaft und Zivilisation zu schützen.

In diesem Zusammenhang ist der Begriff „digitale Fingerabdrücke“ von entscheidender Bedeutung. Im Zuge der Digitalisierung unseres Alltags hinterlassen wir eine immer weiter anschwellende Menge solcher Fingerabdrücke, und zwar nicht nur dann, wenn wir telefonieren oder mit einer Kreditkarte bezahlen. Der Besuch einer Website im Internet, das Abheben von Geld am Automaten, das Ausleihen eines Buches in der Bibliothek, die Zahlung der Busreise mittels sog. Smartcard, das Passieren der Werkstore des Arbeitsplatzes, das Senden von E-Mails, das Entrichten der Autobahngebühr usw. – solche Vorgänge hinterlassen persönlich identifizierbare, digitale Fingerabdrücke. Und immer neue digitale Anwendungsbereiche kommen hinzu. Es gibt bereits „intelligente“ Einkaufswagen, die Informationen darü-



Jede Gesellschaft muss sich entscheiden, wo auf der Skala zwischen Anarchie und Überwachungsstaat sie stehen will. Die meisten Demokratien haben sich bisher für eine Position irgendwo in der Mitte entschieden. Doch derzeit bewegt sich die westliche Welt immer weiter in Richtung Überwachungsstaat. Wie weit wollen wir noch gehen, bevor wir dieser Tendenz Einhalt gebieten? (Quelle: Pär Ström)

ber sammeln, an welchen Regalen des Ladens der Kunde stehen bleibt, um sich eine Ware näher anzuschauen. Mittels interaktiven, digitalen Fernsehens, das ebenfalls bald Wirklichkeit wird, kann unser Verhalten vor dem Fernseher registriert werden. Und so weiter…

Im Teil A dieses Buches werde ich einige der vorhandenen wie auch geplanten Überwachungstechnologien näher beschreiben.

Zweckentfremdung eröffnet neue Möglichkeiten

Die digitalen Fingerabdrücke sind für den Laien kaum wahrnehmbar, und die meisten Menschen denken nicht an sie – vorläufig jedenfalls nicht. Das Beunruhigende dabei ist, dass digitale Fingerabdrücke die Tendenz haben, haften zu bleiben. Und dann tauchen plötzlich immer neue Vorschläge auf, wie man diese „nützlichen“ und „wichtigen“ Daten verwerten könnte. Häufig stellt gerade diese sekundäre Verwertung von Informationen (ein Ergebnis ihrer multiplen Anwendungsmöglichkeit) die größte Bedrohung für Privatsphäre und Persönlichkeitsrechte dar.

Als Robert Rivera in unserem Beispiel oben erfahren musste, dass seine getätigten Einkäufe zu seinem Nachteil verwendet wurden, war dies eins von vielen Beispielen für die multiple Anwendung elektronischer Daten. Auch die Polizei hat erkannt, dass ihr Alltag durch das Überwachen elektronischer Fingerabdrücke einfacher wird. Die neuen Mautstationen am Rande der Londoner Innenstadt, die jedes Fahrzeug (und ihren Besitzer) identifizieren können, werden bereits für die Verbrechensbekämpfung eingesetzt. Die Werbefachleute von Unternehmen haben ebenfalls erkannt, dass digitale Fingerabdrücke wertvollen Aufschluss über unser Konsumverhalten liefern und somit für die Verkaufsförderung einer Ware genutzt werden können. Einzelne Staaten haben erkannt, dass Spionage via elektroni-

sche Kanäle sowohl in industrieller wie politischer Hinsicht wirkungsvoll die Position des eigenen Landes stärkt. Es wäre also naiv zu glauben, dass eine Nutzung elektronischer Daten nicht stattfindet.

Wir sind in der Tat dabei, eine Spitzel- und „Schnüffel“-Gesellschaft zu schaffen – eine Gesellschaft, in der gigantische Datenmengen angehäuft werden, die Informationen über die intimsten Angelegenheiten des Einzelnen sowie die wichtigsten Geheimnisse von Unternehmen und Staaten liefern.

Sind diese Daten erst einmal vorhanden, üben sie natürlich auf Schnüffler einen unwiderstehlichen Lockreiz aus so wie die Marmelade auf Fliegen: Amateurschnüffler und professionelle Schnüffler, staatlich angestellte und private Schnüffler, legale und illegale Schnüffler, einheimische und ausländische Schnüffler, alle werden sie angelockt. Und wir stehen erst am Anfang dieser Entwicklung.

Diejenigen, die sich mit dem Gedanken an die wohlmeinenden Absichten des Staates beruhigen, stört dies vielleicht nicht besonders, da ja angeblich „die Informationen hinreichend gesichert und vor Missbrauch geschützt“ sind.

Dies entpuppt sich jedoch als Wunschdenken. Trotz aller schönen Reden über die Sicherheit der Informationstechnologie lecken die angeblich so sicheren elektronischen Schutzwälle wie ein Sieb. „Sie wissen ja gar nicht, wie es wirklich aussieht“, ist ein häufiger Kommentar gewiefter Experten in Sachen IT-Sicherheit. Es gibt zahllose Beispiele dafür, wie „sicher verschlossene“ Informationen durch technische Mängel, menschliche Fehler oder vorsätzlichen Betrug nach außen dringen konnten. Und jedes Mal wird erneut versichert, dass man jetzt Maßnahmen getroffen habe, die eine Wiederholung ausschließen.

Ein Computer ist extrem anfällig für das Auskundschaften. Das gilt jedoch nicht nur für Computer. Von sämtlichen produzierten Mikroprozessoren (dem „Gehirn“ eines Computers) landen nur zwei bis drei Prozent in Computern; der

Rest wird in alle möglichen Apparate gesteckt, von Autos bis zu Spielsachen. Sobald sich ein Mikroprozessor in einer Ware befindet, steigen die Möglichkeiten zur Registrierung von Fingerabdrücken des Anwenders ganz erheblich (denn der Mikroprozessor ist ja selbst schon ein kleiner Computer). Das führt zu einer ständig wachsenden Menge an Fingerabdrücken.

Die Entwicklung wird durch den neuesten Trend im IT-Bereich – die Telematik – noch beschleunigt: Verschiedene mechanische Geräte (keine Computer) können ans Internet angeschlossen und via Internet ferngesteuert werden. Diese sog. M2M-Kommunikation (Maschine zu Maschine) ermöglicht z. B. einem Autofahrer, seine Position, Geschwindigkeit und ähnliche Angaben im Minutentakt via Mobilfunknetz einzugeben und an andere weiterzuleiten. In der chinesischen Provinz Tianjin sind private Geschäftsinhaber bereits gesetzlich dazu angehalten, ihre Ladenkassen via M2M-Technik anzuschließen und die Tageseinnahmen unverzüglich in die Computer der Steuerbehörde einzugeben.

Die heutige Technik in Kombination mit vorhandenen gesellschaftlichen Trends führt offensichtlich zu einer fragwürdigen Erscheinung, die im Englischen „Automated Law Enforcement“ genannt wird, also ungefähr „automatischer Gesetzesvollzug“. Ein weiterer Begriff in diesem Zusammenhang ist „Ubiquitous Law Enforcement“, d. h. „allgegenwärtiger Gesetzesvollzug“. Dahinter steht folgender Gedanke: Warum sollen Gerichte und Polizeikräfte teure Zeit darauf verschwenden, Bagatelldelikte zu ahnden, wenn das Ganze automatisiert werden kann? Sogar die Strafzumessung erfolgt via Internet mittels spezieller Software (engl. Punishware, d. h. Strafzumessungssoftware). Hier ein Beispiel aus dem Verkehrsbereich, das zeigt, wie es funktionieren könnte:

> Sämtliche Fahrzeuge eines Landes werden via Satellitennavigation (GPS) und Telematik ans Internet angeschlos-

sen. Damit können alle Fahrzeugbewegungen im gesamten Land überwacht werden. Die Software eines zentralen Computers schreibt automatisch die Bußgeldbescheide aus, wenn ein Fahrer die vorgeschriebene Geschwindigkeit überschreitet, in eine Einbahnstraße falsch einbiegt, im Halteverbot parkt usw. Wenn der Computer entdeckt, dass die Kfz-Steuer des betreffenden Fahrzeugs nicht bezahlt ist, schaltet die Software einfach die Zündung aus. Das Gleiche erfolgt, wenn ein Auto als gestohlen gemeldet wird. Alles sehr praktisch und effizient. Wer könnte etwas dagegen einwenden? Niemand will doch eine Gesetzesübertretung verteidigen, und außerdem spart man dabei das Geld der Steuerzahler!

Wem dies als höchst unwahrscheinliches Horrorszenario erscheint, ist sich nicht bewusst, dass die englische Regierung genau dies bereits ins Auge fasst, nämlich mit einem obligatorischen „Spionagechip“, der in jedes Fahrzeug eingebaut werden soll. Die entsprechenden Pläne wurden im August 2003 bekannt.

Die sog. „automatische Strafzumessung“ wird vielerorts als eine gute Alternative diskutiert und bereits im Ansatz verwirklicht. So wurde bekannt, dass eine amerikanische Leihwagenfirma mit der Telematiküberwachung ihres Wagenparks begonnen hat: Bei Geschwindigkeitsübertretung folgt ein Bußgeld (das also privat verhängt wird, nicht durch die Polizei). Und in der Gegend von Paris findet ein Versuch statt, bei dem Fahrzeugen mit Satellitennavigation der Sprit via Fernsteuerung gesperrt wird, wenn sie die Geschwindigkeit überschreiten.

Digitale Fingerabdrücke geben Aufschluss über die Persönlichkeit

Das Aufspüren digitaler Fingerabdrücke, die eine Person im Alltag hinterlässt, kann dazu dienen, sich ein äußerst genaues Bild über diese Person zu verschaffen. Digitale Spuren

können ganz persönliche Verhältnisse an den Tag bringen – z. B. den Freundeskreis, Gewohnheiten und Interessen, Krankheiten, finanzielle Verhältnisse, eventuelle Eheprobleme oder die Absicht, den Arbeitsplatz zu wechseln usw.

Um herauszufinden, welche Schlussfolgerungen aus der Offenlegung rein geografischer digitaler Fingerabdrücke gezogen werden können, fand 2002 ein Experiment an der Technischen Hochschule in Stockholm statt:

> Da die Studenten der untersuchten Fakultät sämtlich an schnurlos angeschlossenen Laptops arbeiteten, konnte das System erkennen, in welchem Raum sich die Studenten mit ihrem Computer befanden. Eine Untersuchung der sog. Logdatei lieferte Aufschlüsse darüber, welcher Student sich an welchem Ort zu welchem Zeitpunkt befand. Folgende Erkenntnisse konnten aus diesen Angaben gewonnen werden:
>
> - welche Freunde ein bestimmter Student hatte;
> - wo Liebesbeziehungen zwischen Studenten und Studentinnen vermutet werden konnten;
> - was für ein Persönlichkeitstyp ein Student war – einige saßen fast immer allein (Einzelgängertyp), während andere fast immer gemeinsam zusammenhockten (geselliger Typ);
> - wann ein bestimmter Lehrer eine „langweilige“ Vorlesung hielt (zu diesem Zeitpunkt stieg die Anzahl der Studenten, die sich ins Netzwerk einloggten, nämlich sprunghaft an).

Nebenbei kann zu diesem Thema erwähnt werden, dass ähnliche Informationen wie die obigen bereits allgemein gespeichert werden – nämlich über unsere Mobiltelefone, die ständig unseren Standort angeben, und zwar auch dann, wenn wir nicht telefonieren (d. h. wenn das Handy eingeschaltet ist). Eine übersichtliche Strukturierung dieser Daten wäre eine die Privatsphäre äußerst verletzende Informationsquelle. Dem Böswilligen bieten sich hier automatisch

große Möglichkeiten, anderen Personen zu schaden. Man könnte darauf das lateinische Motto „scientia est potentia“ – „Wissen ist Macht“ – anwenden. Die digitalen Fingerabdrücke ermöglichen es somit, sich Informationsvorteile, und d.h. Machtvorteile, zu verschaffen. Dies kann u.a. zu wesentlichen wirtschaftlichen Vorteilen führen.

Gespeicherte digitale Informationen können also missbraucht werden. Die Gefahr droht aus dreierlei Richtung, oder anders ausgedrückt, es gibt drei Hauptkategorien von „Schnüfflern“: einzelne Individuen, bestimmte Unternehmen sowie der Staat. Bisher gehören die beiden letztgenannten Gruppen – Unternehmen und Staat – zu den eifrigsten Schnüfflern, während Individuen häufig als sog. Hacker auftreten, um eventuell Schaden zu verursachen.

Entsprechend gibt es auch drei Hauptgruppen von Opfern, nämlich Individuen, Firmen oder andere Staaten. Mittels digitaler Schnüffelei und Überwachung können Individuen einer Verletzung ihrer Privatsphäre sowie Betrugs- oder Erpressungsversuchen ausgesetzt sein; Firmen können ausspioniert und einzelne Staaten können ebenfalls aus wirtschaftlichen bzw. politischen Gründen infiltriert werden.

Das Diagramm auf Seite 11 zeigt die verschiedenen Arten der Bedrohung. Nehmen wir einmal die Bedrohung der individuellen Persönlichkeitsrechte. Wie der Versuch an der Technischen Hochschule in Stockholm zeigt, reicht bereits eine einzige Informationsquelle aus, um ein recht genaues Bild der Gewohnheiten eines Menschen zu erstellen. Weit schlimmer wird es, wenn die Informationen verschiedener Quellen zusammengestellt werden. Dies ist der Fall, wenn Datenbanken und Register von Behörden miteinander abgeglichen werden.

Ein solcher Datenabgleich geht leichter vonstatten, wenn man über einen sog. „eindeutigen Identifikator“ verfügt, der mit einem Hauptschlüssel verglichen werden kann. Die „Personennummer“, die jeder Mensch in Schweden bei

Wer bedroht? \ Wer ist bedroht?	Individuum	Unternehmen	Staat
Staat	■ Staatl. Überwachung ■ Erfassung politisch Andersdenkender	■ Technische Spionage ■ Wirtschaftsspionage	■ Technische, wirtschaftliche und militärische Spionage ■ Sabotage ■ Angriffe auf die IT
Unternehmen	■ Erfassung von Kunden ■ Überwachung der Mitarbeiter ■ Überprüfung von Anstellungsbewerbern	■ Technische Spionage ■ Wirtschaftsspionage ■ Sabotage	■ Politische Spionage
Individuum	■ Schädigung ■ Erpressung ■ Rufmord, böser Leumund (z. B. bei Scheidung)	■ Schädigung ■ Erpressung ■ Diebstahl von Informationen ■ IT-Terrorismus	■ Schädigung ■ Erpressung ■ Diebstahl von Informationen ■ IT-Terrorismus

der Geburt oder bei der Zuwanderung ins Land zugewiesen erhält, ist ein solcher eindeutiger Identifikator. Deshalb ist die Personennummer in vielen Ländern äußerst umstritten bzw. verboten.

Ganz allgemein gesprochen, ist jede Überwachung umso leichter durchzuführen, je einheitlicher die vorhandenen IT-Lösungen sind, wobei ein gemeinsamer IT-Standard flächendeckend für unterschiedliche Bereiche gilt. Das vereinfacht natürlich auch die Arbeit von Behörden und Firmen, welche die Datenbanken betreiben. Umgekehrt gilt auch: Je mehr aufgesplittert die Technik ist (d. h. auf zahlreiche und verschiedene Teilsysteme, Standards und Plattformen verteilt), desto größer ist auch der Schutz des einzelnen Anwenders, da die Überwachung schwieriger wird. Die Kehrseite

technischer Vielfalt sind natürlich höhere Kosten und schwierigere Kompatibilität der IT-Systeme.

Leider besteht somit ein deutlicher Gegensatz zwischen Schutz der Privatsphäre und Anwenderfreundlichkeit – will man das eine haben, kommt häufig das andere zu kurz. Jedoch ist es mittels gut durchdachter IT-Lösungen durchaus möglich, diesen Gegensatz aufzuheben.

Ein Abgleich der Daten verschiedener Datenbanken ist heute vielfach mit gesetzlichen Einschränkungen verbunden. Leider ist es nicht selbstverständlich, dass dies auch so bleiben wird. Aus Anlass der Anschläge vom 11. September wird heute vermehrt Gewicht auf Sicherheitsfaktoren anstelle des Schutzes der Privatsphäre gelegt. Zahlreiche polizeiliche Eingriffe, die früher undenkbar waren, werden jetzt ohne größeren Widerstand als Mittel der Terroristenjagd akzeptiert. (Gleichzeitig wurde die Definition des Begriffs „Terrorismus“ erweitert – heute fallen darunter bereits bestimmte Arten des „Hackens“ und politischer Demonstrationen.)

Eine zentrale Rolle spielt dabei der Datenabgleich. Dies gilt nicht zuletzt für die USA, wo er zu einem Hauptmittel von Polizei und Sicherheitsdiensten geworden ist, um der Bevölkerung die versprochene Sicherheit zu geben. Präsident Bush schuf eine besondere Datenabgleichbehörde unter dem Namen Information Awareness Office (Amt für Informationskenntnis). Das gigantische Datenabgleichprojekt dieser Behörde läuft unter dem Namen Terrorism Information Awareness.

Neue Gesetze zur staatlichen Überwachung

Die Terroranschläge vom 11. September führten, wie gesagt, zu einer grundsätzlichen Sinneswandlung von Regierungen und Behörden, was sich weltweit in neuen Gesetzestexten niederschlug. Hier folgen einige Beispiele an

Gesetzen und Vorschriften, die den Behörden stärkere Überwachungsmöglichkeiten bieten – und zwar um den Preis einer Schwächung des Schutzes der Privatsphäre und der Persönlichkeitsrechte:

- 2005 greift in Deutschland die Version 4.1 der Technischen Richtlinie der Telekommunikationsüberwachung (TRTKÜ). Ab dann kann man damit rechnen, dass die Überwachung analoger und digitaler Telekommunikation deutlich zunimmt. Experten gehen davon aus, dass die Kosten fürs Abhören künftig 15 Prozent der Telekommunikationspreise ausmachen werden.
- Die Europäische Union plant den Erlass von Vorschriften für Telekomfirmen und Internetanbieter, die Verkehrsdaten sämtlicher Teilnehmer zu speichern, z. B. wen wir anrufen oder an wen wir unsere E-Mail richten, welche Websites wir besuchen und wo wir uns geografisch bei Handytelefonaten befinden.
- In Dänemark erhielt die Polizei 2001 die gesetzliche Möglichkeit, bei schweren Delikten die Logdateien von Telekomfirmen zu sichten, um z. B. die Verbindungsdaten von Handybesitzern im Umkreis des Tatorts kontrollieren zu können. Das neue dänische Antiterrorismusgesetz von 2002 gibt der Polizei das Recht, sog. Spyware in den Computern verdächtiger Personen zu installieren.
- In Großbritannien erließ man ein stark kritisiertes Gesetz (den Regulation of Investigatory Powers Act = RIP), das Behörden das Recht einräumt, von Privatanwendern die Auslieferung von Schlüsseln für Chiffrierprogramme zu erzwingen. Somit darf es vor dem Staat keine Geheimnisse mehr geben. Auf eine Weigerung steht Gefängnis – ebenso wie es verboten ist, überhaupt jemand davon zu unterrichten, dass man gezwungen wurde, den Chiffrierschlüssel auszuliefern! Ein ähnliches Gesetz ist in Spanien geplant.

- In den USA gibt der neue Patriot Act den Behörden wesentlich mehr Befugnisse gegenüber dem Individuum. Beispielsweise erhalten die Behörden das Recht, von Bibliotheken und Buchhändlern eine Liste derjenigen Bücher zu verlangen, die eine bestimmte Person dort geliehen bzw. gekauft hat, und zwar ohne Vorliegen eines formellen Durchsuchungsbefehls oder konkreten Verdachtsmoments. Das betreffende Personal darf – unter Androhung einer Gefängnisstrafe – nicht darüber berichten, dass überhaupt eine solche Aufforderung gestellt wurde. Das Gesetz gibt amerikanischen Gerichten unter bestimmten Umständen auch die Befugnis, Personen außerhalb der USA juristisch zu verfolgen.
- Im amerikanischen Bundesstaat Michigan erließ man Gesetze, die es praktisch unmöglich machen, E-Mail-Sendungen zu chiffrieren, und in den Bundesstaaten Massachusetts und Texas sind ähnliche Gesetze in Vorbereitung.
- In Ungarn muss man sich ausweisen, wenn man Waren für mehr als zwei Millionen Forint (ca. 7500 Euro) kauft, und die Angaben zum Kauf werden zehn Jahre lang gespeichert. Auch bei Käufen zu geringeren Summen kann der Verkäufer verlangen, dass man sich ausweist, wenn er aus irgendeinem Grunde Verdacht schöpft.

Auch an unseren Arbeitsplätzen beginnt das Schnüffeln um sich zu greifen. Es begann mit Softwareprogrammen, die automatisch kontrollieren, welche Websites der Angestellte während der Arbeitszeit besucht und welche E-Mail-Nachrichten er verschickt. Doch damit ist es nicht mehr getan. Die neuesten Programme untersuchen das gesamte Verhalten von Mitarbeitern an ihren Computern, erstellen anhand dieser Angaben ein Profil des Mitarbeiters und melden der Firmenleitung, ob sich der betreffende Mitarbeiter künftig illoyal verhalten könnte.

Leider gibt es in dieser Hinsicht noch weit größere poten-

zielle Gefahren für Individuen, Firmen und Nationen. Zu unserer Beschreibung der „Schnüffelgesellschaft“ gehört auch Echelon. Echelon ist der Name eines geheimen Systems zur Überwachung elektronischer Kommunikation. Das System verfügt über eine globale Reichweite und überwacht u.a. Telefongepräche, Faxmeldungen, E-Mail, Fernschreiben, Videokonferenzen, Surfen im Internet usw. Echelon wird seit mehreren Jahrzehnten von den englischsprachigen Ländern USA, Großbritannien, Kanada, Australien und Neuseeland (unter Federführung der USA) betrieben. Das System ist nach den Aussagen ehemaliger Mitarbeiter außerordentlich effizient. Die Kommunikation kann u.a. nach Suchwörtern durchforstet werden, es funktioniert also ungefähr wie eine Suchmaschine im Internet. Auch die Möglichkeit zur Spracherkennung soll vorhanden sein.

Echelon scheint gegenwärtig hauptsächlich für die Industriespionage gegen europäische Unternehmen verwendet zu werden. Die bloße Existenz des Systems wurde lange Zeit hartnäckig geleugnet. Heute besteht jedoch kein Zweifel mehr an dessen Existenz, was u.a. durch eine Echelon-Resolution des Europaparlaments bestätigt wurde.

Eine weitere Gefährdung vertraulicher Informationen geht von sog. Spionageprogrammen (Spyware) aus, die sich heimlich in fremden Computern einnisten, um dann die gesuchten Daten zu stehlen. Dies ist ein relativ neues Phänomen, das voraussichtlich immer häufiger auftauchen wird. Die Spywareprogramme können auf unterschiedliche Weise mittels Fernsteuerung und via Internet in fremden Computern installiert werden, und da sie eine völlige Kontrolle des fremden Computers ermöglichen, sind sie für alle denkbaren Operationen verwendbar. Zum Beispiel können sie Dateien, die bestimmte Stichwörter enthalten, von der Festplatte kopieren und an die Spionagezentrale senden. Sie können auch vertrauliche Angaben aufschnappen, die der nichts ahnende Anwender in die Tastatur eingibt (z.B. das Passwort oder die Kreditkartennummer). Sie können sogar

über die Computerlautsprecher abhören, was im Raum gesprochen wird, sei es zu Hause oder am Arbeitsplatz.

Damit nicht genug: Gefahr droht auch von Microsoft. Die führende Softwarefirma bereitet nämlich eine grundlegend neue Computerarchitektur vor, die uns eine „sichere Datenhandhabung“ schenken soll. Das Konzept trägt den Arbeitsnamen „Palladium“ und basiert auf einer Art Fernsteuerung unserer Computer von Microsoft aus (oder dessen Vertreter). Falls dies Wirklichkeit wird, erhält Microsoft oder dessen Vertreter einen umfassenden Einblick in den Inhalt unserer Festplatten.

Nach dem 11. September 2001 ist auch das Interesse an Biometrie stark gestiegen, einer Technologie, die Personen durch digitalisierte körperliche Merkmale identifiziert. Diese Merkmale werden in einer Datenbank gespeichert. Dabei kann es sich um die biometrische Erkennung und digitale Speicherung von Fingerabdrücken, der Iris im Auge oder der Gesichtsform handeln. In den USA und in Großbritannien sind die Behörden stark an der Kameraüberwachung öffentlicher Plätze interessiert; diese Überwachung wird dann z. B. an eine Datenbank für digitale Gesichtserkennung angeschlossen. Vielerorts sind solche Systeme bereits in Betrieb. Das bedeutet in der Folge, dass ich noch nicht einmal mit meinem Hund ausgehen kann, ohne meine Schritte registrieren zu lassen – in der Tat eine elektronische Spurensuche par excellence!

Eine spezielle Form der Biometrie besteht aus Mikrochips, die in Menschen eingepflanzt werden. Auch damit hat man bereits in den USA und in Großbritannien begonnen. Kevin Warwick ist Professor an der englischen Reading-Universität und betreibt das sog. „Chippen“ von Menschen. Er ist auch dafür, dass alle Menschen bereits von der Geburt an „gechippt“ werden sollten, weil sich dann – so meint er – die Sicherheit erhöht.

Verräterische Backdoors (digitale Hintertüren)

Nicht nur die Privatsphäre des Einzelnen, sondern ebenso die Geheimnisse von Unternehmen und Staaten sind in der sich formierenden „Schnüffelgesellschaft“ bedroht. Industriespionage mittels digitaler Hilfsmittel dürfte bereits relativ weit verbreitet sein, jedoch auf Grund der technischen Entwicklung noch sprunghaft ansteigen. Das Gleiche gilt für die staatlich betriebene Spionage.

Jetzt kommen neue Methoden wirtschaftlicher und militärischer Spionage auf uns zu, z. B. durch die Anwendung von sog. Spyware. Auch gibt es hartnäckige Gerüchte, dass es einigen mächtigen Nachrichtendiensten gelungen ist, sich digitale Backdoors (Hintertüren) in normalen Softwareprogrammen zu verschaffen. Eine solche „Hintertür“ kann in diesem Fall bedeuten, dass das betreffende Programm bewusst mit einer Schwachstelle versehen wurde, so dass die Sicherheitsfunktionen leichter umgangen werden können – und zwar nur von demjenigen, der um diesen Schwachpunkt des Programms weiß! Dies kann sogar so weit gehen, dass das Programm – selbst wenn es von einem großen und angesehenen Softwareunternehmen stammt – eine geheime Doppelfunktion als Spionageprogramm erfüllt!

Diese neuartige Schnüffelei ist vor allem durch den fortschreitenden Übergang zur elektronischen Datenverarbeitung und die Koordinierung von Computern und Informationssystemen möglich geworden. Dies liegt an zwei wichtigen Eigenschaften digitaler Informationen: Sie haben „Flügel“, und sie bleiben „haften“. Dass Informationen Flügel bekommen, bedeutet, dass sie die wundersame Fähigkeit besitzen, sich schnell und unmerklich von einer Stelle zur anderen zu bewegen. Gleichzeitig pflegen sie sich dabei zu vermehren. Und dass Informationen „haften“ bleiben oder „klebrig“ sind, bedeutet, dass sie schwierig zu entfernen sind, wenn sie erst einmal Eingang in verschiedene Systeme

gefunden haben. In vielen Fällen sind diese Eigenschaften von großem Nutzen für die Kommunikation, und auf ihnen basiert ja auch das phantastische Potenzial der Informationstechnologie. Sie haben jedoch auch, wie wir gesehen haben, ihre Schattenseite.

Computer gibt es schon recht lange, das Internet ist seit etwa zehn Jahren allgemein zugänglich. Und es verstreicht immer eine gewisse Zeit, bevor sämtliche Konsequenzen einer völlig neuen Technik deutlich werden. Darum müssen wir davon ausgehen, dass wir bisher nur den Gipfel des Eisbergs der neuen „Schnüffelgesellschaft“ erblickt haben. Das Problem wird noch dadurch erschwert, dass es global und international ist. Die binären Ziffern der EDV machen nicht vor Staatsgrenzen Halt. Deshalb gilt es, die Entwicklung in anderen Staaten aufmerksam zu verfolgen.

Als ein interessantes Zeichen der Zeit wurde im Frühjahr 2003 bekannt, dass das Justizministerium der USA sich von neun lateinamerikanischen Ländern die vollständigen Einwohnermeldekarteien, angereichert mit verschiedenen anderen Personenangaben, über illegale Zwischenhände verschafft hat.

Kann der Schutz der Privatsphäre gewahrt bleiben?

Die Ausbreitung der „Schnüffelgesellschaft“ sollte uns veranlassen, korrekte Schlussfolgerungen zu ziehen und danach zu handeln. Dies gilt für Individuen, Unternehmen und Nationen gleichermaßen. Die Schlussfolgerungen sind politischer bzw. philosophischer Natur. Vielleicht schlussfolgern wir, dass automatische Überwachung der Bevölkerung ausgezeichnet ist, da sie auf kosteneffiziente Weise die Kriminalität verringert. Es gibt viele Menschen, die so denken. Und vielleicht ziehen wir den Schluss, dass es ganz hervorragend wäre, wenn Supermärkte und andere Geschäfte den Kunden genau ausforschen, um ihm dafür einen

bequemeren und individuell angepassten Lebensstil zu bieten.

Die Befürworter einer solchen Meinung könnten sich als ihren Sprecher Scott McNealy wählen, Konzernchef des Serverproduzenten Sun Microsystems, der sich mit folgender Äußerung über die Bedrohung der Privatsphäre profiliert hat:

> Die Privatsphäre gibt es sowieso nicht mehr – damit muss man sich halt abfinden!

Ich persönlich sehe das etwas anders. Die Schlacht um die Persönlichkeitsrechte ist noch nicht verloren, und wir können immer noch die Entwicklung beeinflussen. Dabei sollten jedoch weit mehr als bisher auch ethische Fragen beachtet werden. Dies bedeutet keineswegs, technologiefeindlich zu handeln. Es ist eine Tatsache, dass Einzelne, Firmen und die gesamte Gesellschaft außerordentlichen Nutzen von der Informationstechnologie haben. Der Nutzen muss jedoch korrekt erfolgen. Wir können nicht weiterhin völlig unkritisch alles durchführen, was technisch möglich ist. Die Schaffung eines Verhaltenskodex für Informationstechnologie muss daher Priorität erlangen – bei Politikern und Behörden, bei Unternehmen, die sich IT anschaffen und verwenden, und nicht zuletzt bei der IT-Branche selbst. Eine Voraussetzung dafür ist, dass wir Normalverbraucher selbst beginnen, den Schutz unserer Privatsphäre an die erste Stelle zu setzen. Ein klarer Verhaltenskodex ist nötig – jetzt!

Wenn man Anarchie bzw. Polizeistaat als die beiden möglichen Extreme gesellschaftlicher Entwicklung setzt, dann kann man sagen, dass unsere westliche Gesellschaft sich meist irgendwo in der Mitte zwischen diesen Extremen befunden hat. Nach den Terroranschlägen vom 11. September – und denen des 11. März 2004 in Madrid – bewegen wir uns jedoch plötzlich in Richtung Polizeistaat. Die Frage ist: Wollen wir wirklich in diese Richtung gehen? Und wenn ja – wie weit wollen wir dabei gehen?

Das vorliegende Buch besteht aus zwei Teilen. Im ersten Teil werden verschiedene Formen bereits vorhandener oder im Entstehen begriffener digitaler Fingerabdrücke und ihrer Überwachungsmöglichkeiten behandelt. Der zweite Teil handelt davon, was mit den gesammelten Informationen geschieht. Wir gehen dabei auf Nutzen und Triebkräfte, auf Folgen und Risiken beim Sammeln von Informationen ein.

Und falls Sie den Hinweis im Vorwort übersehen haben: Ein Sternchen (*) hinter dem Namen einer Firma oder Organisation bedeutet, dass deren Webanschrift in der Linkliste im Anhang des Buches aufgeführt ist.