



REDLINE | VERLAG

Gerald Reischl

Unter Kontrolle

Die fatalen Folgen der staatlichen
Überwachung für Wirtschaft und
Gesellschaft

89875-010-8

Gerald Reischl
Unter Kontrolle

REDLINE | VERLAG

Gerald Reischl

Unter Kontrolle

Die fatalen Folgen der staatlichen
Überwachung für Wirtschaft und Gesellschaft

REDLINE | VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Für Fragen und Anregungen:
reischl@redline-verlag.de

Nachdruck 2012

© 2002 by Redline Verlag, ein Imprint der Münchner Verlagsgruppe GmbH
Nymphenburger Straße 86
D-80636 München
Tel.: 089 651285-0
Fax: 089 652096

© 2002 by Wirtschaftsverlag Carl Ueberreuter, Frankfurt/Wien

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung des Verlages reproduziert oder unter Verwendung elektronischer Systeme gespeichert, verarbeitet, vervielfältigt oder verbreitet werden.

Umschlaggestaltung: INIT, Büro für Gestaltung, Bielefeld
Druck: Books on Demand GmbH, Norderstedt

ISBN Print 978-3-86881-435-4
ISBN E-Book (PDF) 978-3-86414-380-9

Weitere Informationen zum Verlag finden Sie unter

www.redline-verlag.de

Beachten Sie auch unsere weiteren Verlage unter
www.muenchner-verlagsgruppe.de

_Inhalt

__Vorwort **__009**

__Einleitung **__013**

Die Filmwelt wird real _013 / Die (Überwachungs)-Welt hat sich geändert _014 / Misstrauen und Angst dominieren unser Leben _015 / Datenjagd kann nach hinten los gehen _016 / Ein Status-Quo-Bericht über die Überwacher _017 / Die Globalisierung der Überwachung _020 / Datenjagd und Informationshunger _021 / US-Überwachung für die ganze Welt _021

__Die Allmacht der Behörden **__023**

Die tägliche Rasterfahndung in unserem Leben _023 / Überwachung statt Freiheit: Der Kontroll-Katalog _24 / Prävention als Schlagwort der Stunde _026 / Die Fratze des Verbrechens _031 / Mit der Stimme suchen _033 / Jeder hinterlässt ein Profil _34 / Gerastert, gefiltert und aussortiert _038 / Nicht unschuldig und nicht gleich _043 / Negative und positive, kleine und große Rasterfahndung _045 / Die Macht des Wissens _046 / Die Suche nach dem verlorenen Schatz _048 / Den Genen auf der Spur _049 / Das DNA-Phantombild _050 / Die europäische DNA-Datenbank _055 / Wir hinterlassen überall unsere Spuren _056 / Ein Horrorszenario? _060

__Wie das Leben vermessen wird **__061**

Der Körper als Ausweis _061 / Die gefährliche Zentraldatei _065 / Fälschungssicher? _067 / Video-Über-

_005 Unter Kontrolle

wachung _070 / Die Biometrie-Touristen 073 / Die Einreise nach Schengen _075 / Männlein oder Weiblein _075 / Verhaltens-Kontrolle _077 / Die Gedankenleser kommen 079 / Die Fingerprint-Datei _081 / Mit Phantombildern auf Verbrecherjagd _082 / Wenn die Software Verwandtschaften aufdeckt _083 / Schau mir in die Augen, Kleines – Die Iris als Pass _085 / Der Hintergrund der Hysterie _087 / Die Flughafen-Kontrolle _088 / Der Background-Check _091 / Das globale Informationssystem _095

__Die Finanzwelt steht unter Kontrolle **__097**

Die zentrale Fahndungsdatei _101 / Geldwäsche im WAP-Gang oder beim Online-Roulette _108 / Die Banken im Untergrund – Underground- und Hawala-Banking _111 / Die globale schwarze Liste _113 / Waschbär jagt Geldwäscher _117 / Die USA-EU-Connection _120 / Zollfahndung _126 / Die Schmuggel-jäger der EU _127

__Die Kontrolle des Netzes **__131**

Der Fleischfresser _131 / Computerviren als Spione _134 / Kekse, die nicht schmecken _137 / Das europäische Echelon – Der ETSI-Standard _138 / Röntgenuntersuchung für Handys _141 / Telefonüberwachung _144 / Videoüberwachung _148

__Die kontrollierte Welt der Kommunikation **__151**

Handys als Peilsender und Bewegungsmelder _151 / Lokalisieren und Bewegungsprofile vom Gericht erlaubt _152 / Die Ortung übernimmt der Computer

_155 / Tempokontrolle vom All aus _ 161/ Mit der elektronischen Maut zum gläsernen Menschen _159 / Abhängig von Amerika _161 / Abhängig und kontrolliert von den USA _162 / USA drohen Europa 163 / Das Spionagenetzwerk Echelon _165 / Die Opfer der Spionage _168 / Problem Wirtschaftsspionage _169 / Krypto-Handy und Lauscher im Ausland _170 / Verschlüsselt und abgesichert _173 / Die Abhörfunktion im Computer _175 / Das abhörsichere Netz _176 / Der Blauzahn zeigt Zähne _179 / Die Identität auf vier Quadratmillimetern _180

__Literaturliste **__185**

__Links **__187**

**__Liste der Datenbanken,
in denen der Autor enthalten ist** **__197**



—Vorwort

„A society that will trade
a little liberty for a little order
will lose both, and deserve neither.“

Thomas Jefferson

Der Schock des 11. September traf die internationalen Datenschützer besonders tief. Auf der internen Mailingliste der Global Internet Liberty Campaign (GILC), dem Dachverband von über fünfzig Bürgerrechts- und Datenschutzorganisationen, riss der Verkehr ebenso plötzlich ab, wie die Anschläge gekommen waren.

US Mitglieder wie die American Civil Liberties Union (200.000 Mitglieder, gegründet von Martin Luther King) verschwanden für Tage aus der weltweiten virtuellen Öffentlichkeit. Wenn jemand seine Stimme auf dieser oder einer anderen wichtigen Liste erhob, hatten die Postings immer denselben Tenor. Bin Laden habe auf die US-Regierung gezielt und voll das Netz getroffen, nun werde hier das bisschen Freiheit drastisch eingeschränkt. Die Realität schien diese von Südafrika bis zur Ukraine, von Japan bis in die USA geäußerten Befürchtungen, nun sei der Super-GAU des weltweiten Datenschutzes passiert, eindrucksvoll zu bestätigen.

Nach einer Schrecksekunde, während der den Geheimdiensten unter anderem von US-Vizepräsident Richard Cheney und CIA-Kenner Tom Clancy vorgeworfen wurde, die klassische Geheimdienst-Arbeit zugun-

sten eines Overkills an Überwachungstechnologie vernachlässigt zu haben, kamen der Patriot Act und andere Notstandsgesetze heraus. FBI und Geheimdienste aller Art, die nicht nur in Angelegenheiten der nationalen Sicherheit eng zusammenarbeiten, drangen gedeckt durch die neuen Gesetze in die Kommunikationszentren der Informationsgesellschaft vor. Um die 1000 Personen wurden aufgrund der großteils in staatlichen und privaten Datenbanken, bei Internet Providern und Telefoniebetreibern gesammelten Daten verhaftet und ohne Gerichtsverhandlung interniert.

Das ging sehr schnell, denn das Setup dafür hatte man bereits seit Jahren vorbereitet. Mit dem 1994 verabschiedeten Communications Assistance Law Enforcement Act wurden US-Telekoms und Mobilfunk-Betreiber gezwungen, ihre Netze Polizei und Diensten technisch zu öffnen. Seitdem werden immer mehr Schnittstellen eingebaut, an denen die Behörden mit Standleitungen andocken können, um Datensätze abzusaugen. Bei Internet-Providern erschien das FBI mit „Carnivore“ genannten Datenfressern, die ähnlichen Zwecken dienen. Erhoben wurden unterschiedlichste Datensätze – alle Internet-Kontakte bestimmter IP-Adressen, wer wann in bestimmte Foren im Internet gepostet hatte, alle Verbindungsdaten bestimmter Nummern aus den letzten drei Monaten, der gesamte Verkehr in diversen Funkzellen der New Yorker Handynetze in den Tagen vor dem Anschlag und Ähnliches mehr.

Dann wurde dieser Datenwust zusammen mit den Inhalten von unterschiedlichen Datenbanken einem Data Mining zugeführt: sie wurden abgeglichen. Nach Kriterien, die man wohl nicht so schnell erfahren wird, blieben die danach Internierten im Raster hängen. Neben der überwiegenden Mehrzahl völlig Unschuldiger wird man vielleicht einige kleine Fische gefangen haben, vom Ergreifen eines echten Terroristen ist wenigstens bis jetzt nichts bekannt.

Auch wenn die Ereignisse vom 11. September 2001 einmalig waren, Parallelen dazu, wie es danach weiterging und wer vor allem nicht gefasst wurde, gibt es allemal.

Während der letzten beiden Jahrzehnte des vorigen Jahrhunderts wurde als Reaktion gegen den Terror der IRA ein Verbund aus mittler-

weile 30.000 Überwachungskameras in Großbritannien aufgebaut. Die Beamten, die das so genannte CCTV-System betreiben, beantworten die Frage, ob denn auch IRA-Terroristen durch CCTV erwischt worden seien mit „leider nein“. Als Vorteile des mit enormem Finanz- und Personalaufwand betriebenen Systems, das alle wichtigen Orte in britischen Städten erfasst, führen sie an, man habe durch CCTV vermehrt Parksünder und Auto-Einbrecher überführt. Zusätzlicher Benefit des Systems: die Leute würden sich seit Einführung der Kameras in der Öffentlichkeit besser benehmen.

Was passiert, wenn ein terroristisches Regime sich existierender Datenbanken über die Bevölkerung bedienen kann, hat Thomas Mathiesen, Professor für Rechtssoziologie an der Universität Oslo, in einem Essay für *Telepolis* skizziert.

Während des Zweiten Weltkriegs hatten deutsche Besatzungstruppen verschiedene Bevölkerungsregister benutzt. Als nützlich erwies sich das Register des norwegischen Radioamtes. Gleich nach der Invasion 1940 ordneten die deutschen Behörden nach einem „Datenbankabgleich“ an, alle Radios, die Juden in der Hauptstadt gehörten, zu beschlagnahmen. Weil das norwegische Büro für Volkszählung die Juden seit 1866 als eigene Bevölkerungsgruppe registriert hatte, stand den Nazis auch eine Todesliste zur Verfügung. Das Ergebnis war, dass über 50 Prozent der 1400 Juden in Norwegen 1942 ermordet waren, in Dänemark, wo den Nazis keine ähnlichen Register zur Verfügung standen, starb „nur“ ein Prozent der 5600.

Wer das berühmt gewordene Zitat von Thomas Jefferson – jenes US-Präsidenten, der das Land in die Unabhängigkeit geführt hatte – genauer ansieht, dem wird auffallen, dass es ein an sich unbedeutendes Wort gleich zweimal enthält. Es sind die kleinen Freiheiten hier und dort, die täglich aufgegeben werden, weil wir allesamt mehr oder weniger rechtschaffen sind und ohnehin kaum etwas oder gar nichts zu verbergen haben.

Wer diese verloren gehenden Kleinteile der Freiheit – sich unbeobachtet bewegen zu können, sich nicht ohne triftigen Grund für irgendetwas rechtfertigen zu müssen, und seine Ruhe zu haben, wenn einem der

Sinn danach steht – zusammenzählt, könnte bald eine beunruhigende Summe vor sich haben. Wenn nämlich unter der Rechnung Null, die furchtbarste aller Zahlen, steht.

Wer dieses Netz, das die unzähligen, individuellen Informationen, die für sich allein an ihrem jeweiligen Speicherort durchwegs harmlos sind, verknüpfen kann, wird dem Individuum als solchem die Luft abdrehen. Wie dieser Prozess vor sich geht, das beschreibt Gerald Reischls neues Buch.

Erich Moechel

Leitender Redakteur von FutureZone.orf.at und Editor des Newsletters q/depesche www.quintessenz.org, online seit 1990



Einleitung

Die Filmwelt wird real

Robert Clayton Dean ist ein erfolgreicher Rechtsanwalt, glücklich verheiratet und Vater eines Sohnes. Er hat keine Geldsorgen, lebt im Luxus, all seine Wünsche kann er sich erfüllen. Ein perfektes Leben, bis zu jenem Tag, an dem er für seine Frau ein Geschenk kaufen will und in einem Dessousgeschäft einen Bekannten trifft, der kurz darauf von einem Auto überfahren wird. Ab diesem Zeitpunkt ist nichts, wie es vorher war, schlittert sein Leben in ein totales Chaos. Er verliert seinen Job, seine Frau verdächtigt ihn der Untreue, seine Kreditkarten und Konten werden gesperrt. Der Mann mit Einfluss, Macht und Geld hat die Kontrolle über sein Leben verloren, die plötzlich ein anderer zu haben scheint. Warum?

Der alte Bekannte im Dessousgeschäft hatte ihm ohne sein Wissen eine Diskette in die Tasche gesteckt, auf der der Mord an einem Senator zu sehen war, der sich geweigert hatte, ein neues Gesetz zu verabschieden, das die lückenlose technische Überwachung von Verdächtigen gestattet. Robert ist nun selbst Opfer dieser Technologien. Egal, was er tut, wohin er geht – er ist unter totaler Kontrolle. Er ist der „Staatsfeind Nummer 1“, der im gleichnamigen Hollywood-Streifen verwandt und ständig abgehört wird, der per Satellit oder per Mobilfunk geortet und

über den in wenigen Sekunden jede Information aus einer Megadatenbank abgerufen werden kann.

Mitarbeiter von Geheimdiensten können ob dieses Szenarios, in dem Will Smith und Gene Hackman die Hauptrollen spielen, nur schmunzeln. Filmfans finden den Thriller in manchen Bereichen übertrieben, man habe zu tief in die Trickkiste gegriffen, einiges sei technisch nicht machbar. Für die „anderen“, die Kriminalisten und Geheimdienst-Mitarbeiter, ist der Film nicht nur „sehr realistisch“, sie behaupten sogar, die Realität übertreffe den Film: „Glauben Sie wirklich, dass wir das alles nicht können? Wir können noch viel mehr. Und die Technik kann auch noch viel mehr, als im Film angedeutet ist“, versicherte ein Vertreter dieser Gruppe dem Autor.

Der Film „Der Staatsfeind Nr. 1“ ist, so paradox und absurd dies klingt, ein Pflichtfilm für diverse Agenten aus aller Herren Länder, der Streifen gehört zur Ausbildung von Mitarbeitern des deutschen Bundesnachrichten-Dienst (BND) oder des österreichischen Heeres-Nachrichten-Amtes (HNA), des britischen MI5, der amerikanische National Security Agency (NSA) sowieso, wobei letztere den Filmemachern in Hollywood Tipps gegeben hat. Gene Hackman, einer der Hauptdarsteller, hat sich von NSA-Agenten beraten lassen, wie er bestimmte Dinge richtig darstellen könne und was realistisch sei. Es gibt keinen Spion auf dieser Welt, der diesen Film nicht kennt.

__Die (Überwachungs)-Welt hat sich geändert

Seit dem 11. September 2001, dem Tag der Terroranschläge auf das World Trade Center in New York und das Pentagon in Washington, ist die Welt nicht so, wie sie vorher war. Nach den Attentaten ist die Diskussion um Sicherheitsvorkehrungen, die solche Attentate verhindern hätten können, neu entbrannt. Dabei werden immer wieder Methoden genannt, die einen schweren Angriff auf die Privatsphäre der Bürger darstellen und die jenen gleichen, die im Film „Der Staatsfeind Nr. 1“ verwendet werden.

Unter dem Deckmantel der Terrorbekämpfung wollen einige Staaten nun Überwachungssysteme installieren, die einer Totalkontrolle gleich kommen und mit der auch unschuldige, unbescholtene Bürger überwacht und kontrolliert werden.

Die für die Installation solcher Systeme zuständigen Behörden (Innenministerien, Justizministerien, Verkehrsministerien, EU-Kommission) nutzen dabei die derzeitige Angst und Stimmung in der Bevölkerung – der Terrorismus müsse mit allen Mitteln bekämpft werden – um ihre ohnehin schon lange geplanten Überwachungssysteme quer durch alle Bereiche zu realisieren. Der Staat wird – und das hat nichts mit Panikmache, Verfolgungswahn oder Hysterie zu tun – zum Big Brother, der uns Bürger ständig unter Kontrolle haben will. Er arbeitet an der völligen Transparenz – von Bürgern und Unternehmern, oder, anders formuliert: von Gesellschaft und Wirtschaft.

Die staatliche Kontrolle hat in den vergangenen Jahren kräftig zugenommen. Ein schleichender Prozess. Lauschangriff und Rasterfahndung sind heute ebenso „state of the art“ wie Videoüberwachung, DNA-Analyse, das Durchleuchten von Geldflüssen oder die Kontrolle der Kommunikation.

__ Misstrauen und Angst dominieren unser Leben

Dieses Buch zeigt auf, warum es Regierungen und bestimmte Behörden bei der Realisierung ihrer Überwachungspläne so leicht haben. Unter anderem deshalb, weil es derzeit nur wenig Widerstand in der Bevölkerung gibt. Zitate wie „Mir egal, was die von mir wissen“ oder „Ich habe nichts zu verbergen“ sind Indizien dafür, dass man die staatliche Überwachung nicht fürchtet. Die persönliche Sicherheit ist Menschen wichtiger geworden als die persönliche Freiheit. Man lässt sich offenbar lieber in die Privatsphäre schauen als sich unsicher zu fühlen. Und einen weiteren Grund gibt es: Wer sich heute gegen Überwachungsmethoden ausspricht, macht sich offiziell verdächtig, weil er

damit ja indirekt auf der Seite des Bösen, auf der Seite von Verbrechern oder Terroristen steht.

Denn die Angst vor Terrorismus und Verbrechen ist größer geworden, weil sich seit dem 11. September 2001 die Wahrscheinlichkeit, selbst Opfer von Gewalttaten zu werden – zumindest in den Köpfen der Menschen – vergrößert hat. Weil in den Medien seit dem 11. September 2001 immer wieder propagiert wird, dass das Böse in Form von „Schläfern“ – Terroristen, die erst aktiv werden, wenn sie der Ruf des Terroristenchefs ereilt – perfekt getarnt mitten in unserer Welt lebt. Mit dieser bewusst geschürten Angst wurde gleichzeitig auch das Misstrauen anderen Menschen gegenüber größer. Hinter jeder schönen Fassade kann sich das Verbrechen verstecken.

Doch die totale Kontrolle könnte nach hinten losgehen und genau das Gegenteil dessen bewirken, was damit erzielt werden soll, nämlich der „Sicherheit“ des Staates und der Bürger zu dienen. Das hat der 11. September 2001 gezeigt. Es gibt wohl keine Nation, die mehr Polizeiorganisationen und Geheimdienste hat, als die Vereinigten Staaten, ob es sich nun um das FBI, die CIA oder NSA handelt. Mitarbeiter sind über die gesamte Welt verstreut, sammeln mit den neuesten Technologien, vom Mobilfunk über Satellitentechnik bis zu komplizierten Analyse-Programmen und Software, Informationen über Informationen. Überwacht werden „brave“ europäische Wirtschaftskonzerne, um amerikanischen Unternehmen Aufträge zuzuschancen, ebenso wie terroristische Organisationen – ob sie nun Al Kaida, PKK, HAMAS oder Hizbullah heißen. Die Bulletins, die dabei zusammen getragen werden, sind detailliert und umfassend. In vielen Bereichen so informativ, dass man europäischen Unternehmen Aufträge wegschnappen konnte. In manchen Bereichen aber auch so umfassend, dass sich aus der Fülle der Daten gute und hinweisgebende Informationen nicht mehr herausfiltern ließen.

__Datenjagd kann nach hinten los gehen

Die USA sind Opfer der eigenen Datenjagd geworden. Vor lauter Wald sieht man die Bäume nicht mehr. Anders formuliert: Vor lauter Daten bleiben die wahren, guten Informationen verborgen. Quantität ist nicht Qualität. Quantitative Überwachung sämtlicher Bürger ist qualitativ nicht gut genug, um Verbrechen verhindern oder gar voraus sagen zu können.

Was nützt es, wenn mit modernsten Technologien Telefongespräche abgehört, Persönlichkeits-, Bewegungs- oder Nutzerprofile gemacht, der E-Mail-Verkehr und die Internet-Nutzung mitgeloggt werden? Wer soll diese Daten auswerten, wer soll die Nadel im Heuhaufen suchen?

Pro Tag werden 10 Milliarden SMS verschickt, 4 Milliarden E-Mails mit Millionen von Attachments, von der Datei über die Grafik bis zum Bild, versendet. Es werden 3 Milliarden Telefonate von Festnetzapparaten und einer Milliarde Handys aus geführt sowie einige Milliarden Internet-Seiten aufgerufen. Man müsste mit einem Heer von Tausenden, nein Hunderttausenden Mitarbeitern diese Daten sortieren, durchleuchten und analysieren. Nicht nur nach menschlichem Ermessen unmöglich, sondern technisch auch mit den besten Software-Programmen nicht machbar.

Dem deutschen BND ist es im Zuge der Fernmeldeaufklärung erlaubt, den gesamten Telefonverkehr von und nach Deutschland zu überwachen, was beinahe zehn Millionen Gespräche pro Tag sind. Hochkomplizierte Wortscanner überprüfen dabei die Gespräche und schalten sich automatisch ein, wenn bestimmte Reizworte fallen. Diese „Hit-Wörter“ stammen aus den Bereichen Drogen- und Waffenhandel, Menschenschmuggel und Terrorismus. Da man davon ausgehen kann, dass vor allem um den 11. September in vielen Telefonaten die Worte „Bin Laden“, „Al Kaida“, „Terror“, „George Bush“, „Attentat“ etc. verwendet worden sind und sich daher die Aufnahmemechanismen eingeschaltet haben, wird klar, dass es sich um eine Unmenge von Gesprächen gehandelt haben muss, die nie ausgewertet werden können. Die

Totalüberwachung des Telefonverkehrs ist eine Alibiaktion. Kein Scanner-Programm kann so gut sein, dass man aus zehn Millionen Telefonaten jenes bzw. jene herausfiltern kann, in denen tatsächlich gesuchte Verbrecher oder potentielle Attentäter gesprochen haben.

Die Entwickler der Überwachungssysteme geben dennoch nicht auf, versuchen mit anderen Tricks, etwa mit der Verknüpfung verschiedener Systeme und Technologien nicht nur die Trefferquote zu erhöhen, sondern auch Politiker von ihren Produkten zu überzeugen. Und das gelingt ihnen, wenn man die diversen Pläne und Absichten in Europa verfolgt. Doch die Folgen der totalen Überwachung sind fatal. Zwar werden sie jetzt von einem Großteil der Bevölkerung begrüßt – aber die Bürger werden später, wenn es bereits zu spät ist, erkennen, dass sie ihre Privatsphäre verloren haben, dass der Staat mehr weiß, als ihnen lieb und recht ist. Aus dem Bürger wird ein überwachtes und manipulierbares Individuum, das sich gegen den Staat und gegen die Überwachungs-Demokratie aufbäumen wird. Oder alles wird komplett anders kommen: Die Mehrzahl der Menschen verfällt in völlige Lethargie, Gleichgültigkeit, die nicht mehr umzudrehen ist. Die Privatsphäre ist für die Masse der Bürger nicht mehr wichtig und damit haben auch die persönliche Freiheit und die Freiheit im Allgemeinen ausgedient.

Wäre das Thema nicht so ernst, müsste man über diverse Kommentare und „Enthüllungen“, ja über die Naivität mancher Journalisten schmunzeln: Die Terroristen nutzen das Internet, nutzen Handys, Satellitentelefone und können die „avanciertesten Technologien“ ganz selbstverständlich bedienen. Ach wirklich? – fällt einem da nur ein. Ist es heute eine Sensation, ein Satelliten- oder Mobiltelefon zu besitzen? Eine Milliarde waren es weltweit Anfang 2002. Ist es heute etwas Außergewöhnliches, über einen Internet-Anschluss zu verfügen? E-Mails zu verschicken? Verschlüsselungstechniken zu beherrschen? Das sind Technologien der Gegenwart, unsere Technologien, mit denen wir leben.

__ Ein Status-Quo-Bericht über die Überwacher

Es geht in diesem Buch weder um Verschwörungstheorien, noch leidet der Autor unter Verfolgungswahn oder will Panikmache betreiben. *Unter Kontrolle* ist ein Status-Quo-Bericht. Dieses Buch handelt von der Globalisierung der Überwachung. Es geht darum, aufzuzeigen, dass die Kontrollsysteme nicht nur auf Staaten, Staatenbünde oder auf Kontinente konzentriert sind, sondern dass an globalisierten Systemen gearbeitet wird, die – so das Idealziel – auf Knopfdruck Informationen über jeden Menschen, über jedes Unternehmen auf dieser Welt liefern sollen. Systeme und Datenbanken, wie sie in den Kapiteln „Die Finanzwelt steht unter Kontrolle“, „Die Allmacht der Behörden“ und „Wie das Leben vermessen wird“ beschrieben werden, sind ein Schritt in diese Richtung. Datenbanken, ob sie nun World-Check, KARNAC oder DNA-Database heißen, zielen auf diese globale Kontrolle ab. Eine Suchanfrage in der Mega-Datenbank – und es wird ein Datensatz über uns oder unser Unternehmen ausgeworfen, der detaillierter ist, als wir es selbst für möglich halten. Es ist ein neuer Versuch, die globale Kontrolle einzuführen, wie sie die US-Geheimdienste im Auftrag der Regierung gemeinsam mit alliierten Nationen bereits seit einigen Jahrzehnten mit dem System „Echelon“ versuchen und teilweise auch erfolgreich praktiziert haben. Mit dem weltweiten Schnüffelsystem Echelon, das sämtliche Kommunikationssysteme abgehört hat, wurde etwa erfolgreich Industrie-Spionage betrieben.

In eine ähnliche Richtung geht künftig auch die Kontrolle der Telekommunikation. Die europäische Standardisierungsbehörde ETSI hat einen Überwachungsstandard verabschiedet, der es Behörden auf der ganzen Welt erlaubt, sich in jedes x-beliebige System, ob Handy-Netz oder Internet, einzuklinken und der Kommunikation zu lauschen. In Echtzeit, also ohne Zeitverzögerung.

Tatsache ist, dass man mit jedem Tag mehr über uns, unsere Familie, unsere Firma weiß, dass die Informationen und Datensammlungen bei Staat(en) immer umfangreicher werden. Wir hinterlassen Spuren, die mit