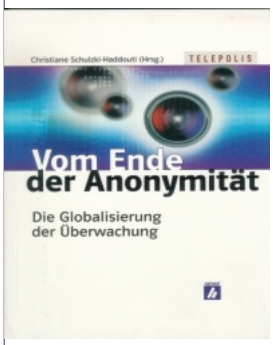
Vom Ende der Anonymität

Die Globalisierung der Überwachung

Christian Hofer



Christiane Schulzki-Haddouti: Vom Ende der Anonymität, 188 Seiten, Verlag Heinz Heise, 2000, ISBN 3-88229-185-0, Eur 14,83.-

Die Herausgeberin hat in diesem Buch mehrere profunde Kenner der Materie eingeladen, in den Themenbereichen staatliche Überwachung, Anonymität und Internet, Privatsphäre und Bürgerrechte die aktuelle Situation und geschichtliche Entwicklung darzustellen.

So berichtet Nicky Hager von seiner Aufsehen erregenden Aufklärungsarbeit, die die Beteilung Neuseelands am weltweiten Echelon-Netzwerk bewies. Wayne Madsen, ehemaliger US-Marineoffizier, beschreibt die Situation der Vereinigten Staaten im sogenannten *Cyberwar*, wobei die Rolle der Geheimdienste und deren problematisches Verhältnis zu den Bürgerrechten aufgezeigt wird. Von einem deutschen Experten für Geheimdienstaktivitäten wird die geschichtliche Entwicklung der Abhöraktivitäten des Bundesnachrichtendienstes bis zum heutigen Status detailliert beschrieben. Ein interessantes Detail daraus: Seit mehr als 20 Jahren betreibt der BND einen gegen Russland gerichteten Horchdienst mit einer Station auch auf chinesischem Staatsgebiet.

In Weiteren Beiträgen versuchen die Autoren zusätzlich zur präzisen Aufarbeitung der Themengebiete auch die vielen Begriffe in diesem Zusammenhang zu ordnen und zu erklären:

Echelon

So wird das System der Überwachung analoger Information während ihrer drahtlosen und unverschlüsselten Übertragung auf Richtfunkstrecken oder Satelliten bezeichnet. Dieses System wurde nach dem zweiten Weltkrieg entwickelt und die US-amerikanische *National Security Agency* (NSA) benutzt es mittlerweile auch dazu, um Unterseekabel und Radioübermittlungen sowie das Internet abzuhören. Zusätzlich zu denen der U.S.A. gehören Stationen zum System, die von Großbritannien, Kanada, Australien und Neuseeland unterhalten werden. Allerdings ist es mit diesem System nicht möglich, wie vielerorts behauptet, dass jede E-Mail und jedes Telefonat aufgezeichnet und verarbeitet wird.

Europol

Die Europäische Polizei- und Aufklärungsbehörde Europol in Den Haag arbeitet daran, solange sie noch nicht mit operativen Befugnissen ausgestattet ist, umfangreiches Informationsmaterial zu sammeln, auszutauschen und zu analysieren. Damit fungiert die europäische Polizeieinheit als Servicestelle für nationale Sicherheitsbehörden, vor allem hinsichtlich des international organisierten Verbrechens. Im Endausbau wird sie die Profile von über einer Million Menschen speichern und untereinander verknüpfen können.

Enfopol

Mit dem Begriff *Enforcement Police* wird ein System (und eine Arbeitsgruppe) bezeichnet, das Telefonanrufe, Faxe und den gesamten Internetverkehr überwachen soll. Laut Europäischer Übereinkunft soll Enfopol den Strafverfolgungsbehörden die Telekommunikationsüberwachung in Realzeit rund um die Uhr ermöglichen, wobei die Verkehrsdaten in Realzeit zur Verfügung gestellt werden. Die Veröffentlichung der bis dahin geheimen Dokumente zu Enfopol im Jahre 1998 durch Telepolis (Heise-Verlag), sorgte für einige Aufregung. Die Pläne fanden dann im Juni 1999 auf Grund massiver Proteste von Datenschützern und der IT-Industrie allerdings keine Mehrheit im EU-Ministerrat.

ETSI

Mehrere Arbeitsgruppen des *European Telecom Standards Institute* versuchen die, in den Dokumenten von Enfopol vorgegebenen Richtlinien, in konkrete technische Spezifikationen zum Anzapfen aller digitalen Netze (ISDN, TCP/IP, UMTS, usw.) einzuarbeiten. Dazu wird ein Meta-Standard (ES 201 671) laufend weiterentwickelt und an die neuen Entwicklungen in der Informationstechnologie angepasst.

Warum sprechen die Autoren nun vom "Ende der Anonymität" und welche Gefahren bergen die eben genannten Überwachungssysteme?

Das Echelon Netzwerk wird von den U.S.A. und ihren Verbündeten explizit auch dafür benutzt, diplomatische und kommerzielle Ziele abzuhören. Eine Untersuchung des EU-Parlamentes zu Echelon stellte fest, dass dieses System von den U.S.A. zur "Industriespionage im großen Stil" genutzt wird. Im Bericht wird daher allen Bürgern und Firmen der EU empfohlen, vor allem E-Mails grundsätzlich zu verschlüsseln.

An sich ist es einleuchtend, dass die Europäische Polizei gegen die internationalen Verbrechensnetzwerke die gemeinsame europäische Analyse der Bedrohungslage einsetzen will. In Zeiten "gewalttätiger Ausschreitungen" wünscht sich die Polizei nun aber die totale Überwachung, ohne richterliche Anordnung und auch mit Auswertung von Daten Unbeteiligter (!). Die Europol wird aber von keinem Parlament und auch von keinem Richter kontrolliert. Die Beamten können jegliche Daten über Personen speichern (z.B.: politische Ideen), auch dann, wenn diese vielleicht erst in Zukunft ein Verbrechen begehen könnten. Besonders problematisch ist sicher, dass der Datenaustausch auch mit Ländern wie Russland oder Kolumbien erlaubt werden soll.

Nicht nur, dass die Einführung des Enfopol Vorgängers über eine Abstimmung im Fischerei-Ausschuss(!) des europäischen Parlamentes als "Beschlossene Sache" bei niedrigster Abstimmungsbeteiligung durchgedrückt wurde, erzeugt Unbehagen. Auch weisen aktuelle Pflichtenhefte den weiteren Weg von Enfopol: Es seien alle Vorkehrungen zu treffen, "um die Identität der überwachenden Behörden zu schützen und so die Vertraulichkeit der Ermittlungen zu gewährleisten". Dies zielt direkt darauf ab, dass die Geheimdienste der Mitgliedsstaaten voll in den polizeilichen Abhörapparat eingebunden werden.

Die Digitalisierung der Kommunikation, noch dazu in einigen Fällen in verschlüsselter Form, führte zur engen Zusammenarbeit von Nachrichtendiensten, Regierungs- und Polizeibehörden und Firmenvertretern im ETSI Gremium. Denn nur durch die Installation von standardisierten Schnittstellen bei den Telekommunikationsbetreibern selbst, kann das Ziel von Enfopol durchgesetzt werden. Spät haben die betroffenen IT-Firmen bemerkt, dass die geplanten Überwachungsverordnungen durch notwendige Neuanschaffung an Hard- und Software und zusätzlicher Personalressourcen Unsummen kosten werden. Und ganz sicher ist damit zu rechnen, dass die Kunden der Mobilfunkfirmen und Internetprovider die Kosten für ihre eigene Überwachung bezahlen werden müssen.

Natürlich sollte jeder für sich entscheiden, wie weit ihm die eigene Anonymität wichtig ist und dementsprechende Maßnahmen ergreifen. Wenn allerdings diesbezügliche Informationen und Beschlüsse am Gesetzgeber vorbei im Geheimen bestehen, ergibt sich diese Entscheidungsfreiheit gar nicht. Die Forderung nach Ende der Anonymität würde bedeuten, wie im Buch sehr bildhaft dargestellt, dass "jeder permanent seinen Ausweis nicht nur mit sich tragen, um ihn auf Aufforderung herzuzeigen, sondern ihn auch gut sichtbar anbringen müsste."

Wollen Sie das wirklich?

Dem Heise Verlag ist es durch Beiträge von Autoren mit unterschiedlichem Zugang zur Thematik gelungen, eine aufschlussreiche Lektüre zusammenzustellen, für die Sie allerdings auch einiges Interesse für die Materie mitbringen und die datentechnischen Zusammenhänge kennen sollten, um von der Informationsfülle zu profitieren. Auf den Seiten von Telepolis (http://www.heise.de/tp/) und in der Futurezone (http://futurezone.orf.at/) können Sie die aktuelle Entwicklung in dieser Thematik weiterverfolgen.