



2003/28 Interview

<https://shop.jungle.world/artikel/2003/28/europa-wird-total-gerastert>

»Europa wird total gerastert«

Von **amon brandt**

Erich Möchel

Auf dem EU-Gipfel von Thessaloniki wurde beschlossen, dass biometrische Daten in die Pässe der EU-Bürger eingetragen werden.

Seit knapp zehn Jahren verfolgt das österreichische Online-Magazin Quintessenz (<http://quintessenz.org>) die fortschreitende Entwicklung der Überwachungstechnologien. Mit dem Administrator der Initiative, Erich Möchel, sprach Amon Brandt über die Zukunft der Kontrolle.

Der Aufbau umfassender Überwachung schreitet mit atemberaubendem Tempo voran. Wie ist der aktuelle Stand?

Wir können einen aktuellen Einstieg wagen. In diesen Minuten, in denen wir miteinander reden, wird ein Dokument im Internet auf zahlreichen Servern hin und her geschossen, das, wenn dieses Interview erscheint, von der US-Behörde für Heimatschutz schon längst offiziell veröffentlicht wurde. Es spezifiziert auf 40 Seiten, welche Informationen die Airlines der Behörde über ihre Passagiere zur Verfügung zu stellen haben. 40 Datenfelder pro Passagier sollen alles erfassen, was eine Airline über ihre Passagiere wissen kann: von der Größe des Gepäcks über die Kreditkartennummer und die E-Mail-Adresse bis zu den Essgewohnheiten.

Aber was hat eine US-Behörde mit der EU zu tun?

Man hat sich Datenfelder vorbehalten, die zum Beispiel für die Integration biometrischer Daten geeignet sind. Diese werden bald in EU-Pässen zu finden sein. Mit Sicherheit werden von der EU auch diese neuen Forderungen des US-Heimatschutzes eins zu eins übernommen.

Anhand dieser Daten lassen sich Personen mehr oder weniger im Voraus berechnen. Bei den angedrohten 15 Jahren Speichermöglichkeiten kann das nur eines bedeuten, und jeder, der jemals mit Data-Mining zu tun hatte, erkennt das sofort: Diese Massen an Daten dienen dazu, umfangreiche Bewegungsbilder von Personen und vor allem von Gruppen zu erstellen. Ich kann damit hervorragend rasterfahnden.

Es heißt, diese Datenhamsterei diene ausschließlich der Terrorbekämpfung.

Diese Daten eignen sich zum Beispiel auch perfekt zur Analyse von Vielfliegern. Vielflieger sind geschäftlich Reisende. Da diese Massen an Daten nun mal da sind, gibt es immer auch andere

Interessenten. Wenn es sich wie hier um geschlossene Systeme handelt, sind den Manipulationsmöglichkeiten keine Grenzen gesetzt.

Ist im Nachhinein betrachtet die Intensität dieser Überwachungsbestrebungen überraschend?

Nein, weil das gesamte Set-Up schon seit langem aufgebaut ist. Beispielsweise wurden die technischen Standards, wie man die G3-Handys zu überwachen hat – das ist die Handy-Generation, die jetzt erst auf den Markt kommt – bereits 1999 definiert. Es wurde vor der Jahrtausendwende bereits festgelegt, wie man all die Videobotschaften, MMS-Bilder, etc. so in Datenbanken unterbringt, dass man sie auch wieder findet.

Bereits seit 1995 wird die Überwachung Schritt für Schritt völlig standardisiert. Im Bereich der Telefonie via Internet wurde bereits genau definiert, über welche Schnittstellen die Telefongesellschaften den berechtigten Behörden ihre Daten zu liefern haben. Diese Schnittstellen werden momentan überall geschaffen.

Wie wird der Ausbau der Überwachung weitergehen?

Im Moment macht man gerade den Anlauf, auch für das Internet einen Standard einzuführen. Die Firma Cisco, Weltmarktführerin im Bereich Routing und Großlieferantin von US-Behörden, wird bei der Tagung der Internet Engineering Task Force Anfang Juli in Wien die Überwachung des Internets als Standard durchzusetzen versuchen. Cisco baut schon seit einiger Zeit Überwachungsschnittstellen in ihre Router ein, wie es im Bereich der Telefonie bereits üblich ist.

Die Wege zum großen Data-Warehouse, in dem die ganz großen Datenschätze gelagert werden, sind nicht mehr weit. Im Consumer-Bereich hat sich durchgesetzt, zwischen dem User und dem Netz eine Batterie von Rechnern zu schalten, so genannte »transparente Proxies«. Transparent heißt, dass der User davon nichts mitbekommt. Mittels dieser Proxies lassen sich wertvolle Interessenprofile der User erstellen.

Somit verbindet sich die Überwachung mit kommerziellen Interessen.

Für detaillierte User-Profile interessiert sich die Marketing-Abteilung. Die Daten steigern den Buchwert der Kunden enorm. Aber ursprünglich wurde Data-Mining für die Nachrichtendienste entwickelt. Das Problem ist nur, dass sie den technischen Aufwand für die Überwachung selbst nicht aufbringen können. Genau das ist die strukturelle Verbindung zwischen dem großen Bruder und den kleinen Brüdern: Die Massen an Daten wurden von den kleinen Brüdern gesammelt. Daher wird der nächste Schritt sein, gesetzliche Rahmenbedingungen zu schaffen, um an diese Daten heranzukommen.

Der große Datenfresser braucht Futter, sonst kommt sein Verdauungssystem durcheinander. Immer wenn es Kapazitäten gibt, wollen sie genutzt werden. Wenn man diese Entwicklungen zulässt, kann man sich sicher sein, dass der Staat früher oder später auf sein Recht pochen wird, das, was man aufgebaut hat, auch uneingeschränkt zu nutzen, um eine mögliche Gefahr abzuwehren. Man kann das Wissen ja nicht einfach brach liegen lassen.

Für Cops und Nachrichtendienste gilt die Faustregel: Was möglich ist, wird gemacht! Und es wird gemacht, wenn es einen plausiblen Anlass gibt, das ist die Folge des 11. September 2001. Es wurde aber nur der Abzug einer Waffe gedrückt, die schon lange vorher existierte.

Welche Konsequenzen hat diese Technologie für das politische System?

Je stärker die Binnengrenzen in ihrer Bedeutung zurückgehen, desto umfassender werden sie durch ein viel dichteres Netz ersetzt. Die neuen Grenzen sind weniger physisch als vielmehr universell, sie sind durch- und weiterschaltbar. Es liegt ein immer feiner werdendes Netz über Europa, ein abstraktes Raster. Du hast keine Sicherheit, dass du nicht bei irgendeinem Raster dabei bist. Eine Opposition in einem autokratischen System, welches diese Überwachungsmittel zur Verfügung hätte, bräuchte jetzt gar nicht mehr anfangen zu arbeiten, denn sie könnte keine elektronischen Kommunikationsmöglichkeiten benutzen.

Welche Möglichkeiten hat denn der Staat, dem entgegenzusetzen?

Datenschützer sind zwar sehr honorige Menschen, aber was bringt es, dass sie in irgendwelchen Gremien ihre Standpunkte drei Minuten lang vortragen dürfen, nur um dabei stets schräg angeschaut zu werden? Simon Davies, der Direktor von »Privacy International«, hat dazu aufgerufen, zu ungewöhnlichen Maßnahmen und zu zivilem Umgehorsam zu greifen.

Gibt es nicht derzeit ein großes Desinteresse an Bürgerrechten, bestenfalls ein Unbehagen?

Das Unbehagen wird mit Sicherheit größer werden, denn die allgemeine Überwachung wird sich für die Gesellschaft als lästig, unpraktisch und einschränkend erweisen. Skandale werden unvermeidlich sein. Nicht zuletzt die Wirtschaftsministerien werden allen Grund haben, die ungehemmte Datensammlung zu blockieren. Es schadet den volkswirtschaftlichen Interessen, wenn Vertreter anderer Volkswirtschaften an Nachrichten gelangen, die nicht für sie bestimmt sind.

»Transparente Proxies« haben sich schließlich auch nur im Consumer-Bereich durchsetzen können, weil Business-Kunden sich aus geschäftlichen Interessen vehement gegen diese Schnüffelei wehren.