



Tony Bunyan

Überwachungsstaat Europa?

Die seit dem 11. September 2001 geplanten oder schon eingeführten Maßnahmen zum Schutz der Bevölkerung, so meinen viele, halten das Gleichgewicht zwischen Sicherheit und Bürgerrechten. Doch es sind genau diese Maßnahmen, durch die die gesamte EU-Bevölkerung unter Beobachtung gestellt wird. Das Advanced Passenger Information System (APIS) zur Überwachung von Flugreisenden wurde 2005 in den USA eingeführt; der EU-Personalausweis soll Fingerabdrücke enthalten, die überall im Schengener Raum weiter gegeben werden dürfen; Informationen aus dem Personalausweis werden in absehbarer Zukunft mit medizinischen Daten und dem Führerschein kombiniert werden; Telekommunikationsanbieter sollen ihre Kundendaten mindestens zwölf Monate speichern und auf Verlangen an europäische oder andere Strafverfolgungsbehörden weitergeben. Unterdessen stellen sich die multinationalen Technologiekonzerne darauf ein, mit der neuen Überwachungstechnologie Milliarden Gewinne einzufahren. Die Zivilgesellschaft muss auf diese enorme Machtverschiebung erst noch reagieren.

Das gängige Argument, man müsse für ein bisschen Sicherheit auf ein bisschen Freiheit verzichten, ist inzwischen unglaubwürdig geworden. Trotzdem hört man es weiterhin auf den Korridoren der EU-Behörden, mit dem Vorbehalt, dass die Einschränkungen unserer Freiheiten vorübergehend seien und mit dem Ende des "Kriegs gegen den Terror" auch aufgehoben würden. Der offenkundigste Denkfehler dieser Argumentation liegt darin, dass der "Krieg gegen den Terror" zum Dauerzustand geworden ist und den Kalten Krieg als ideologische Legitimierungsgrundlage für die Globalisierung abgelöst hat. Das Ökonomische und das Politische gehen Hand in Hand.

Dieser neue "Krieg" ist jedoch viel gefährlicher und alles durchdringender, als es der alte jemals war. Während des Kalten Krieges übte eine Reihe konkurrierender Ideologien — westlicher Kapitalismus und "freiheitliche Demokratie", sowjetischer Kommunismus, Kommunismus des chinesischen Typs sowie verschiedene sozialistische Modelle in der Dritten Welt — auf die kapitalistischen Staaten eine Art Bremsfunktion aus; um sich von der staatlichen Überwachung im Sowjetblock abgrenzen zu können, musste sich die "freiheitliche Demokratie" als solche beweisen. Heute hat jedoch die Mischung aus "Krieg gegen den Terror", westlichem Kapitalismus, freier Marktwirtschaft und "Freiheit und Demokratie" keine Konkurrenz mehr.

Das Paket der Vorkehrungen, die seit dem 11. September 2001 eingeführt oder geplant wurden, so die Behauptung, biete ein ausgewogenes Gleichgewicht zwischen Sicherheit und Bürgerrechten. Regierungen, Minister, Beamte und viele Abgeordnete sind dieser Ansicht und sind dennoch gleichzeitig damit beschäftigt, Maßnahmen auszulegen, die die gesamte europäische Bevölkerung unter Beobachtung stellen werden.

Zunächst steht die Bewegungsfreiheit unter Beschuss. Als erstes wurde eine der vier grundlegenden "Freiheiten" innerhalb der EU aufgegeben — die Freiheit, sich ohne Kontrolle innerhalb Europas bewegen zu dürfen. Um ein Flugzeug zu besteigen, muss jeder Passagier einen Pass oder Personalausweis vorlegen, und dies gilt sogar auf manchen Inlandsflügen. Im April 2004 einigten sich die EU-Vertreter darauf, die Passagierlisten aller Flüge innerhalb und außerhalb Europas kontrollieren zu lassen; gleichermaßen sollen EU-Bürger und Reisende von außerhalb der EU vor dem Besteigen des Flugzeugs überprüft werden. Dabei ist völlig unklar, wie diese Überprüfung stattfinden soll; werden die Namenslisten mit der EU-Liste "terroristischer" Organisationen und Personen abgeglichen; oder mit einer umfassenderen Liste von "Terrorverdächtigen"? Oder vielleicht gar mit einem allgemeinen Verzeichnis jener Personen, die als Terroristen oder Verbrecher, ob organisiert oder nicht, gesucht oder verdächtigt werden?

Es ist nur eine Frage der Zeit, bis ein *Advanced Passenger Information System* (APIS) eingeführt wird, das alle Passagiere in eine von drei Kategorien einteilt: Bei Grün darf der Fluggast einsteigen; bei Gelb muss er sich einer zusätzlichen Überprüfung von Gepäck und Person unterziehen und / oder er wird nach der Ankunft weiter befragt oder gar unter Überwachung gestellt; bei Rot wird er gleich bei Ankunft am Flughafen oder beim Einchecken verhaftet. Tests haben die Fehler im System aufgedeckt: Je nachdem, ob eine spezifische (nur auf Terrorverdächtige beschränkte) Liste zugrunde gelegt wird oder eine allgemeinere (die auch das organisierte und andere Verbrechen einschließt), fallen fünf bis fünfzehn Prozent der Passagiere in die Kategorie "Gelb". Und das ist nicht das Schlimmste: Wenn Geheimdiensten und Sicherheitsbehörden keine Kenntnisse darüber vorliegen, dass es sich bei einer bestimmten Person um einen Terroristen handelt, wird diese das Flugzeug problemlos als Passagier der Kategorie "Grün" besteigen dürfen.

Der zweite Aspekt bezieht sich auf die EU-Entscheidung vom Dezember 2004 zur Einführung biometrischer Pässe. Das Europaparlament wurde in dieser Frage lediglich "konsultiert"; tatsächlich wurde es erpresst, möglichst schnell "Stellung zu beziehen". Der Europarat kündigte an, die Mitbestimmungsrechte des Parlaments bezüglich Immigrations- und Asylfragen bereits zum 1. Januar 2005 auszuweiten, anstatt erst im April 2005 — ein Schritt, der dem Parlament die Mitbestimmung bei Maßnahmen wie der Einführung des biometrischen PASSES einräumte.

Wie die EU behauptet, sind solche Maßnahmen erforderlich, um den internationalen Anforderungen an "biometrische" Reisedokumente zu genügen, entsprechend den Standards der ICAO (International Civil Aviation Organization) — ein Vorhaben der G8-Staaten unter Federführung der USA und Großbritanniens. Der ICAO-Standard erfordert jedoch nur ein digitales Foto, welches nichts weiter ist als eine digitalisierte Version des üblichen Passbilds, das mit dem Passantrag eingesandt und in einen Chip eingelesen wird. Somit kann bei Personenkontrollen bei der Ein- und Ausreise überprüft werden, ob der Passbesitzer tatsächlich die Person auf dem digitalisierten Foto ist. Es handelt sich hierbei um eine sehr einfache Form der Überprüfung, die fälschlicherweise von Ministern und Regierungsbeamten als Einführung des "biometrischen Reisepasses" bezeichnet wurde.

Die von der EU geplanten Neuerungen hingegen sehen vor, dass jeder, der zum ersten Mal einen Reisepass beantragt oder seinen alten Reisepass verlängern lassen möchte, sich zwei oder mehr Fingerabdrücke nehmen lassen muss. Viele Reisende, die sich innerhalb der Grenzen des Schengener

Abkommens bewegen, führen lediglich ihren Personalausweis mit; es gibt jedoch Bestrebungen im Rahmen des Haager Programms, neue Standards für Personalausweise festzulegen, die auch die Speicherung von Fingerabdrücken vorsehen. Da sich Großbritannien nicht am Schengener Abkommen beteiligt, das Fragen zu Grenzkontrollen und Immigration regelt, wird es seinen eigenen biometrischen Reisepass einführen. In Irland, das ebenfalls nicht am Schengener Abkommen teilnimmt, steht eine Entscheidung noch aus.

Großbritannien sieht die Einführung des biometrischen Reisepasses für Erstantragsteller ab 2009 und anschließend für alle Passverlängerungen vor. Dies setzt die Speicherung von Fingerabdrücken und einen Scan voraus, der bis zu 1840 Merkmale des Gesichts erfasst, unter Umständen auch einen Iris-Scan. Biometrische und personenbezogene Angaben des Antragstellers sollen zunächst landesweit gespeichert und später in einer EU-weiten Datenbank zusammengefasst werden.

Die Auswirkungen eines solchen Schritts sind enorm. Im Laufe der nächsten zehn Jahre, während die alten Reisepässe nach und nach ersetzt werden, müssen Millionen Menschen persönlich so genannte "Bearbeitungszentren" aufsuchen, um sich "anzumelden". Für Großbritannien belaufen sich Schätzungen auf über fünf Millionen Antragsteller pro Jahr. Die "Anmeldung" beinhaltet nicht nur den Besuch des Zentrums — bislang konnte ein Reisepass postalisch beantragt werden —, sondern auch ein persönliches Gespräch und die Vorlage von Dokumenten zum Nachweis der Identität. Anschließend werden zwangsweise die biometrischen Daten erhoben. Die britische Regierung versucht darüber hinaus, im Parlament ein Gesetz durchzubringen, nach dem jedem Passinhaber automatisch ein Personalausweis ausgestellt wird.

Doch die Einführung biometrischer Pässe und Personalausweise ist nur ein Teil der Geschichte. Seit Januar 2006 gibt es eine neue EU-Krankenversicherungskarte, auf der auf einem Chip schließlich auch die medizinischen Daten des Karteninhabers gespeichert werden sollen. Neue Richtlinien für den EU-Führerschein sehen vor, dass die Fahrerlaubnis — so wie der Reisepass — alle zehn Jahre (nach Vorstellung einiger Instanzen: alle fünf Jahre) erneuert werden und darüber hinaus mit einem digitalisierten Foto ausgestattet sein muss. Es ist nicht schwer vorzusehen, dass es in der nahen Zukunft Bestrebungen geben wird, den EU-Pass, den Personalausweis, den Führerschein und die Versichertenkarte in einer einzigen biometrischen Chipkarte zusammenzufassen. Die Privatsphäre des Bürgers wird der Bequemlichkeit der Beamten geopfert — oder zumindest hoffen die Behörden darauf. Nach Befürchtung des britischen Datenschutzbeauftragten Richard Thomas "geraten wir schlafwandelnd in die Überwachungsgesellschaft", und diese Sorge betrifft fraglos auch die 450 Millionen Einwohner Europas.

Der dritte kontrovers diskutierte Punkt betrifft die Pflichtspeicherung von Daten. Seit Jahren verlangen die Strafverfolgungsbehörden freien Zugriff auf Telekommunikationsdaten; bislang haben sich Bürgerrechts- und Datenschützergruppen, mit Unterstützung der Medien und der öffentlichen Meinung, erfolgreich dagegen gewehrt. Am 20. September 2001, nur neun Tage nach den Anschlägen auf das World Trade Center, wurde das Thema bei einem außerordentlichen Treffen des europäischen Rats "Justiz und Inneres" (JI) wieder ganz oben auf die Tagesordnung gesetzt.

Der nun zur Debatte stehende Vorschlag würde die Kommunikations- und Dienstleistungsanbieter dazu verpflichten, den Datenverkehr zumindest der

letzten 12 Monate — alle Telefon- und Faxverbindungen, alle Verbindungen im Mobilfunknetz (einschließlich der Standorte, von denen aus die Anrufe getätigt wurden), die E-Mails und Internetdaten — zu speichern und auf Verlangen den Strafverfolgungsbehörden zur Verfügung zu stellen. Der Plan sieht außerdem den Austausch dieser Daten zwischen den Behörden der einzelnen europäischen und nicht-europäischen Länder vor.

Der Vorschlag birgt jedoch eine Reihe von Schwierigkeiten. Technologische Neuerungen haben es mit sich gebracht, dass Internet- und Mailprovider einen unbegrenzten Netzzugang über DSL anbieten und deswegen keine detaillierten Nutzerdaten mehr aufzeichnen (die überholte Technologie beruhte noch auf einem Abrechnungssystem, das sich an der tatsächlichen Nutzung orientierte). Dem aktuellen Vorschlag zufolge müssten Internetanbieter die nicht mehr benötigten Nutzungsdaten für mindestens 12 Monate speichern (früher war diese Spanne auf drei Monate beschränkt). Wer soll die zusätzlichen Kosten tragen, der Staat oder die Telekommunikationsanbieter? Die rechtlichen Grundlagen der Initiative bleiben unklar — was die beteiligten Regierungen nicht davon abgehalten hat, ihre Pläne voranzutreiben.

Die vorgesehene groß angelegte Überwachung von Reisenden und Telekommunikation, unterstützt durch die Einführung einer europaweiten Datei für Fingerabdrücke, personenbezogene Informationen und biometrische Daten, soll durch das "Zugriffsprinzip" weiter ergänzt werden. Nach diesem Prinzip werden die Daten und Geheimdienstinformationen der jeweiligen nationalen Strafverfolgungsbehörden den anderen Strafverfolgungsbehörden in den 27 EU Ländern zugänglich gemacht. Ein unveröffentlichter Bericht zum Thema (EU-Dokument 7416/05) legt nahe, dass das Ziel nicht nur darin besteht, allen EU-Strafverfolgungsbehörden zum Schutz der öffentlichen Ordnung Zugriff auf Personendaten (die auch Fingerabdrücke und DNA-Proben beinhalten) zu gewähren, sondern ihnen gleichzeitig

direkten Zugriff auf die nationalen Verwaltungssysteme aller EU-Mitgliedsländer zu gewähren, beispielsweise zu Verzeichnissen von Personen (einschließlich juristischer Personen), Fahrzeugen, Schusswaffen, Ausweispapieren, Führerscheinen sowie zu Aufzeichnungen über den Flug- und Schiffsverkehr.

Die "nationalen Verwaltungssysteme" werden zweifellos persönliche Krankengeschichten enthalten, sobald diese über eine landesweite Datenbank verfügbar sind. In Großbritannien wird das ab 2006 der Fall sein.

Die damit verbundenen Gefahren liegen auf der Hand: Das "Zugriffsprinzip" überlässt die Behörden einer Selbstregulierung, so dass keine Kontrollen etwaigen Missbrauchs mehr möglich sind. Wurde eine Anfrage bislang auf dem Dienstweg behandelt und durch das jeweilige Innenministerium geprüft, bevor ihr stattgegeben wurde, gibt es zukünftig einen freien Markt für Personendaten, auf dem kein nennenswerter Datenschutz mehr existiert.

Obwohl die Strafverfolgungsbehörden im Kampf gegen den Terrorismus nur eine untergeordnete und eher unterstützende Rolle spielen, wird immer wieder behauptet, sie benötigten diese Maßnahmen, um ihre Durchsetzungsfähigkeit zu erhöhen. Im Kampf gegen den Terrorismus stehen jedoch nicht die Strafverfolgungsbehörden, sondern die Geheim- und Sicherheitsdienste an vorderster Front; nur erstere sammeln Informationen, sei es nachrichtendienstlich (SIGINT), mit Mitteln der Fernmeldeaufklärung

(COMINT) oder mittels menschlicher Quellen (HUMINT), und in den meisten Ländern sind sie mit ausreichenden Befugnissen ausgestattet.

So wie der "Krieg gegen den Terror" als Vorwand dient, um die umfassende Überwachung der Bürger durchzusetzen, wird er von einigen Regierungen und Strafverfolgungsbehörden zum Ausbau ihrer Macht benutzt — ganz zu schweigen von bestimmten multinationalen Konzernen, die sich von der Nachfrage nach den neuen Überwachungstechnologien Aufträge in Milliardenhöhe versprechen. Haben sich die neuen Standards erst in den USA und Europa durchgesetzt, werden sie zum weltweiten Maßstab in Überwachungsfragen werden — und der damit verbundenen Profite.

Wie bei allen Brüsseler Entscheidungen, die in den Medien kaum en detail besprochen werden, bleibt auch diesmal die Reaktion der Zivilgesellschaft auf die enorme Verschiebung des Gleichgewichts zwischen der Macht des Staates einerseits und den Rechten und Freiheiten des Individuums andererseits abzuwarten. Hana Stepankova vom Tschechischen Datenschutzamt meint dazu:

Der Schutz der Privatsphäre ist ein menschlicher Grundwert, und erst das Sammeln personenbezogener Daten ermöglicht das Eindringen in diese Sphäre. Die Bürger derjenigen Länder, die ehemals von totalitären Regimes regiert wurden, haben auf bittere Weise erfahren müssen, dass ihrer Privatsphäre kein Wert beigemessen und sie den staatlichen Interessen geopfert wurde. Sollten Europas Bürger erfahren, dass sie allesamt zu "Verdächtigen" gemacht werden, könnte ihre Duldsamkeit in Opposition umschlagen.

Published 2007-09-04

Original in English

Translation by Eva Bonné

Contribution by Index on Censorship

First published in *Index on Censorship* 3/2005 (English version)

© Tony Bunyan/Index on Censorship

© Eurozine