



****LASST MICH IN RUHE****

• • •

Weil Demokratie ohne Aktion nicht möglich ist!
Weil Information die Basis des Nachdenkens ist!
Weil Nachdenken die Basis der Aktion ist!

**Weil es an jedem Einzelnen liegt,
ob unsere Rechte weiter eingeschränkt werden!**

Das Infomagazin
von und über STOP1984

November 2004

Inhaltsverzeichnis

<i>Neues von der Redaktion</i>	4
<i>Neues vom Datenschutzbeauftragten</i>	5
Gemeinsame Dateien zwischen Polizei und Nachrichtendiensten datenschutzgerecht gestalten	5
EU-Datenschutzbeauftragte verabschieden Informationstexte für Flugpassagiere in die USA	5
Lauschangriffsurteil auch bei anderen heimlichen Eingriffen des Staates zu beachten	6
<i>Neues vom ULD</i>	8
Gemeinsame Presseerklärung zur Beteiligung der GEZ am Adresshandel	8
ULD-Umfrage zur Videoüberwachung: differenzierte Einschätzung – hoher Informationsbedarf	9
<i>Neues vom BSI</i>	10
Newsletter www.bsi-fuer-buerger.de ab jetzt erhältlich	10
<i>Aktiv-Posten</i>	11
Pro-information.de	11
Gegen Biometrie in Ausweisen	12
<i>Weltweites</i>	13
Deutschland : Fingerabdrücke, Echelon und Kameras	14
0FDP gegen USA: Persönlichkeitsrechte versus Fingerabdruck	14
AK Medien der Datenschutzbeauftragten ist gegen Vorratsdatenspeicherung	14
EU-Pläne zur Telekommunikationsüberwachung werden abgelehnt	14
Kamera-Überwachung in Cuxhaven	14
Echelon nun in Darmstadt	14
Deutschland:	
Aufruf gegen EU-Pläne zur Einführung einer Verkehrsdaten-Speicherungspflicht	15
China - Cyberdissidenten und Zensur...	17
Französischer Präsident soll für Cyber-Dissidenten eintreten	17
Zensur von ausländischen Radiostationen	17
Symantec unterstützt Internet-Zensur	17
Unterstützt Google die offizielle Zensur?	17
<i>Neu bei STOP1984 & Co.</i>	18
Neues von anderen NGOs	19
Chaos Computer Club	19
Fahndungsplakat für Datenschneüfler und Überwachungstäter	19
Biometrische Merkmale in Ausweisen erhöhen Sicherheit nicht	19
Überwindbarkeit Biometrischer Systeme beim Chaos Communication Congress	21
Foebud	22
Vier Bundesministerien beraten über RFID	22
Der FoeBuD besucht die EU in Brüssel	23
Datenschutzshoppen beim FoeBuD	23

Erklärung gegen Datenvorratsspeicherung	24
Humanistische Union	25
Stellungnahme zur geplanten Verlängerung der "Auskunft über Telekommunikationsdaten" (lt. §100g / 100h der Strafprozessordnung.)	25
Veranstaltungshinweise	27
17.11.2004 Chaostreff Münster/Osnabrück	27
24.11.2004 Chaostreff Leipzig (Gründungstreffen)	27
30.11.2004 Dresden, SCIENCE-CAFÉ: Wie zerbrechlich ist der gläserne Mensch?	27
Kreativecke	28
Buchrezensionen:	28
Das RAF- Phantom	
Wozu Politik und Wirtschaft Terroristen brauchen	28
Bedingt Dienstbereit	
Im Herzen des BND - die Abrechnung eines Aussteigers	29
Redaktionelles	30

Neues von der Redaktion

Die Möglichkeiten, sich als Terrorist effektiv zu tarnen werden immer geringer. Jedenfalls scheint dies so, schenkt man den aktuellen Bestrebungen Glauben. Die Videoüberwachung soll es beispielsweise richten – und soll „ziellos umherschleudernde Menschen“ gleich als Verdächtige interpretieren und entsprechend handeln. Nein nein, keine Sorge, die automatische Präventiv-Liquidierung ist noch nicht im Gespräch, so weit sind wir noch nicht. Aber wenn einerseits in den USA vor denjenigen gewarnt wird, die zielstrebig mit dem Photohandy auf Schnappschussjagd gehen, andererseits aber das ziellose Schlendern verdächtig wird... tja, was mache ich denn dann um nicht gleich als „Mutmaßlicher“ angesehen zu werden? Einen Kopfstand? Übe ich mich in Breakdance oder schlafe ich auf der Bank, unter der Bank, neben der Bank? Stehe ich mit geschlossenen Augen herum? So ganz ausgereift scheinen jedenfalls die Ideen noch nicht ganz zu sein, die die Politik auf beiden Seiten des Atlantiks zur Zeit ausbrütet.

Das Argument „ich habe nichts zu verbergen“ kann also auf der nächstgelegenen Altwörter-Müllkippe entsorgt werden. Denn die Entscheidung trifft man nicht mehr selbst sondern Maschinen, Gesetze und Paranoia in trauter Dreieinigkeit.

Unverdächtig sein...

Ja, WIE denn bloß?



Der große Bruder in Wartestellung

Während einerseits überall der „Große Bruder“ seine wachsamen (elektronischen) Augen nicht mehr schließt, wird anderorts schon an der passenden Laudatio für jene gefeilt, die sich in besonderer Weise um Datenschutz und Privatsphäre „verdient gemacht haben“ – die BigBrotherAwards stehen fast schon vor der Tür. Grund genug, sich einmal kurz mit denjenigen zu befassen, die diesen Negativpreis alljährlich verleihen.

STOP1984 hat sich derweil bemüht, das Magazin noch etwas übersichtlicher zu gestalten und hat jeder Rubrik nun ein Logo zugeordnet, das den Überblick erleichtern soll. Und auch sonst präsentieren wir uns ein wenig verändert – daher: Viel Spaß beim Lesen.

Twister

Neues vom Datenschutzbeauftragten

DBA

Gemeinsame Dateien zwischen Polizei und Nachrichtendiensten datenschutzgerecht gestalten

Auf Einladung des Bundeskriminalamtes hat der Bundesbeauftragte für den Datenschutz Peter Schaar im Rahmen der BKA-Herbsttagung am 4. November 2004 an einer Podiumsdiskussion zum Thema „Sind unsere Netzwerke gegen Terrorismus schlagkräftig genug?“ teilgenommen. Dabei erklärte er:

Eine gezielte projektbezogene Zusammenarbeit zwischen Polizei und Nachrichtendiensten zur besseren Bekämpfung des internationalen Terrorismus ist datenschutzrechtlich vertretbar, soweit dabei dem Trennungsgebot sowie dem vom Bundesverfassungsgericht im Volkszählungs-rteil postulierten Prinzip der informationellen Gewaltenteilung Rechnung getragen wird.

Auch das Führen gemeinsamer Dateien, in die Erkenntnisse von Nachrichtendiensten und Polizei einfließen, ist in diesem Rahmen unter engen Voraussetzungen möglich. Insbesondere dürfen die beteiligten Stellen nur nach Maßgabe der für sie geltenden Übermittlungsregelungen berechtigt werden, Daten in gemeinsame Dateien einzustellen und daraus abzurufen.

Die Daten müssen einer strikten Zweckbindung unterworfen bleiben. Ihre Herkunft muss im gesamten Verarbeitungsprozess durch eine entsprechende Kennzeichnung ersichtlich sein. Zudem muss stets erkennbar sein, welche Stelle die Daten weitergegeben hat. Die Abrufe sind zu protokollieren und müssen einer effektiven

datenschutzrechtlichen Kontrolle zugänglich sein.

Schließlich müssen die Rechte der durch die Datenverarbeitung Betroffenen, insbesondere deren Recht auf Auskunft, gewährleistet bleiben.

Gemeinsame Dateien müssen sich auf terroristische Aktivitäten beschränken und dürfen den Extremismus ohne terroristischen Hintergrund nicht einbeziehen.

Die Polizei ist für die Beobachtung des islamistischen Extremismus ohne terroristischen Hintergrund nicht zuständig und darf nicht über eine gemeinsame Datei insoweit Datenerhebungsbefugnisse des Verfassungsschutzes erhalten. Derartige Datenerhebungsbefugnisse für die Polizei würden die Grenze zwischen Polizei und Verfassungsschutz verwischen.

EU-Datenschutzbeauftragte verabschieden Informationstexte für Flugpassagiere in die USA

Die Gruppe der EU-Datenschutzbeauftragten nach Artikel 29 der EU-Datenschutzrichtlinie hat sich unter Vorsitz des Bundesbeauftragten für den Datenschutz Peter Schaar auf einheitliche Informationstexte für Passagiere, die in die USA fliegen, verständigt.

Nach Abschluss des Abkommens zwischen der EU-Kommission und den USA über die Übermittlung von Passagierdaten hielt es die Datenschutzgruppe für erforderlich, die Fluggäste um-

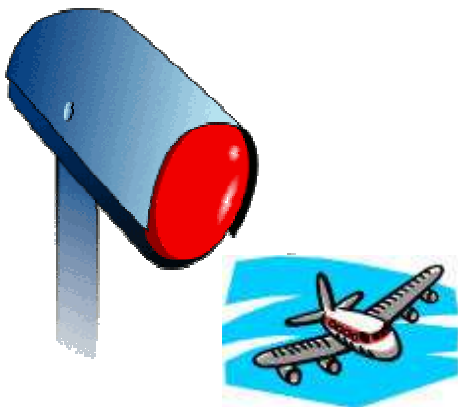
fassend über die Auswirkungen des Abkommens und die Rechte der Betroffenen zu unterrichten. Jährlich fliegen mehrere Millionen EU-Bürgerinnen und Bürger in die USA und fallen damit unter das Abkommen.

Bei den jetzt erarbeiteten Texten handelt es sich zum einen um einen Kurzttext, den die Passagiere zum Beispiel erhalten, wenn sie ihren Flugschein in einer Reiseagentur oder per Telefon buchen.

Die Langversion, erhältlich unter anderem auf den Internetseiten der Fluggesellschaften, gibt ein umfassendes Bild über den Zweck der Datenübermittlung, den Empfänger der Daten und die Speicherdauer und informiert eingehend über die Rechte der betroffenen Fluggäste.

So können sich die Passagiere an das US-Ministerium für Heimatschutz wenden und Auskunft über die dort gespeicherten Daten verlangen und die Berichtigung falscher Eintragungen fordern.

Mit großer Befriedigung stellt Peter Schaar fest, dass mit diesen Informationstexten zukünftig alle Flugpassagiere, gleich wo und wie sie ihren Flug von Europa aus in die USA buchen, einheitlich unterrichtet werden. Er sieht darin ein gelungenes Beispiel für die enge Zusammenarbeit der EU-Datenschutzbehörden.



Lauschangriffsurteil auch bei anderen heimlichen Eingriffen des Staates zu beachten

Symposium des Bundesbeauftragten für
den Datenschutz
Bonn, den 9. November 2004

Anlässlich eines Symposiums zum "Großen Lauschangriff", zu dem der Bundesbeauftragte für den Datenschutz Peter Schaar eingeladen hatte, waren sich Vertreter der Wissenschaft und der Politik einig, dass das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung Auswirkungen auf alle heimlichen staatlichen Eingriffsbefugnisse hat.

Betroffen davon sind nicht nur bundesrechtliche Vorschriften, sondern auch die Polizei- und Verfassungsschutzgesetze der Länder. Der Bundesbeauftragte für den Datenschutz sieht sich durch die Ergebnisse des Symposiums in seinen Forderungen bestätigt, die er bereits anlässlich der Verkündung der Entscheidung zum Großen Lauschangriff erhoben hatte: "Alle Befugnisregelungen des Bundes und der Länder zu verdeckten Datenerhebungen sind nun auf den Prüfstand zu stellen und in weiten Bereichen neu zu fassen."

Das Symposium in der Berliner Staatsbibliothek diente dem Ziel, die rechtspolitische Diskussion im Anschluss an das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung vom 3. März 2004 voranzubringen. Die Tagung fand mit rund 200 Teilnehmern aus Politik, Wissenschaft, Verwaltung und Sicherheitsbehörden großen Zuspruch.

Aufgezeigt werden sollte insbesondere, inwiefern neben der akustischen Wohnraumüberwachung auch andere staatliche Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung, an die

Forderungen des Bundesverfassungsgerichts anzupassen sind.

Vier namhafte Rechtsgelehrte und Universitätsprofessoren äußerten sich in Vorträgen zu diesem Problemkreis:

Spiros Simitis (Frankfurt),
Manfred Baldus (Erfurt),
Friedhelm Hufen (Mainz) und
Christoph Gusy (Bielefeld).

Im Anschluss fand unter der Leitung des Datenschutzbeauftragten Peter Schaar eine Podiumsdiskussion mit Rechts- und Innenpolitikern der Fraktionen des Deutschen Bundestages statt:

für die SPD-Fraktion Dieter Wiefelspütz,
für die CDU/CSU-Fraktion Stephan Mayer,
für die Fraktion Bündnis 90/Die Grünen Jerzy Montag
und für die FDP-Fraktion Rainer Funke.

Als Vertreter der Kläger vor dem Bundesverfassungsgericht nahm der ehemalige Vizepräsident des Deutschen Bundestages Burkhard Hirsch teil.

Alle Beteiligten würdigten die Entscheidung des Bundesverfassungsgerichts, die deutliche Grenzen für das heimliche Abhören von Wohnungen mit akustischen Hilfsmitteln setzt, als Urteil mit herausragender Bedeutung.



Die Rechtsprofessoren kamen übereinstimmend zu dem Ergebnis, dass aus der Entscheidung auch Folgerungen für andere staatliche Eingriffsbefugnisse zu ziehen sind. Angesichts des hohen Stellenwerts, den das Bundesverfassungsgericht dem "absolut geschützten Kernbereich privater Lebensgestaltung" beimesse, seien auch die gesetzlichen Ermächtigungen zu anderen strafprozessualen, aber auch zu präventiv-polizeilichen Überwachungsmaßnahmen reformbedürftig.

Keines der Polizei- und Verfassungsschutzgesetze des Bundes und der Länder enthält nämlich bislang Vorschriften zum Schutz dieses absolut geschützten Kernbereichs. Außerdem müssen verfahrensrechtliche Regelungen zur Benachrichtigung der durch die heimliche Maßnahme betroffenen Personen und zur Kennzeichnung der verdeckt gewonnenen Daten aufgenommen werden.

Auch im Rahmen der Podiumsdiskussion war man sich parteiübergreifend einig, dass das Urteil Ausstrahlungswirkung auf die politische Debatte und die Gesetzgebung auch in anderen Bereichen staatlicher Eingriffsbefugnisse hat.

Neues vom ULD

ULD

Gemeinsame Presseerklärung zur Beteiligung der GEZ am Adresshandel

Die Datenschutzbeauftragten der Länder Berlin, Brandenburg, Bremen, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Sachsen und Schleswig-Holstein erklären gemeinsam zum Entwurf des 8. Rundfunkänderungsstaatsvertrages:

Wiederholt haben sich die Datenschutzbeauftragten des Bundes und der Länder dafür eingesetzt, bei der Finanzierung des öffentlich-rechtlichen Rundfunks in Deutschland das Prinzip von Datenvermeidung und Datensparsamkeit in stärkerem Maße zu berücksichtigen.

In der Kritik steht dabei im Besonderen die Beschaffung von jährlich mehreren Millionen Adressen hinter dem Rücken der Betroffenen beim kommerziellen Adresshandel durch die von den Rundfunkanstalten beauftragte Gebühreneinzugszentrale (GEZ), die diese Adressen für flächendeckende Mailing-Aktionen nutzt. Zahlreiche Beschwerden und Anfragen von Bürgerinnen und Bürgern beziehen sich auf diese Praxis der GEZ, die die zuständigen Landesdatenschutzbeauftragten als rechtswidrig bezeichnet haben.

Anstatt gemeinsam mit den Datenschutzbeauftragten datenschutzfreundliche Varianten einer gerechten Finanzierung des öffentlich-rechtlichen Rundfunks ernsthaft zu prüfen, haben die Ministerpräsidenten der Länder mit dem Entwurf eines 8. Rundfunkänderungsstaatsvertrages neben der Erhöhung der Rundfunkgebühren und deren Erreckung auf Computer weitgehend ohne die gebotene Beteiligung der in einigen Ländern zuständigen Landesdaten-

schutzbeauftragten eine weitere Verschlechterung des Datenschutzes beschlossen:

Um die Beschaffung von Daten beim kommerziellen Adresshandel gesetzlich zu legitimieren, soll der Rundfunkgebührenstaatsvertrag um eine Befugnis erweitert werden, nach der die Rundfunkanstalten und die GEZ personenbezogene Daten unter den gleichen Bedingungen verarbeiten dürfen wie privatwirtschaftliche Unternehmen.

Die vorgesehene Befugnis ist mit datenschutzrechtlichen Grundsätzen nicht zu vereinbaren. Während öffentlich-rechtliche Institutionen personenbezogene Daten nur verarbeiten dürfen, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, ist die Datenverarbeitung der im Wettbewerb stehenden Privatwirtschaft vom Prinzip der Vertragsfreiheit geprägt.

Die öffentlich-rechtlichen Rundfunkanstalten stehen hinsichtlich des Gebühreneinzugs in keinem Wettbewerb zu anderen Rundfunkveranstaltern. Schließlich haben die Länder gegen das Votum der Datenschutzbeauftragten bereits vor Jahren regelmäßige Übermittlungen von Meldedaten an die Rundfunkanstalten zugelassen, weil dies für erforderlich gehalten wurde.

V.I.S.P Schraut, Kleinmachnow, 8. November 2004

ULD-Umfrage zur Videoüberwachung: differenzierte Einschätzung – hoher Informationsbedarf

Mitarbeiter des Unabhängigen Landes-
zentrums für Datenschutz Schleswig-Hol-
stein haben im Rahmen des Schleswig-Hol-
stein-Tags in Flensburg Mitte August und
beim Tag der offenen Tür im Schleswig-Hol-
steinischen Landtag Anfang September 2004
in 300 Interviews eine Bevölkerungs-
befragung zum Thema Videoüberwachung
durchgeführt. Entgegen der weit verbreiteten
Meinung, Videoüberwachung finde breite
Zustimmung in der Bevölkerung, ergab sich
ein äußerst differenziertes Bild:

Zwar meinten ca. 62% der Befragten, dass
Videoüberwachung für die Sicherheit
förderlich sein kann, doch wünschten sich
nur ca. 28% eine stärkere Nutzung dieses
Instruments.

Der Einsatz wird in klassischen Situationen
(Bahnhöfe, Banken, Tiefgaragen,
Tankstellen) allgemein weitgehend akzep-
tiert.

Eine flächendeckende Überwachung wird
dagegen von der ganz großen Mehrheit
abgelehnt.

Dies gilt insbesondere für Lebensbereiche
und Situationen, die als besonders privat
oder persönlich wahrgenommen werden
(Toiletten, Umkleidekabinen).

Auch im pädagogischen Umfeld (Schulen,
Kindergärten) wird der Einsatz technischer

Überwachung überwiegend abgelehnt.
Hinsichtlich der Überwachung von
Fußgängerzonen und öffentlichen Plätzen
bestehen kontroverse Einschätzungen bei
den befragten Bürgerinnen und Bürgern.

Ein eindeutiges Ergebnis der Umfrage ist,
dass die Menschen zu wenig über die tat-
sächlich stattfindende Videoüberwachung
informiert sind und dass sie sich eine ver-
besserte Information wünschen.

Für den Leiter des ULD, Thilo Weichert,
zeigt die Umfrage, dass in Sachen
Transparenz bei der Videoüberwachung
großer Nachholbedarf besteht.

Dies bestätigt die vom ULD schon lange
vertretene Meinung, dass die Installation von
Videokameras im öffentlichen Raum melde-
pflichtig und deren Standorte bekannt gege-
ben werden sollten, z.B. über das Internet.
Für eine Ausweitung der Überwachungsbe-
fugnisse oder eine Ausweitung der Praxis
bestünde dagegen keinerlei Veranlassung:

"Die Befragung hat ergeben, dass die
optische Dauerbeobachtung die Un-
befangenheit und das Persönlichkeitsrecht
der Betroffenen beeinträchtigen kann.
Daher darf von dieser Maßnahme, die
keinesfalls ein Allheilmittel in Sachen
Sicherheit ist, nur gezielt und
ausnahmsweise Gebrauch gemacht werden.

Das ULD sieht weiterhin in der Kontrolle
der Videoüberwachung einen Schwerpunkt
seiner Arbeit.

Neues vom BSI

Newsletter www.bsi-fuer-buerger.de ab jetzt erhältlich

SICHER ° INFORMIERT

Der Newsletter von www.bsi-fuer-buerger.de

Ausgabe vom 04.11.2004

Guten Tag,
wer sich mit IT-Sicherheit beschäftigt, dem wird nie langweilig: Kaum wird eine Lücke geschlossen, taucht mindestens eine neue auf. So geschehen zuletzt gleich nach dem großen "Patch-Day" von Microsoft, an dem eine ganze Reihe von Sicherheitslöchern geschlossen wurden: Rund um den Internet Explorer traten bereits wieder neue Sicherheitslücken auf.

Anlass zur Sorge gibt auch die neue Desktop-Suche von Google. Mit ihrer Hilfe ist es möglich auf PCs, die von mehreren Personen genutzt werden, private Daten zu recherchieren. Vorsichtig sollte man aber nicht nur am PC sein - in unserem Newsletter finden sich auch Meldungen zu Sicherheitsproblemen rund ums Telefonieren. So können etwa Java-fähige Handys aufgrund einer Schwachstelle ferngesteuert werden.

Inmitten all der warnenden Rufe gibt es aber auch Positives zu vermelden: Die internationale Zusammenarbeit im Kampf gegen die Computerkriminalität wächst. Und wir tun etwas dafür, um Sie mit aktuellen Sicherheitstechnologien vertraut zu machen. Ein Beispiel dafür ist die digitale Signatur, mit der dieser Newsletter "beglaubigt" wird. Entspannte und sichere Stunden am Computer wünscht Ihnen

BSI-FUER-BUERGER

So beginnt der neue Newsletter des Bundesministerium für Sicherheit in der Informa-

tionstechnik (BSI), der sich in seiner ersten Ausgabe mit folgenden Themen befasst:

- ° Schnüffeln mit Javascript: Internet Explorer leckt
- ° Ferngesteuerte Handys: Sicherheitslücke bei Sun
- ° Wurmstichige Umfragen: Gefälschte E-Mail von eBay infiziert PCs
- ° Mit gutem Beispiel voran: »SICHER ° INFORMIERT« mit digitaler Signatur
- ° Gläserne E-Mails: Abrufen persönlicher Inhalte mit Google Desktop-Suche
- ° Schau genau: Gefälschte 0190-Rechnungen im Umlauf
- ° Immer auf der Hut sein: Gefälschte Sicherheitswarnungen von Red Hat
- ° Grund zur Fr.eu.de: Die .eu-Domains kommen
- ° Grenzenlos sicher: 15 Staaten arbeiten bei IT-Sicherheit zusammen

Der Newsletter abonniert werden durch eine Mail an die folgende Adresse:

newsletter_anmelden@bsi-fuer-buerger.de.

Aktiv-Posten

Unter Aktiv-Posten sollen aktuelle Aktionen von Initiativen und Vereinen vorgestellt werden, die jedem die Möglichkeit geben, direkt „dabei zu sein“. Ob Protestkundgebungen oder Online-Petitionen, Unterschriftensammlungen oder einfache Stimmabgabe – „Aktiv-Posten“ soll helfen, über momentan laufende Aktionen auf dem Laufenden zu bleiben und so einen Überblick über das zu bekommen, was man selbst unterstützen kann.

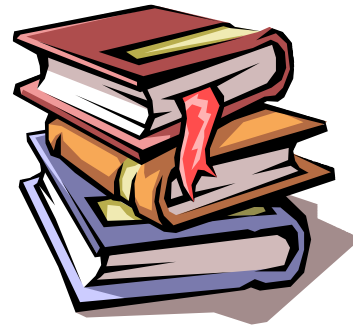
Pro-information.de

Die Online-Kampagne für ein Informationsfreiheitsgesetz in Deutschland.
Mehr Transparenz bei Behördenentscheidungen, mehr Informationen über Sachverhalte, mehr Möglichkeiten, Korruption aufzudecken...

Informationsfreiheit bedeutet für den Bürger ein großes Plus! Die Kampagne „pro-information.de“ ruft daher auf, sie durch Unterschriften zu unterstützen.

Warum ist Informationsfreiheit wichtig?

Die Humanistische Union, die unter anderem bei der Kampagne pro-information.de mitwirkt, stellt es folgendermaßen dar:



Mit einem Informationsfreiheitsgesetz, das es bereits in über 50 Staaten gibt, erhält jeder Bürger das Recht, Akten einzusehen oder Kopien von Unterlagen öffentlicher Stellen zu bekommen, ohne dass eine persönliche Betroffenheit oder eine Antragsbegründung erforderlich ist. Genau definierte Ausnahmeklauseln sorgen dafür, dass sensible Informationen, z.B. personenbezogene Daten oder Geschäftsgeheimnisse, geschützt bleiben. Durch ein Informationsfreiheitsgesetz würde ein Bürgerrecht verwirklicht, das aus Sicht der acht Organisationen in einer modernen Demokratie unverzichtbar ist. Nur wer Zugang zu Informationen hat, kann sich sinnvoll politisch beteiligen.

Gegen Biometrie in Ausweisen

Biometrisch sind wir alle... irgendwie...

Ganz unbemerkt zuweilen, aber auch ganz massiv zuweilen. So kommt diese Technologie über die Menschen der entwickelten westlichen Welt. Und so soll sie auch vorgeblich zum Besten, zu seiner Sicherheit und seinem eigen Schutz dienen und eingesetzt werden.

Doch ist es nicht ein wenig übertrieben, wenn man in New York sein Gepäck an der gerade wieder eröffneten Freiheitsstatute nur gegen Abgabe seiner eigenen Freiheit in Sachen der biometrischen Merkmale hinterlegen kann? Da soll doch jeder einen Fingerabdruck abgeben, nur um sein Gepäck zu sichern, sicher aufbewahren zu können. Freiheit...?

Ob daran die Franzosen dachten, als sie Amerika die Freiheitsstatute schenkten? Oder was soll man davon halten, dass jeder Reisende wie ein Schwerverbrecher behandelt, seine Fingerabdrücke nebst digital aufbereitetem Foto zu einem biometrischen Pass vereint wiederfindet, nur um schnell die Einreise-Kontrollen oder die Visa-Pflichten in den USA zu passieren?

Aber es geht noch schleichender. Es geht immer einen Schritt weiter. So werden in den USA bereits Hotel-Suiten der gehobenen Preisklassen mit entsprechenden Iris-Scannern vor unbefugtem Betreten gesichert. Eine Erregenschaft, die die zahlende Klientel sicher zu schätzen weis. Aber es gibt ja dort bereits Einkaufs-Ketten, wo per Fingerabdruck auch der gemeine Bürger sich in die vermeintliche Sicherheit biometrischer Techniken begeben darf.

Bedenkenswert sollte aber sein, dass selbst Experten zuweilen am sicheren Funktionieren der biometrischen Sicherungen zweifeln. Warum das wohl so ist?

Nun, wir sind alle Individuen und auch wenn es nicht mehr erlaubt sein sollte, beim Passfoto zu lächeln, so haben wir die Angewohnheit, zuweilen in aller Öffentlichkeit selbiges zu tun. Und schon verwehrt uns die biometrische Zutrittskontrolle deswegen den Einlass...

Weil wir womöglich nicht der sind, der wir sind? Weil wir biometrischer sind, als es jede derzeit bekannte Technik erfassen kann, das ist wohl genauer.

(von Hannes*)

Doch es geht noch weiter - auch in Deutschland wird Biometrie seinen Einzug halten. Pässe und demnächst, wenn es nach dem Willen der Polizei geht, auch Personalausweise sollen mit Fingerabdrücken des Besitzers ausgestattet werden.

Einwände sowie Argumente dagegen, wie sie beispielsweise der Chaos Computer Club formulierte, werden süffisant bis arrogant abgeschmettert, wenn die Verantwortlichen nicht mehr als ein „Der CCC soll bei seinen Leisten bleiben“ dafür über hat.

Nichtsdestotrotz formiert sich Widerstand. Auf der Seite

<http://www.freiraumverein.de/projekte/datenschutz>

hat man „mit dem Einrichten einer von den Projektteilnehmern direkt über das Internet pflegbaren Seite begonnen

Und auch auf

<http://www.bumens.org>.

sind erste Argumente und erste Ideen gesammelt worden.

Eine Mailingliste steht ebenfalls zur Verfügung ist per Mail an majordomo@stop1984.com (Text: subscribe biometrie) abonniebar.

Weltweites

Zusätzlich zum täglichen Nachrichtenüberblick auf unserer Homepage und em Newsletter wollen wir hier einen Überblick über die momentanen Entwicklungen, Gesetze etc. bieten, die in den letzten vier Wochen Schlagzeilen machten (oder eben nicht, denn viele Themen werden noch immer eher zögerlich oder gar nicht aufgegriffen).

Weltweites soll aber auch helfen, einmal Nachrichten aus Regionen zu finden, von denen man eher selten oder nur am Rande hört. Pressefreiheit auf den Malediven, der maßgeschneiderte Führerschein in Ohio, die Medien in Weißrussland... all das sind Themen, die wir kurz anreißen wollen, die wir ins Gespräch bringen wollen. Mehr Informationen dazu findet man unter den angegebenen Links und oft auch bei STOP1984 direkt.



Deutschland : Fingerabdrücke, Echelon und Kameras

• **FDP gegen USA: Persönlichkeitsrechte versus Fingerabdruck**

Vor dem Hintergrund verschärfter Einreisebestimmungen in die USA mahnt die FDP vor der Aufgabe der Persönlichkeitsrechte zugunsten "vermeintlicher Sicherheit". Einreisende in die USA müssen seit neustem ein Digitalfoto und Fingerabdrücke von sich machen lassen. Die Daten bleiben auf unbestimmte Zeit gespeichert und werden mit den Daten bekannter Terroristen verglichen.

Quelle:

<http://www.de.internet.com/index.php?id=2031266§ion=Marketing-News>

• **AK Medien der Datenschutzbeauftragten ist gegen Vorratsdatenspeicherung**

Der Arbeitskreis Medien der Datenschutzbeauftragten von Bund und Ländern hat sich erneut gegen eine Vorratsspeicherung von Verkehrs- und Nutzungsdaten in der Telekommunikation ausgesprochen. Die geforderte systematische verdachtslose Aufzeichnung der Kommunikation der Menschen ist laut dem AK Medien nicht mit dem europäischen Menschenrecht auf Schutz des Privatlebens und mit dem deutschen Grundrecht des Fernmeldegeheimnisses vereinbar.

Quelle:

<http://www.datenschutz.de/news/detail/?nid=1360>

• **EU-Pläne zur Telekommunikationsüberwachung werden abgelehnt**

In einer gemeinsamen Presseerklärung haben die "Deutsche Vereinigung für Datenschutz" (DVD) und das Forum "InformatikerInnen für Frieden und gesellschaftliche Verantwortung" (FifF) die Pläne der EU abgelehnt,



umfangreiche Verkehrsdaten über Telekommunikationsverbindungen über lange Zeit zu speichern.

Quelle:

<http://www.datenschutz.de/news/detail/?nid=1362>

• **Kamera-Überwachung in Cuxhaven**

Viele privat betriebene Kameras überwachen den öffentlichen Raum im Stadtgebiet von Cuxhaven. Es stellt sich die Frage nach dem Datenschutz. Auch Befürworter der Kamera-Überwachung zur Verbrechensabwehr machen sich Sorgen. Bernd Michaels vom kommunalen Präventionsrat: "Wer kontrolliert die Überwacher. Man weiß nicht, wo die Daten landen und wie sie benutzt werden."

Quelle:

http://www.cn-online.de/archiv_artikel.cfm?Artikel=7112

• **Echelon nun in Darmstadt**

Nach der Schließung der zum Echelon-Abhörsystem gehörenden Anlage in Bad Aibling ist nun vom Kommando des US-Militärs bestätigt worden, dass eine neue Anlage in Darmstadt-Griesheim ihre Aufgaben übernommen hat. Nach wie vor bleibt das Echelon-System umstritten.

Welche Signale von Militär und Geheimdiensten genau aufgezeichnet werden, ist nach wie vor nicht genau klar. Geheimdienstexperten behaupten: Echelon fängt Faxe, E-Mails und Telefonate ab, deren Inhalt per Computer auf verdächtige Inhalte überprüft werde. Potenziell verdächtige Inhalte werden in die USA übermittelt, wo sie von Spezialisten überprüft werden. Kritiker meinen, das Echelon-System diene zudem nicht nur der Terrorabwehr, sondern auch der Industriespionage. Die Genehmigung der Anlage ist vorerst bis Ende 2012 befristet.

Deutschland:

Aufruf gegen EU-Pläne zur Einführung einer Verkehrsdaten-Speicherungspflicht

(Offener Brief an die Mitglieder der zuständigen Bundestagsausschüsse vom 15.11.2004)

Sehr geehrte... (Name der/des Abgeordneten), dem Bundestag liegt derzeit ein EU-Vorschlag zur Beratung vor, der die Einführung einer generellen Vorratsspeicherung von Telekommunikationsdaten vorsieht (BR-Drs. 406/04, BT-Drs. 15/3696, Ziff. 2.15).

Wegen vielfältiger Umgehungsmöglichkeiten für ernsthafte Kriminelle (z.B. durch Nutzung vorausbezahlter Mobilfunkkarten, die auf den Namen einer anderen Person registriert sind) sind Auswirkungen einer solchen Verkehrsdaten-Speicherungspflicht auf die Kriminalitätsrate nicht zu erwarten. Auch EU-Staaten, in denen eine Verkehrsdaten-Speicherungspflicht existiert, haben derartiges nicht zu berichten.

Dass eine Vorratsspeicherung gar terroristische Anschläge verhindern könnte, kann nicht ernstlich erwartet werden. Selbst in den USA gibt es daher weder eine Verkehrsdaten-Speicherungspflicht noch Pläne zu deren Einführung.

Der Möglichkeit, in Einzelfällen Ermittlungserfolge erzielen zu können, stünde die lückenlose Aufzeichnung des Telekommunikationsverhaltens der gesamten Bevölkerung (einschließlich der Bewegungen von Handybesitzern sowie der Aktivitäten von Internetnutzern) gegenüber. Außerdem drohen der Industrie Kosten in dreistelliger Millionenhöhe. Dementsprechend wird eine Verkehrsdaten-Speicherungspflicht fast geschlossen abgelehnt:

- In einem Aufruf von 90 europäischen Bürgerrechtsorganisationen wird eine Verkehrsdaten-Speicherungspflicht als unverhältnismäßige Einschränkung der Grund- und Menschenrechte, insbesondere von Artikel 8 der Europäischen Menschenrechtskonvention, bezeichnet (<http://www.privacyinternational.org/issues/terrorism/rpt/responsetorention.html>).
- Diese Einschätzung bestätigt eine neue Entscheidung des Bundesarbeitsgerichts zum Thema Videoüberwachung, derzufolge eine allgemeine und verdachtslose Verhaltensüberwachung und -aufzeichnung unverhältnismäßig ist (BAG, 1 ABR 21/03 vom 29.06.2004).
- Im Rahmen der Beratung des Telekommunikationsgesetzes (TKG) dieses Jahr haben sich alle Bundestagsfraktionen geschlossen gegen die Einführung einer Verkehrsdaten-Speicherungspflicht ausgesprochen.
- Auch der Bundesrat stimmte diesem Ergebnis nach Abschluss des Vermittlungsverfahrens zu. Zudem lehnte er im Herbst einen Vorschlag seines Innen- und Rechtsausschusses ab, der den EU-Plan zur Einführung einer Verkehrsdaten-Speicherungspflicht begrüßen sollte (BR-Drs. 406/1/04).
- Schließlich hat auch das Europaparlament wiederholt die Unvereinbarkeit einer Verkehrsdaten-Speicherungspflicht mit den Menschenrechten hervorgehoben (Empfehlung vom 06.09.2001, Dokument Nr. T5-0452/2001 sowie Entschließung vom 09.03.2004, Dokument Nr. T5-0104/2004, Ziff. 18).

- Befürwortet werden die Pläne zur Einführung einer Verkehrsdaten-Speicherungspflicht einzig von den Innen- und Justizministerien, die sich leider in der Bundesregierung durchzusetzen scheinen (siehe Stellungnahme der Bundesregierung in BT-Drs. 15/3901).

Der geplante EU-Rahmenbeschluss kann ohne Zustimmung des Europaparlaments gefasst werden. Seine Annahme bedarf allerdings eines einstimmigen Beschlusses des Rates "Justiz und Inneres" (JI), dem die Justiz- und Innenminister der Mitgliedstaaten angehören.

Außerdem treten Rahmenbeschlüsse erst nach Ratifikation durch die nationalen Parlamente in Kraft. Wie bei völkerrechtlichen Verträgen besteht keine Pflicht zur Ratifikation.

Es darf nicht sein, dass der auf demokratischem Weg in Deutschland gefundene Konsens, keine Vorratsspeicherung von Verkehrsdaten einzuführen, durch einen hinter verschlossenen Türen gefassten Exekutivbeschluss des EU-Rates umgangen wird.

Ich appelliere daher an Sie, in dem aktuellen Beratungsverfahren einen Bundestagsbeschluss herbeizuführen, der klar und eindeutig

1. die Bundesregierung auffordert, die Einführung einer Verkehrsdaten-Speicherungspflicht auf EU-Ebene zu verhindern, indem sie gegen jeden solchen Vorschlag stimmt, und
2. ankündigt, dass der Deutsche Bundestag einen Rahmenbeschluss, der die Einführung einer Verkehrsdaten-Speicherungspflicht vorsieht, in keinem Fall ratifizieren wird.

Ein klares Votum des Bundestags ist entscheidend, um die generelle Aufzeichnung des Telekommunikations- und Bewegungsverhaltens unschuldiger Bürgerinnen und Bürger zu verhindern.

Mit freundlichen Grüßen,

Patrick Breyer

Diesem Aufruf haben sich angeschlossen (Stand: 15.11.2004):

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF) e.V. (www.fiff.de), vertreten durch Werner Hülsmann, Vorstandsmitglied

Institut für Bürgerrechte & öffentliche Sicherheit e.V. (www.cilip.de), vertreten durch Martina Kant, Vorstandsmitglied

STOP1984 (www.stop1984.com)

Der Aufruf findet sich unter:

<http://tkg-verfassungsbeschwerde.de/presse.htm>

China - Cyberdissidenten und Zensur...

• **Französischer Präsident soll für Cyber-Dissidenten eintreten**

Der französische Präsident Jacques Chirac, der sich hauptsächlich wegen des Ausbaus der wirtschaftlichen Beziehungen in China ab morgen aufhält, wurde von der NGO "Reporters Without Borders" (RSF) aufgefordert, sich für die sofortige Freilassung des Cyber-Dissidenten Huang Qi einzusetzen.

Huang Qi wurde der Subversion beschuldigt und ist seit Juni 2000 unter schwersten Bedingungen in Haft. Die RSF fordert, dass auch alle weiteren einsitzenden Cyber-Dissidenten frei gelassen werden.

Quelle:

<http://peacehall.com/news/gb/english/2004/10/200410072241.shtml>

• **Zensur von ausländischen Radiostationen**

Anlässlich des Besuchs des französischen Präsidenten Jacques Chirac in China wurde bekannt, dass eine französische Firma über die Lieferung von Technik an die Regierung verhandelt, die eine Unterbindung der Ausstrahlung von ausländischen Radiosendungen nach China ermöglichen soll.

Dabei geht es um ausländische Radiosender wie der in Norwegen ansässigen "Voice of Tibet", des "BBC World Service", der "Voice of America" und "Radio Free Asia". Dies ist Zensur und eine Unterdrückung der Informationsfreiheit, urteilt die NGO "Reporters Without Borders" (RSF).

Quelle:

<http://peacehall.com/news/gb/english/2004/10/200410090706.shtml>



• **Symantec unterstützt Internet-Zensur**

Die Firma "Symantec" bietet für den Markt in China ein spezielles "Norton AntiVirus" an. Dieses hat auf einer mit der chinesischen Regierung abgestimmten Blacklist eine Reihe von Softwareprodukten integriert, von denen so ein Download unterbunden werden soll.

Es handelt sich dabei um Software, wie das Produkt "Freegate", welches Webseiten dem Nutzer zugänglich machen kann, die eigentlich von China blockiert werden, indem es alternative Proxy-Server benutzt.

Quelle:

<http://asia.cnet.com/news/software/0,39037051,39194057,00.htm>

• **Unterstützt Google die offizielle Zensur?**

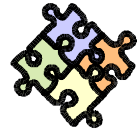
Die Suchmaschine Google muss sich fragen lassen, ob sie es in China zulässt, Daten ihrer Nutzer ungefragt und ohne richterliche beziehungsweise schriftliche Anordnung an die chinesischen Strafverfolgungsbehörden weiterzugeben. Zwar gibt es auch in den USA die Möglichkeit, Nutzerdaten von den Internet-Service-Providern zu erfragen, dies erfordert aber rechtlich klar definierte Schritte.

Dies ist in China nicht der Fall und die Suchmaschine hat mit der Regierung Chinas entsprechende Vereinbarungen zugelassen, die einen schnellen Zugriff auf Nutzerdaten ohne vorherige rechtliche Prüfung erlaubt.

Quelle:

<http://peacehall.com/news/gb/english/2004/10/200410132322.shtml>

Neu bei STOP1984 & Co.



„Sagt mal, warum macht eigentlich niemand etwas zum Thema RFID?“
Die Frage ist nur ein Beispiel für das, was heute, trotz aller Suchmaschinen und Vernetzungsmöglichkeiten fehlt: ein Überblick.

Initiativen, Vereine oder Organisationen kommen und gehen, Webseiten verschwinden ebenso schnell wie sie entstanden sind, Ansprechpartner wechseln... Das Ergebnis ist oft genug Verwunderung, wenn man herausfindet, dass es bereits einige „Eckchen“ gibt, die sich mit einem Thema befassen, das man selbst gerade neu aufgreifen wollte. So wird das Rad oft genug doppelt und dreifach erfunden.

Neben unseren eigenen Aktivitäten wollen wir bei STOP1984 deshalb vor allen Dingen eines:
Die Vernetzung der verschiedenen Initiativen vorantreiben und als Informationsschnittstelle dienen.



Wir wollen Initiativen und Ansprechpartner vorstellen, Aktionen mehr Aufmerksamkeit verschaffen, Linktips geben. Wir hoffen, dass das Magazin in den nächsten Monaten daher auch immer öfter von anderen Initiativen berichten kann, dass sich diese bei uns melden, sich vorstellen, ihre Aktivitäten bei uns „melden“, so dass STOP1984 seinen Teil dazu beitragen kann, weltweit die verschiedenen Bürgerrechtler mehr miteinander in Kontakt zu bringen.

Beiträge von anderen sind also willkommen, genauso wie Veranstaltungstips, Presseerklärungen, Aktionsvorankündigungen...
Als Kontaktadresse steht die infoteam@stop1984.com zur Verfügung, ein passender Betreff erleichtert natürlich die Bearbeitung ;-)

Neues von anderen NGOs

• Chaos Computer Club

Fahndungsplakat für Datenschnüffler und Überwachungsstäter

Auf dem Fahndungsplakat des CCC werden Politiker wie Industrielle gesucht, die per Gesetz und Firmenphilosophie die Privatsphäre vieler verletzen und das Recht auf informationelle Selbstbestimmung einschränken.

Unter anderem mit Ulla Schmidts Gesundheitskarte, den veraeterischen Farbkopierern von Canon und niveauvoller Lobbyarbeit auf EU-Ebene zu Lasten des immer glaeserner werdenen Musikhoeers.

Das Plakat gibt es online zum Selbstaussdruck (pdf) unter folgender Adresse:
A4 Fassung in schwarz/weiss mit 300 dpi zum Selbstaussdrucken (PDF)
http://www.ccc.de/campaigns/fahndung/CC_C_-_Fahndungsplakat_v0.4_-_A4_sw_300dpi.pdf?language=de

A4 Fassung in Vollfarbe mit 300 dpi zum Selbstaussdrucken (PDF)
http://www.ccc.de/campaigns/fahndung/CC_C_-_Fahndungsplakat_v0.4_-_A4_4c_300dpi.pdf?language=de

Mehr Infos zum Plakat gibt es unter:
<http://www.ccc.de/campaigns/fahndungsplakat>



Biometrische Merkmale in Ausweisen erhöhen Sicherheit nicht



(Presseerklärung)

Anlässlich des Beschluss der Innenminister der G5 Staaten (Deutschland, Frankreich, Großbritannien, Italien und Spanien), neben dem bereits beschlossenen zur Gesichtserkennung geeignetem Digitalfoto, ab dem Jahre 2006 auch noch den Fingerabdruck als biometrisches Merkmal für Reisepässe einzuführen [1] weist der Chaos Computer Club auf die einfache Fälschbarkeit der biometrischen Merkmale hin.

CCC-Sprecher Andy Müller-Maguhn bezeichnete den Beschluss unter Hinweis auf jüngste Forschungsergebnisse einer CCC-Arbeitsgruppe als "fragwürdige Sicherheits-simulation". "Die vermeintliche Erhöhung der Fälschungssicherheit von Ausweis-papieren durch die Einführung biometrischer Merkmale ist in der Praxis de facto nicht gegeben. Zum Preis von mehreren Hundert Millionen Euro wird hier mit Steuergeldern dem Bürger eine Sicherheitssimulation verkauft, die auch nicht im entferntesten eine Erhöhung des Sicherheitsniveaus gegenüber qualifizierten Angreifern oder gar Terroristen bringt.", sagte Müller-Maguhn in Berlin.

Die CCC-Arbeitsgruppe Biometrie dokumentiert auf einer Internet-Seite [2] des Chaos Computer Club wie einfach sich Fingerabdrücke fremder Personen zur Überlistung biometrischer Erkennungsgeräte fälschen lassen. Im wesentlich genügt es, sich den Fingerabdruck z.B. durch kurzzeitigen Zugriff auf ein Trinkglas oder einen anderen berührten Gegenstand zu verschaffen.

Die Einführung eines Identifikations-Systems, das eine entwürdigende erkennungsdienstliche Erfassung aller Bürger erfordert, wie sie bisher nur für Straftäter üblich ist, steht in keinem vertretbaren Verhältnis zum erzielbaren Sicherheitsgewinn.

Angesichts der unbestritten hohen Fälschungssicherheit der deutschen Ausweisdokumente konnte das Innenministerium auch auf Anfrage von Bundestags-Abgeordneten keine Statistik vorlegen, die einen dringenden Handlungsbedarf für die flächendeckende Verwendung von Biometrie in Ausweisdokumenten rechtfertigt. Die Kriminalstatistik weist einen gleichbleibend niedrigen Stand an Fälschungsversuchen auf.

Offenbar dient das Projekt aus Sicht des CCC zu nicht unwesentlichen Teilen der Förderung der "Sicherheits"-Industrie, die händeringend nach einem repräsentativen Pilotprojekt für ihre praxisuntaugliche Technologie sucht. Die Verfolgung von Zielen der Wirtschaftsförderung unter dem Deckmantel der Sicherheitspolitik führt hier zur schlechtestmöglichen Lösung.

Die Berufung auf angebliche "Internationale Standards" wird dabei nach Ansicht des CCC von Politikern aller beteiligten Länder als Universalentschuldigung für eklatante Einschränkungen von Bürgerrechten benutzt. Diese "Internationalen Standards" sind ohne jegliche demokratische Kontrolle entstandene informelle Abmachungen. Hier sind die nationalen Parlamente in der Pflicht, sich nicht zum Erfüllungsgehilfen von internationalen Kungelrunden der Sicherheitsbehörden zu machen.

Befremdlich erscheint dem CCC dabei, das die jetzt vom deutschen Innenminister Schily mitgefällte Entscheidung sich klar gegen das Volkszählungsurteil des Bundesverfassungsgerichts [3] von 1983 richtet. Das Bundesverfassungsgericht legte das Verbot eines universellen Personenkennzeichens fest. Durch die Verwendung von unveränderlichen biometrischen Merkmalen als Bestandteil der Ausweisdokumente wird nun

gegen dieses Verbot verstossen, da aus diesen Merkmalen zwangsläufig ein universell eindeutiges Personenkennzeichen errechnet wird.

Angesichts der Kombination von internationaler Sicherheitshysterie und massiven wirtschaftlichen Interessen ist ein sachbezogener Umgang mit dem Thema Biometrie dringend erforderlich.

Daher hat der Chaos Computer Club einen Forderungskatalog [4] für die Einführung biometrischer Technologie im staatlichen und sonstigem Kontext erarbeitet, der einen menschenwürdigen und sinnvollen Einsatz ermöglichen soll.

"Abgesehen von den datenschutz- und sicherheitspolitischen Bedenken, die sich durch die erkennungsdienstliche Behandlung der Gesamtbevölkerung ergeben, gibt es völlig profane Gründe, die gegen biometrische Sicherheitsmerkmale in Ausweisdokumenten sprechen. Die Systeme sind extrem störanfällig. Zudem haben etwa 2% der Bevölkerung überhaupt keine ausreichend ausgeprägten Fingerabdrücke für eine biometrische Erfassung. Für 8 Millionen Europäer sind also ständige Probleme bei der Grenzkontrolle bereits vorprogrammiert." fasste CCC-Sprecher Müller-Maguhn die Kritik zusammen.

Die CCC Forderungen im einzelnen:

- 1. Eine öffentliche Debatte und die Aufklärung der Bevölkerung über die Risiken.

Die Einführung von Biometrischen Systemen ausschliesslich auf der Grundlage eines sachlich objektiv nachgewiesenen Bedarfs, nachausführlicher öffentlicher und parlamentarischer Diskussion und Kontrolle.

- 2. Der CCC fordert, nur Systeme zu verwenden, die eine aktive Teilnahme der Personen bei der Überprüfung erfordern, d.h. nicht für eine verdeckte Fern-Identifikation geeignet sind, um das Recht auf informationelle Selbstbestimmung zu erhalten.
- 3. Bei der Auswahl einer geeigneten Technologie für die staatliche Einführung von biometrischen Merkmalen muss nicht nur eine fälschungssichere Technologie gewählt werden, sondern auch die Haftungsfrage bei Mißbrauchsfällen für unbescholtene Bürger geklärt werden.
- 4. Der Verzicht auf die Speicherung von biometrischen Merkmalen in einer zentralen oder in vernetzten dezentralen Datenbanken, gesetzlich vorgeschriebener Einsatz von dezentralen autonomen Verifikationssystemen (z.B. auf Smart-Card Basis).
- 5. Keine Speicherung von Biometrie-Rohdaten aufgrund der vielfältigen Mißbrauchsmöglichkeiten (Krankheitserkennung etc.).
- 6. Keine Verwendung von biometrischer Technologie, die zu einer Diskriminierung einzelner Personen bzw. Personengruppen führt.
- 7. Test der geplanten Systeme durch unabhängige Organisationen, umfassende Feldtests vor der Einführung sowie eine öffentliche wissenschaftliche Begleitung des Einsatzes.
- 8. Die strenge Zweckbindung der biometrischen Daten muß durch robuste rechtliche und technische Maßnahmen gewährleistet sein.
- 9. Verzicht der Verwendung von RFID-Technologie zur Speicherung und Abfrage der biometrischen Daten.

Überwindbarkeit Biometrischer Systeme beim Chaos Communication Congress



Anlässlich unserer Pressemitteilung zur nicht gegebenen Erhöhung der Sicherheit durch biometrische Merkmale in Ausweisdokumenten, weisen wir darauf hin, dass unsere Fachgruppe »Biometrie« eine Demonstration der technischen Überwindbarkeit auf dem Chaos Communication Congress vornehmen wird.

Während eines Vortrags wird eine Einführung in die Technik gegeben und die politischen Entscheidungen unter Berücksichtigung von Studien und Tests zur Tauglichkeit vorraussichtlich verwendeter Systeme vorgestellt. Ziel ist es aufzuzeigen, wie wenig die Systeme in den geplanten Einsatzszenarien den versprochenen Sicherheitsgewinn bringen.

Im Anschluss daran wird die Überwindung der drei wichtigsten Systeme (Gesichtserkennung, Fingerabdruck- und Iriserkennung) demonstriert. Eine abschließende Diskussion zur politischen Lage und den technischen Systemen lädt zum Einbringen in das Thema ein.

»21C3: The Usual Suspects«: Der 21. Chaos Communication Congress ist ein jährlich stattfindender Fachkongress über Computertechnik und -sicherheit, Datenschutz, die Auswirkungen der Technik auf die Gesellschaft als auch ein Treffen der Hackerkultur.

Er wird vom Chaos Computer Club e.V. organisiert. Wie jedes Jahr findet der Congress vom 27. bis 29. Dezember in Berlin statt. Weitere Informationen sind auf den Webseiten des CCC [verfügbar](#).

• **Foebud**

Vier Bundesministerien beraten über RFID

Der FoeBuD kämpft dafür, dass RFID-Technik, die Gegenstände per Funkwellen identifiziert und per Lesegerät Informationen aussendet, keinesfalls unkontrolliert eingeführt wird.

Am 17. August luden Wirtschafts-, Verbraucherschutz-, Innen- und Justizministerium gemeinsam zu einer Diskussionsveranstaltung mit dem Titel »RFID und Verbraucherschutz« nach Berlin.. Auch der FoeBuD war eingeladen und fragt sich, ob dies nun ein erster Schritt das geforderte Gremium, dem Daten-, Verbraucher- und UmweltschützerInnen (Elektrosmog) sowie Arbeitnehmer-Vertretungen und BürgerrechtlerInnen angehören, einzurichten, sein soll.

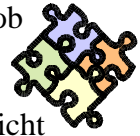
Noch gar nicht geklärt ist die Frage der Kostenübernahme. Der FoeBuD fordert nämlich auch, dass die Kosten der Mitarbeit in diesem Gremium nach dem Verursacherprinzip von den Nutznießern der RFID-Technik getragen werden müssen.

Bei dem Forum waren die RFID-Kritiker deutlich in der Minderheit. Der Bundesdatenschutzbeauftragte und FoeBuD als der Verein, der mit seiner Kritik den Bund erst auf die Probleme, die mit dem RFID-Einsatz einhergehen, aufmerksam gemacht hat, waren eingeladen. Rund dreiviertel der Anwesenden waren Vertreter von Organisationen, die RFID-Technik herstellen, normieren oder sie anwenden.

So saßen in der Runde neben der Pro-RFID-Lobby-Gruppe Eicar auch der Einzelhandelsverband und die Handelskonzerne Metro, Rewe, Procter&Gamle und Kraft. Ihr Tenor: Die Anwendung von RFID solle keinesfalls durch Gesetze geregelt werden.

Mit dabei auch Patrick von Braumnühl vom Bundesverband Verbraucherzentrale. Er be-

zog eine klare Position und hob hervor, dass sich bereits heute Handelsunternehmen bei dem Umgang mit Kundenkarten nicht immer an Gesetze halten. Spätestens an der Kasse müsse RFID standardmäßig deaktiviert werden.



Für Rena Tangens gibt es keinen Grund für blindes Vertrauen in die Konzerne. Sie plädierte entschieden für Gesetze, die den Umgang mit RFID regeln, da RFID »vielfältige Risiken für eine demokratische Gesellschaft birgt«. Sie könne zur umfassenden Kontrolle, Überwachung und Manipulation der Bürger eingesetzt werden. Weltweit eindeutige Seriennummern der RFID-Chips in Koppelung mit Datenbanken ermöglichten detaillierte Bewegungs-, Konsum- und Interessenprofile der Menschen.

Bei der Einführung von RFID seien daher nicht nur die Interessen der Hersteller, des Handels und der Verbraucher berührt, sondern auch fundamentale Rechte der Bürger. Eine gesetzliche Regulierung würde die »good guys« – also die Firmen, die die Privatsphäre der Bürger tatsächlich achten – schützen: vor der böswilligen Konkurrenz und vor ihren eigenen Aktionären.



Der FoeBuD besucht die EU in Brüssel

Anfang September waren Rena Tangens und Jan Hennig vom FoeBuD zu einem Vortrag vor der §29 AG nach Brüssel eingeladen [1]. Die Artikel 29-Arbeitsgruppe der Europäischen Kommission nimmt sich Fragen des Datenschutzes an. Rena Tangens und Jan Hennig reisten zu diesem Termin gemeinsam nach Brüssel.

Nach einigem bürokratischen Hin und Her (eigentlich sollte der Besuch in Brüssel schon früher stattfinden) kam es doch noch zu diesem Termin. »Ich bin von der Arbeitsgruppe angenehm überrascht«, sagt Tangens. Die Datenschutzbeauftragten aus 15 europäischen Mitgliedsstaaten und von der EU-Kommission lauschten aufmerksam dem Vortrag und diskutierten. Offensichtlich war ihr Interesse sehr groß.

»Ich habe den Eindruck, dass die Arbeitsgruppe sehr ernsthaft an einer Empfehlung zur Nutzung von RFID arbeitet«, schildert Tangens.

Die Arbeitsgruppe kann allerdings nur Empfehlungen aussprechen und zur Gesetzgebung anregen. Die Veranstaltung in Brüssel zeigt, dass die Arbeit des FoeBuD gegen eine unkontrollierte Einführung von RFID auch europaweit Früchte trägt.

Einen Zwischenstopp legten Rena Tangens und Jan Hennig bei Mechthild Rothe, der Europaabgeordnete der SPD im Kreis Ovestfalen-Lippe, die sich kurzfristig Zeit genommen hatte, ein. Sie trafen sie in ihrem Büro im zwölften Stock des EU-Gebäudes. Anfangs höflich, später hingerissen ließ sie sich von der FoeBuD-Arbeit, den BigBrotherAwards und der RFID-Technik berichten. Der FoeBuD hofft, dass es hier noch zu fruchtbaren Kooperationen kommt. Auf jeden Fall, so Rena Tangens, habe sie eine beeindruckende Frau kennengelernt. [2]

Datenschutzshoppen beim FoeBuD



Der FoeBuD hat jetzt einen richtigen Internetshop mit bunten Bildern, Bestsellerliste und Sonderangeboten – alles garantiert ohne Kundenkarte. Gehandelt wird mit allerlei Nützlichem und Identitätsstiftenden in Sachen Datenschutz: Da gibt es Pesthörnchen-Aufkleber, Kapuzen-Shirts oder Stempel zur Abwehr von Werbung. Nützlich auch die „RFID-Cardprotection“: Durch dieses Kästchen, praktischerweise in Visitenkartengröße, kommen kaum elektromagnetische Strahlen durch. Wer darin seine mit RFID-Chip bestückte Kundenkarte aufbewahrt, kann nicht heimlich gescannt werden.

Sinnhaftend, eindeutig und praktisch ein Aufkleber, der vor Videouberwachung warnt. Auf ihm ist ein Rutenbündel zu sehen, in dem statt eines Beiles eine Videokamera steckt. [1]. Das Rutenbündel (lat fasces) mit Beil wurde im römischen Reich als Symbol der Macht über Leben und Tod eingesetzt. Mussolini setzte das Rutenbündel als Zeichen seiner totalitären Herrschaft ein. Vom lateinischen Wort ‚fasces‘ leitet sich das Wort Faschismus ab.

Der FoeBuD-Aufkleber ist zugleich ein Vorschlag für ein standardisiertes Kamerawarnschild. Denn das »Deutsche Institut für Normung (DIIN)« will die Warnschilder in euphemistischem Blau halten. Keine Farbe, die der FoeBuD für die Warnung vor Überwachungskameras schätzt.

Warnschilder seien im öffentlichen Raum niemals blau, sondern auffallend orange. Blaue Schilder signalisierten im öffentlichen Raum eher eine Empfehlung: »Hier sollten Sie 130 km/h fahren« zum Beispiel.

Dies habe keine Warnwirkung, sagt der FoeBuD. Der FoeBuD-Aufkleber hingegen sorgt mit seinem leuchtend-orangenem Piktogramm für Klarheit: „Videoüberwachung gefährdet die Demokratie“, sagt padeluun, „und dies soll der Aufkleber eindeutig darstellen“.



[1] Informationen zum Rutenbündel:
http://de.wikipedia.org/wiki/Rutenb%C3%BCndel_mit_Beil
Shoppen beim FoeBuD:
<http://shop.foebud.org/>

Erklärung gegen Datenvorratsspeicherung



Wenn es nach dem Willen von Großbritannien, Irland, Spanien und Frankreich geht, sollen alle Telekommunikationsgesellschaften und Internetprovider in den EU-Staaten verpflichtet werden, die Verkehrsdaten aller Telekommunikationsvorgänge und Internetnutzungen aller Kundinnen und Kunden für mindestens 12 und bis zu 36 Monate zu speichern.

Bisher dürfen in Deutschland ohne besondere Verdachtsmomente nur die Abrechnungsdaten für bis zu sechs Monaten nach Rechnungsversand gespeichert werden. Mit der geplanten Neuregelung würden die Telekommunikations-Verkehrsdaten von 450 Millionen Menschen in der EU für mindestens 12 Monate gespeichert, weil nicht auszuschließen sei, dass unter Ausnutzung von Telefon, SMS, MMS, E-Mail und Internet Straftaten begangen werden.

Der FoeBuD gehört zu den Mitunterzeichnern einer Erklärung gegen die Datenvorratsspeicherung.

• **Humanistische Union**

**Stellungnahme zur geplanten
Verlängerung der
"Auskunft über
Telekommunikationsdaten"
(lt. §100g / 100h der
Strafprozessordnung.)**

Zugriff der Strafverfolgungsbehörden auf
Telekommunikations-Verbindungsdaten soll
um drei Jahre verlängert werden
Humanistische Union verlangt Berichtspflichten
und Evaluierung
(Presseerklärung vom 28. September 2004)

Die Humanistische Union (HU) hält es für
völlig unangemessen, wenn ein Gesetz [1],
das massiv in das Fernmeldegeheimnis
(Artikel 10 Grundgesetz) eingreift, vom
Bundestag ohne jede Debatte im Plenum
beschlossen würde.

Angesichts der tiefen Eingriffe in die
Grundrechte aller Bürgerinnen und Bürger
spricht sie sich gegen eine automatische
Verlängerung der bisherigen Gesetzesregelung aus.

Die Bürgerrechtsorganisation appelliert in
einem Brief an die Mitglieder des
Rechtsausschusses, dem vorliegenden
Gesetzesentwurf der Bundesregierung nicht
zuzustimmen.

Obwohl die Auskunft über Verbindungsdaten
bereits vor drei Jahren neu geregelt
wurde, gibt es bis heute keinerlei statistisches
Zahlenmaterial über Umfang und
Wirksamkeit solcher Auskunftserteilungen.
So ist weder bekannt, wie oft solche
Auskünfte eingeholt wurden, wie viele
unbeteiligte Bürgerinnen und Bürger davon
betroffen sind, noch welche Relevanz diese
Auskünfte für laufende Ermittlungsverfahren
hatten.

Die HU schlägt daher in ihrer Stellungnahme
jährliche Berichtspflichten an den Bundestag

vor, damit eine Bewertung dieser Eingriffe
in das Fernmeldegeheimnis möglich wird.
Nur so sei gewährleistet, dass bei einer
künftigen Gesamtnovelle der Telekom-
munikationsüberwachung eine sinnvolle
Abwägung zwischen den Erfordernissen der
Strafverfolgung und dem Schutz des
Grundrechts auf freie Kommunikation
stattfinden könne.

Verfassungsrechtlich außerordentlich
bedenklich ist nach Ansicht der Humanistischen
Union die sogenannte
Zielwahlsuche.

Um Rufnummern der ankommenden Gespräche
für einen "verdächtigen" Anschluss zu
ermitteln, müssen die abgehenden Gespräche
aller Bürgerinnen, Bürger und Institutionen
in einem aufwändigen technischen Verfahren
abgeglichen werden.

Nach einer von dem Strafrechtler Prof. Dr.
Jürgen Welp (Münster) im Jahre 2000
veröffentlichten Abhandlung werden bei
jeder Zielwahlsuche bis zu 450 Millionen
Telekommunikationsdaten abgeglichen.

Angesichts dieser Reichweite der
Auskunftserteilung sollten Eingriffe in das
Fernmeldegeheimnis nur dann zugelassen
werden, wenn nachweisbar ist, dass sie für
eine wirksame Strafverfolgung unabdingbar
sind.

Die Stellungnahme an die Mitglieder des
Rechtsausschusses ist im Internet abrufbar
unter: <http://www.humanistische-union.de/article.php?sid=200>

Für Rückfragen:
Sven Lüders (Bundesgeschäftsführung) über
Telefon 030 / 204 502 56

[1]
Die Regelungen in §§ 100g / 100h der
Strafprozessordnung über den Zugriff der
Strafverfolgungsbehörden auf Telekom-
munikationsverbindungsdaten, die

ursprünglich bis zum 31. Dezember 2004 befristet waren, sollen um weitere drei Jahre verlängert werden.

Durch die Änderungen der Strafprozessordnung können die Strafverfolgungsbehörden von den Betreibern der Telekommunikationsanlagen (Telekom, Vodafone usw.) Auskunft darüber verlangen, wer, wann wie lange welche Rufnummern angerufen hat. Bei Mobilfunktelefonen können zusätzlich die Standortdaten abgefragt werden.

Der Rechtsausschuss des Deutschen Bundestags wird sich voraussichtlich am kommenden Mittwoch, dem 29. September 2004, mit dem Gesetzentwurf der Bundesregierung befassen.

Nach derzeitigem Kenntnisstand soll das Gesetz schon am Donnerstag, dem 30. September 2004 - also einen Tag nach der Sitzung des Rechtsausschusses - im Bundestag ohne Aussprache verabschiedet werden.

Veranstaltungshinweise

November 2004

17.11.2004 Chaostreff Münster/Osnabrück

Unser Treff findet statt im Büro von [Attac Osnabrück](http://www.attac.de/osnabrueck) (<http://www.attac.de/osnabrueck>) in der [Wörthstraße 71z](http://www.attac.de/osnabrueck/aktionen/buero/weg.htm) (<http://www.attac.de/osnabrueck/aktionen/buero/weg.htm>). Parkplätze für PKW finden sich in der Regel an der Hauptstraße oder in einer Nebenstraße, zu Fuß liegt das Büro etwa 10-15 Minuten Weg vom Hauptbahnhof entfernt. Ab Münster besteht in der Regel eine [Mitfahrmöglichkeit](#), anderes eventuell auf Absprache.

Beim Treff gibt es Strom und (schmalbandiges = 128 kBit) Internet über WLAN. Notebooks sollten also mitgebracht werden. Das Netz steht aber primär zum Arbeiten und Recherchieren zur Verfügung, der Chaostreff ist kein Hackcenter und kein Internet-Cafe. Wir treffen uns jeweils in den ungeraden Kalenderwochen, die nächsten Termine sind also:

- **KW47, Dienstag 17. November 2004**
- **KW49, Dienstag 1. Dezember 2004**
- **KW51, Dienstag 15. Dezember 2004.**

Beginn ist jeweils **gegen 20 Uhr**. Meist wird kurz danach erst einmal Essen geholt, Hunger darf also mitgebracht werden. Es kann sein, daß wir zum Essen kurzzeitig nicht vor Ort sind, daher lohnt sich pünktliches Erscheinen. Über aktuelle Terminverschiebungen und ähnliches informiert zuverlässig unsere Mailingliste (Abonnieren durch Mail an: public-subscribe@mos.name)

24.11.2004 Chaostreff Leipzig (Gründungstreffen)

Am Mittwoch, den 24.11.2004 können sich die, die daran interessiert sind, einen Chaostreff in Leipzig zu gründen, treffen:

Ort: Reudnitz Terrassen
Zeit: ab 20.00 Uhr

Adresse: Oststr. 81 (Ecke Holsteinstr)
PLZ, Ort: 04317 Leipzig

30.11.2004 Dresden, SCIENCE-CAFÉ: Wie zerbrechlich ist der gläserne Mensch?

30 NOVEMBER, DIENSTAG, 18 UHR
Deutsches Hygienemuseum Dresden
RESTAURANT LINGNER
SCIENCE-CAFÉ: Wie zerbrechlich ist der gläserne Mensch?

Datenschutz und genetische Tests.
Zu Gast:
Andreas Schurig, Datenschutzbeauftragter des Freistaates Sachsen
und Giuseppe Testa, Tobias Heckel, Max-Planck-Institut für molekulare Zellbiologie und Genetik

Das Science-Café findet statt in Kooperation mit dem MPI.
<http://www.dhmd.de/neu/index.php?id=82>

Kreativecke

Buchrezensionen:

- **Das RAF- Phantom
Wozu Politik und Wirtschaft
Terroristen brauchen**

(Gerhard Wisnewski, Wolfgang
Landgraeber, Ekkehard Sieker)

Wir brauchen Berichterstattung und Kommentierung der Wirklichkeit, nicht der Unwirklichkeit. Wir müssen sagen, was ist. Bemühen wir uns also um Offenheit. Wir brauchen Glasnost für den Kapitalismus - auch und gerade für den Kapitalismus.
(Alfred Herrhausen)

Jetzt ein Rezesion zu einem Buch, was ein Phantom aus längst vergangener Zeit beschreibt, ist das nicht mehr etwas für eineGeschichtsstunde? Sicher, in diesem Buch wird ein unfassbares Ding, eine Organisation beschrieben, die RAF, welche schon lange aus den Schlagzeilen der Medien verschwunden ist.

Aber: Das Buch ist nach wie vor hochaktuell und brisant. Denn es geht insbesondere auf ein Phantom der RAF in Dritter Generation ein, dass sich konsequent und systematisch jedem Ermittlungserfolg der Polizei und Strafverfolgungsbehörden entzieht. Ein Phantom, was nie wirklich gesichtet, den erfasst, gefasst wurde.

Warum istdas so? Warum gelingt es dieser Dritten Generation der RAF unterden Augen einer wohl blinden Polizei komplizierteste Attentate mit so weitreichenden, aber zumeist totgeschwiegenen Konsequenzen auszuführen?

Der Verdacht drängt sich auf und er wird in diesem Buch mit Fakten untermauert, dass es diese Dritte Generation der RAF in dem Sinne nicht gibt.

Sondern dass wir es hier mit Verschwörungen zu tun haben, die auch von staatlicher Seite zuweilen sehr wohlwollend gesehen

und entsprechend geschützt werden. Wenn sie nicht sogar von ganz hoch angesiedelten Kreisen initiiert wurden. Den es gibt viele politische und wirtschaftliche Interessen, die es zu wahren gilt und was zählt da schon ein Menschenleben, wenn man doch damit eine Entwicklung aufhalten kann oder ihr das Wasser abgraben kann. Und andere Entwicklungen dafür in Gang setzen kann, die sonst kaum machbar wären. Der Terror der RAF in Dritter Generation macht's möglich...

Das Buch geht sehr ausführlich auf die Attentate dieser Dritten Generation der RAF ein, beleuchtet Hintergründe und befragt Zeitzeugen. Und es zeigt die Auswirkungen dieser Attentate, die zuweilen ganz dramatische Auswirkungen hatten über alle politischen, wirtschaftlichen und territorialen Grenzen hinweg.

Und das Buch beschwört den Leser immer wieder auf die Details zu achten und die Konsequenzen und Auswirkungen dieser Attentate auf die bürgerlichen Rechte und Freiheiten zu sehen. Viel zuoft wurden gerade diese Attentate ausgenutzt, um von staatlicher Seite mit einem Bündel von Massnahmen die bürgerlichen Freiheiten zu beschneiden. Auch dafür zeigt dies Buch Beispiele.

Und an dieser Stelle zeigen sich die Parallelen zu den aktuellen Ereignissen um den weltweiten Terrorismus, an dieser Stelle schliesst sich gleichsam der Kreis. Auch heute wird ein Kampf gegen den Terror mit der Jagd nach einem Phantom begründet, ein Kampf der genauso erfolglos bleibt und der genauso ausgenutzt wird, die bürgerlichen Rechte und Freiheiten zu beschneiden - ein weiteres Mal.

(Rezension von Hannes*)

Ausgabe: Oktober 1997

Verlag: Knauer

ISBN: 3-426-80010-1

482 Seiten ,9,90 EUR

• **Bedingt Dienstbereit**
Im Herzen des BND - die
Abrechnung eines Aussteigers

(Norbert Juretzko / Wilhelm Dietl)

Um es vorweg zu nehmen. Das Buch der Autoren Norbert Juretzko und Wilhelm Dietl liest sich locker und flüssig und nimmt stellenweise romanhafte Züge an. Insofern eine handwerklich gelungene Arbeit.

Das Buch soll eine schonungslose Abrechnung mit dem Auslandsgeheimdienst BND sein und als solches steht es in der Kritik aus verschiedenen Richtungen. Das ist nur zu verständlich, letztlich handelt es sich in dem Buch um Vorgänge aus der jüngsten und zugleich geheimsten Geschichte der nun wieder vereinten BRD. Zugleich sind sie ausschliesslich auf einen sehr beschränkten Bereich des BND bezogen. Es geht hauptsächlich um die Auslandsspionage gegen die ehemalige Sowjetunion und ihre Nachfolgestaaten. Und so können und werden nur begrenzte Innenansichten dieses Geheimdienstes, der dort agierenden Menschen und der Aktivitäten beschrieben.

In den ersten Kapiteln werden interessante Details der Spionage gegen die damalige Westgruppe der sowjetischen Armee und ihren Abzug aus der ehemaligen DDR offenbart. Hier kommt sehr stark das Interesse der USA, die notwendige Zusammenarbeit und die gleichzeitig sich entwickelnden Reibereien und Rivalitäten mit dem Auslandsgeheimdiensten der USA ins Spiel. Und es ist erschreckend, zu sehen, wie wenig der BND wirklich in der Lage war, diese Aufgaben im Sinne einer routinierten und profihaften Arbeit zu bewältigen.

Im weiteren wird fast schon emotionslos über den Umgang mit Post und Briefgeheimnissen der Bürger der ehemaligen DDR berichtet

Und bereits in diesen Kapiteln zeigt sich die Gratwanderung dieses Geheimdienstes. Er agierte damals und auch heute in einer Grauzone der Rechtstaatlichkeit, die auch die

Würde und die Privatsphäre der Menschen, die in die Fänge des BND auf die eine oder andere Weise gelangten nicht gerade fürsorglich behandelt.

Darauf folgend wird eine pikante Seite der jüngsten Geschichte der BRD beleuchtet. Nämlich, dass auch sie mit einem Netz aus Schläfern überzogen wurde, um im Falle eines Angriffs und Überrollens durch feindliche, hier speziell sowjetische Armeekräfte ein Netz von funktionierenden Hinterlandspionen parat zu haben.

Auch darauf aufbauend beschreibt das Buch dann die Aktivitäten, die vorgenommen wurden, um in den Nachfolgestaaten der ehemaligen Sowjetunion sogenannte Quellen, andere würden einfach Spione sagen, zu finden, zu werben und zu leiten.

Insbesondere in den letzten Kapiteln verliert sich das Buch zusehends in einer persönlichen, eigenen Abrechnung mit dem BND. So verschwinden Aussagen über die Zusammenarbeit mit dem amerikanischen Geheimdienst sang und klanglos und auch über den Arbeitsbereich und Wirkungskreis des Autos hinausgehende Beschreibungen und Einblicke fehlen fast vollständig. Es zeigt aber die Personen dort im BND, wie sie agieren.

In einem Spannungsfeld aus Menschlichkeit, Gewissen und Verantwortung für ihre externen Quellen einerseits. Sowie der Rechtsstaatlichkeit und der Verpflichtung und Verantwortung gegenüber dem obersten, letztlich Dienstherren, dem Staat andererseits. Und drittens den eigenen Ansprüchen, Besitzdenken, Vorstellungen und Wissen um die Macht und Eigenarten, die ein solcher Apparat irgendwo entwickelt.

In diesem Spannungsfeld agierte jahrelang der Autor und er hat dabei letztlich verloren. Das gibt zu denken.

Verlag: Ullstein Buchverlage
ISBN: 3-550-07605-3, 382 Seiten
ca. 24,00 EUR

! Redaktionelles



„Lass mich in Ruhe“

erscheint monatlich als Informationsmagazin von und über
STOP1984.

Herausgeber und Redaktion:
Twister (Bettina Winsemann)
Kölnstraße 429
53117 Bonn

Kontakt zur Redaktion:
E-Mail: twister@stop1984.com

Wir freuen uns über die Zusendung von Beiträgen - möglichst per E-Mail - an die Redaktionsanschrift. Bei unverlangt eingesandten Bildern und Manuskripten kann keine Gewähr für deren Veröffentlichung übernommen werden. Wird Rücksendung gewünscht, bitte Freiumschlag beifügen.

Hinweis:

***Buchrezensionen sowie Beiträge,
welche explizit mit einem Verfasser benannt sind,
spiegeln nicht automatisch auch die Meinung von STOP1984 wieder.**