H 7625

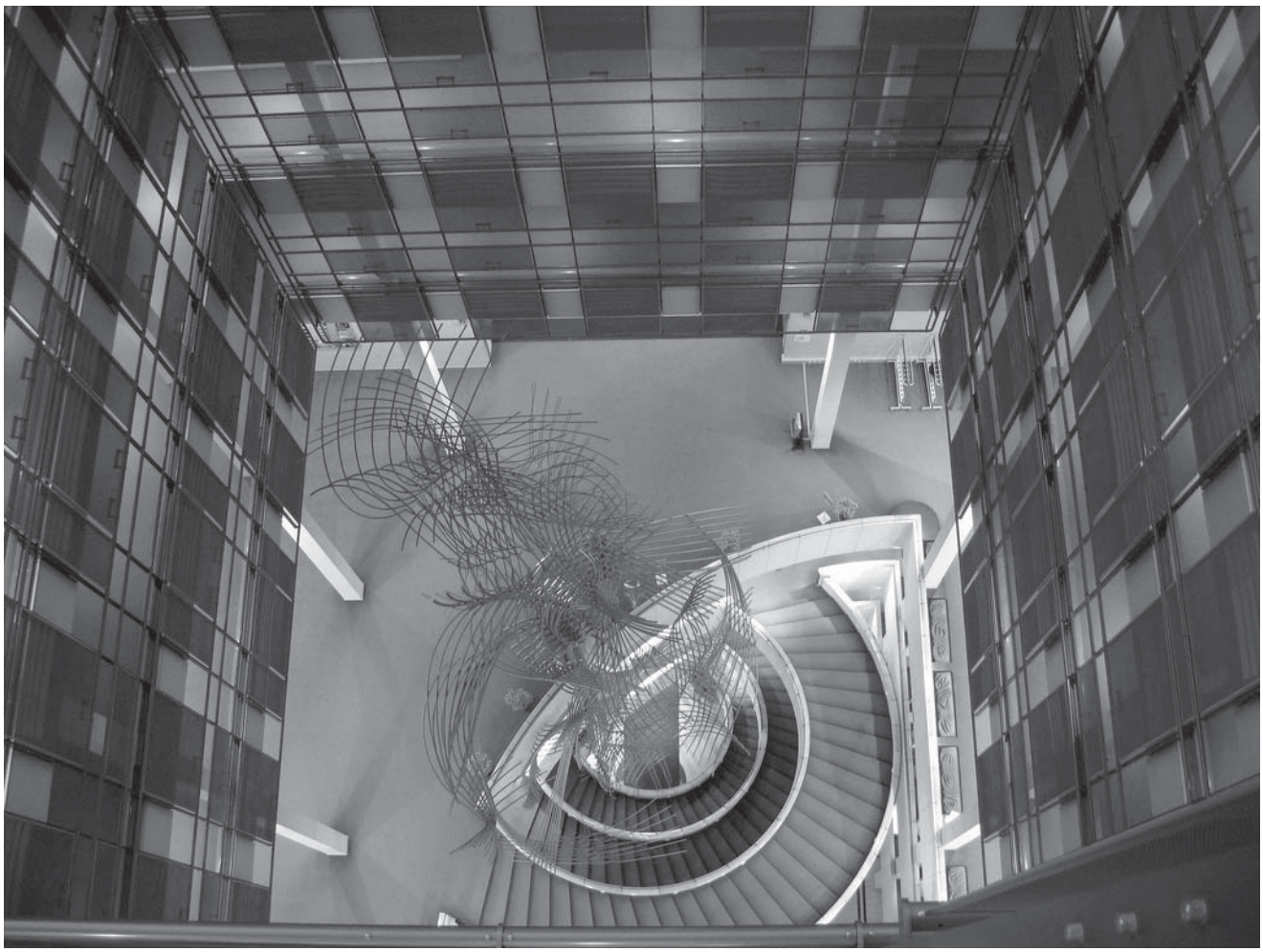
FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

28. Jahrgang 2011 Einzelpreis: 7 EUR

3/2011 – September 2011

IT in Europa



ISSN 0938-3476

• Netzpolitik • Jahrestagung 2011 • Beschäftigtendatenschutz •

FIfF Kommunikation

Titelbild: The Espace Léopold
photo by Lydia González Dios on Flickr – CC BY-NC-SA 3.0

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Inhalt

Ausgabe 3/2011

inhalt

Editorial

Große Ereignisse werfen wieder ihre Schatten voraus – vom 11. bis 13. November 2011 findet in München unsere diesjährige Jahrestagung statt. *Dialektik der Informationssicherheit – Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit*, so der Titel; die Vorschau will darauf neugierig machen und bildet den Anfang dieser Ausgabe der FIfF-Kommunikation.

Europa – in diesem Rahmen werden die wesentlichen politischen Entscheidungen getroffen, die auch die für nationale Politik letztlich maßgebenden Richtlinien festlegen. Viele Entwicklungen der Netzpolitik gehen auf Entscheidungen europäischer Institutionen zurück. Es liegt also nahe, sich mit europäischer IT- und Netzpolitik im Rahmen eines Schwerpunkts zu beschäftigen. In dieser Ausgabe der FIfF-Kommunikation haben wir eine Reihe von Beiträgen zusammengestellt, die unterschiedliche Facetten von Europa beleuchten. Wir behandeln netzpolitische Themen, den Zusammenhang zwischen IT und Arbeit, und Institutionen, die auf europäischer Ebene Einfluss nehmen wollen.

Den Schwerpunkt eröffnet *Stefan Hügel*. In seinem einleitenden Beitrag gibt er einen Überblick über Themen, die in der europäischen Netzpolitik eine Rolle gespielt haben und spielen. Behandelt werden Themen aus den Bereichen Regulierung, Überwachung, Datenschutz, Innen- und Sicherheitspolitik, die in letzter Zeit die Debatten bestimmt haben.

Zentrum europäischer Politik ist das Europäische Parlament. Wir haben Abgeordnete aus dem *Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres* (LIBE), der sich unter anderem mit Datenschutz, Transparenz und Überwachung auseinandersetzt, gebeten, ihre Positionen für uns darzustellen. *Jan Philipp Albrecht* von den Grünen und *Alexander Alvaro* von der FDP haben dies für uns getan – ihre Beiträge sind in dieser Ausgabe nachzulesen.

Digitale Rechte und bürgerliche Freiheiten werden von EDRi – *European Digital Rights* – in Brüssel vertreten. *Tobias Lönnies* hat sich im Rahmen eines Praktikums beim FIfF die Organisation und ihre Mitglieder etwas genauer angesehen. In seiner Untersuchung stellt er die Mitgliedsorganisationen dar: ihre Zusammensetzung, ihre Strukturen und – vor allem – ihre Themen.

„Lassen wir die Fakten sprechen", fordert EDRi-Präsident *Andreas Krisch* in seinem Beitrag. Anhand einer Reihe von Beispielen stellt er dar, dass Gesetzesinitiativen und deren vorgebliche Zielsetzungen bei näherer Betrachtung häufig nicht leicht in Einklang zu bringen sind.

Zur grundlegenden netzpolitischen Frage hat sich die Netzneutralität entwickelt. In Deutschland toben dazu heftige Debatten in der Enquête-Kommission *Internet und digitale Gesellschaft*. Die Niederlande sind hier bereits weiter, und haben Netzneutralität gesetzlich verankert. *Monika Ermert* stellt die Entwicklungen zur Netzneutralität dar – in Europa und darüber hinaus.

Arbeitsplätze in der Informationstechnik galten und gelten vielen als besonders attraktiv. Leider stimmt das nicht bei allen, wie *Sebastian Jekutsch* in seinem Beitrag feststellt. Arbeitsbedingungen von Migranten in der IT in Tschechien – auch dies ist letztlich ein europäisches Thema.

European Parliament, Strasbourg
Foto: Alfredovic, CC BY-SA 3.0

Ein besonders bemerkenswertes Beispiel europäischen Überwachungswahns ist das Projekt INDECT – *Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment* – mit dem Ziel, Werkzeuge für Überwachung und Strafverfolgung bereitzustellen. *Sylvia Johnigk* kritisierte das Projekt im Rahmen eines Vortrags auf dem 27c3 – dem Chaos Communication Congress – im Dezember 2010. Die Protagonisten des Projekts sehen das naturgemäß etwas anders – der Projektbeteiligte *Jan Derkacz*, der bei dem Vortrag anwesend war, nimmt ausführlich aus Sicht der Befürworter Stellung. Seine Stellungnahme und die Replik von *Sylvia Johnigk* und *Kai Nothdurft* bilden den nächsten Beitrag. Darauf folgt, ebenfalls von *Sylvia Johnigk*, ein Projektbericht zur Sicherheitspolitik in der EU.

Auch Bildungspolitik wird in Europa gemacht – der *Bologna-Prozess* ist für die Hochschulen heute bestimmend. *Joerg Zeltner* kommentiert den Bologna-Prozess und seine Folgen für das Studium. Den Abschluss des Schwerpunkts bildet ein weiterer Beitrag von *Sebastian Jekutsch*, der den Weg von Altcomputern aus der Europäischen Union verfolgt hat. Bezug zu Europa hat schließlich auch unsere Retrospektive, in der wir eine Darstellung der europäischen Datenschutz-Richtlinie 95/46/EG wieder abdrucken, die der damalige Bremer Datenschutzbeauftragte *Stefan Walz* 1994 auf der FIfF-Jahrestagung gehalten hat.

Der Datenschutz spielt auch eine zentrale Rolle im aktuellen Teil. *Marie-Theres Tinnefeld* stellt die wesentlichen Knackpunkte der aktuellen Debatte zum Beschäftigten-Datenschutz dar und kommentiert die letzten Entwicklungen. *Armin Schmid* behandelt Callshop-Meetings als Form der politischen Aktion. Dazu gibt es die gewohnten Rubriken – *Ereignis-Log* und *EDRi-Corner* – und von *Göde Both* einen Konferenzbericht von der Tagung *Gender & ICT* in Umeå/Schweden.

Wie jedes Mal wünschen wir unseren Leserinnen und Lesern auch für diese Ausgabe eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Stefan Hügel
für die Redaktion

Dagmar Boedicker für das Orga-Team

Dialektik der Informationssicherheit

Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit

Wir laden ganz herzlich ein zur diesjährigen FIfF-Jahrestagung. Sie wird von Freitag, den 11. November, bis Sonntag, den 13. November 2011, an der Hochschule München in der Lothstr. 64 stattfinden.

Inzwischen ist die Planung weiter gediehen, was niemanden daran hindern soll, das Programm mit Ideen zu Arbeitsgruppen, Ständen oder Aktionen zu bereichern. Der Ablauf hat sich geringfügig geändert, weil die Verleihung des FIfF-Preises leider ausfallen muss, jetzt sieht er so aus:

Programmübersicht FIfF-Jahrestagung 2011	
Freitag, 11. November 2011	
16:30	**Ankunft** Ausstellung/Begleitausstellung
17:15	Grußworte
17:45	**Keynote** von Thomas Petri (Bayerischer Landesbeauftragter für den Datenschutz) »Vorratsdatenspeicherung aus EU-rechtlicher und verfassungsrechtlicher Perspektive«
18:30	Abendessen
19:30	**Podiumsdiskussion** zum Tagungsthema mit • Michael George (Bayerisches Landesamt für Verfassungsschutz) • Prof. Dr. Rainer W. Gerling (IT-Sicherheits- und Datenschutzbeauftragter der Max-Planck-Gesellschaft) • Constanze Kurz (Sprecherin des CCC) • Dr. Thomas Petri (Bayerischer Landesbeauftragter für den Datenschutz) • Enno Rey (Geschäftsführer der IT Sicherheitsfirma ERNW) Moderation: Dagmar Boedicker (FIfF e.V.)

Podiumsdiskussion

Eigene Informationen will jede/r schützen!

- Deutschland hat ein Informationsfreiheits-Gesetz, das den Staat dazu verpflichtet, Interessierten aus der Gesellschaft und den Medien Auskunft zu erteilen. Leider funktioniert es nicht immer so, wie es gedacht ist.
- Unternehmen stecken viel Geld in Produkte und Entwicklungen, den Ertrag dieses geistigen Eigentums möchten sie sich nicht wegnehmen lassen.
- Bürgerinnen und Bürgern ist ihre Privatsphäre wichtig, da soll niemand drin schnüffeln, weder Sicherheitsbehörden noch Unternehmen noch die organisierte Kriminalität (OK).

Samstag, 12. November 2011	
09:30	Ausstellung/Begleitausstellung
10:00	**Arbeitsgruppen** (geplant) AG2 Wenn Daten das Unternehmen verlassen – Wie können mobile Daten abgesichert werden? AG3 Faire Computer (AG zum Filmabend ‚Behind the Screen') AG4 Facebook & Co und meine Daten im WWW AG6 EU Sicherheitspolitik und -forschung AG8 Europäische Vernetzung
13:00	Mittagspause
14:30	**Arbeitsgruppen** (Fortsetzung) AG1 AK Ruin (Rüstung und Informatik) Killerroboter, Cyberwar & Co, die digitale Aufrüstung geht weiter AG5 Data-Mining im Internet – Demo von Maltego, einem Tool zur Verknüpfung und Auswertung von Daten AG7 KRITIS Kritische Infrastrukturen
17:30	Pause
18:00	»Konflikte der IT-Sicherheit in Unternehmen« **Vortrag** von Monika Hansmeier (Sicherheitsbeauftragte in einem DAX-Konzern)
19:00	Abendessen
20:00	**Filmabend** mit Diskussion Behind the Screen – Das Leben meines Computers http://www.behindthescreen.at
22:00	Ausklang im Baal (nahegelegene Kneipe)
Sonntag, 13. November 2011	
10:00	**Vortrag** von Dr. Phillip W. Brunst (FIfF-Studienpreisträger) »Anonymität, Integrität und Vertraulichkeit vs. Strafverfolgung«
11:00	**Mitgliederversammlung des FIfF** (Berichte etc.)
13:00	Pause
14:00	**Mitgliederversammlung** (Wahlen)
15:00	**Konstituierende Vorstandssitzung**
16:00	Ende der Tagung

Es ist Aufgabe jedes Staatswesens, die Sicherheit seiner Bürger zu gewährleisten und Daseinsvorsorge für sie bereitzustellen. Das schließt ein, dass Finanzämter Steuern erheben, ein Ministerium wirtschaftliche Aktivitäten schützt, dass Sicherheitsbehörden der OK vorbeugen und sie bekämpfen, dass ein Staat sein Territorium gegen militärische Bedrohung sichert. Der Staat soll Sicherheitskonzepte beispielsweise für kritische Infrastrukturen entwickeln und sie gegen Angriffe von außen schützen.

Schon Ende der Siebziger wurde deutlich, dass es bei den Atomkraftwerken Interessenskonflikte zwischen dieser Staatsaufgabe und den Abwehrrechten der Bürgerinnen und Bürger gegen den Staat und seine Sicherheitsbehörden gab. Ein Beispiel aus dem Heute ist das Sicherheitskonzept für den inzwischen gestrichenen Transrapid-Bahnhof in München: Weder der Bayerische Rundfunk noch ein Abgeordneter der Grünen erhielten die Information, die sie sich gewünscht hatten. Wer womöglich Information über die Waffensysteme eines Staates unter dem Informationsfreiheits-Gesetz anfordern würde, nun ja ...

Auch Unternehmen haben ein legitimes Interesse daran, entweder eigene Information zu schützen oder vom Staat oder den Bürgerinnen und Bürgern Information zu erhalten: *Scoring* ist wichtig, um nicht auf unbezahlten Rechnungen oder faulen Krediten sitzen zu bleiben. (Wie die Finanzkrise bewiesen hat, ist es kein ausreichendes Mittel gegen spekulative Gier.) Kostspielige eigene Entwicklungen und Produkte sollen Erträge abwerfen, nicht von Konkurrenten geklaut oder vom Staat durch einen gesetzlichen Federstrich zunichte gemacht werden. Produktionssteuerungen sind empfindlich, pfuscht jemand von außen herein, können gewaltige Schäden entstehen. Wenn Kundendaten verloren gehen oder gestohlen werden, kann der Verlust – materiell oder an Renommee – die Existenz des Unternehmens bedrohen. In Deutschland sehen Unternehmen das und sind skeptisch gegenüber dem Cloud-Computing, es sei denn, sie können als kleine Firmen die Hardware- und Software-Infrastruktur gar nicht mehr selbst stemmen.

Wir Menschen haben dazugelernt: Im Idealfall wägen wir sorgfältig ab, bevor wir unsere Daten artig zur Verfügung stellen: Was muss der Staat oder ein Unternehmen über mich wissen? „Ich habe nichts zu verbergen“, gilt bei vielen nur noch für Doofe. Gleichzeitig fordern wir Information: Wie erledigt der Staat seine Aufgaben – in meinem Sinne? Wie kann ich mitbestimmen, wenn starke Interessen sich durchzusetzen drohen und Partizipation gefordert ist? Welche Information wird uns vorenthalten, sowohl durch unsere Regierung als auch durch die *Mediokratie?* Welche Information könnte ich erhalten, wenn *Whistleblower* ihre Stimme erheben? Welches Wissen und welche Kontakte stellen mir soziale Netzwerke oder freie Plattformen wie *Wikipedia* zur Verfügung?

Technik verändert die Machtverhältnisse. So hat auch die Informations- und Kommunikationstechnik das Verhältnis verändert zwischen denen, die Macht und Geld haben, und denen, die nicht über Einfluss, Geld oder technischen Mittel verfügen. Können wir Bürgerinnen und Bürger dieses Ungleichgewicht ausbalancieren? Zwischen frei verfügbaren Informationen, beispielsweise durch Creative Commons, und geistigem Eigentum? Zwischen dem technischen Drohpotenzial im Cyberwar und einer defensiven Anstrengung durch Informationssicherheit?

Arbeitsgruppen und Begleitausstellung

Bis jetzt sind es acht Arbeitsgruppen, weitere AGs oder Änderungen können sich noch ergeben:

AG1: Killerroboter, Cyberwar & Co. – Die digitale Aufrüstung geht weiter

AG2: Wenn Daten das Unternehmen verlassen. Wie können mobile Daten abgesichert werden?

AG3: Faire Computer

AG4: Facebook & Co und meine Daten im WWW

AG5: Data-Mining im Internet – Demonstration eines Werkzeugs (Maltego) zur Verknüpfung und Auswertung von Daten

AG6: EU-Sicherheitspolitik und -forschung

AG7: KRITIS: Interessenskonflikte im Kontext kritischer Infrastrukturen

AG8: Europäische Vernetzung

Kurzbeschreibungen der AGs und ihre Veranstalterinnen oder Veranstalter findet Ihr auf den Seiten 6-9.

Für nicht in den Arbeitsgruppen abgedeckte Themen wird Platz in einer Poster-Session sein, so zum Beispiel zu *Torservers.net* oder zum *Crypto-Chip* der Privacy Foundation. Stände soll es dieses Mal auch von Firmen geben: Eine Unternehmerin wird eine (teil-)Fair-IT-Maus vorstellen; außerdem werden Datenschutz- und IT-Sicherheitsbeauftragte mit Ständen präsent sein. Für den FIfF-Stand können wir noch kreative Vorschläge zu Marketing-Artikeln und -Motiven brauchen, weitere Ideen und Angebote freuen uns natürlich sehr.

Anmelden zum Essen und Trinken

Darüber haben wir mit besonderem Vergnügen beratschlagt. Damit Ihr in den Genuss einer (in jeder Beziehung) nachhaltigen Speisung kommt, sollten wir aber wissen, *wer was wann* essen möchte. Deshalb, und weil auch die Arbeitsgruppen sinnvoll geplant werden wollen, meldet Euch bitte an! Unter *http://fiff.de/2011* steht dafür ein Formular bereit,.

Sonstige leibliche Bedürfnisse

Günstige Übernachtungsmöglichkeiten findet Ihr schon jetzt unter *http://fiff.de/2011*, voraussichtlich wird es aber auch eine Schlafplatzbörse geben, unter http://wiki.fiff.de/FIfF, CategoryJT11. Das ist eine Seite im Mitglieder-Wiki. Ihr kennt das noch nicht? Dann wird's aber Zeit: Schnell anmelden und zugreifen. Und sollte jemand noch nicht FIfF-Mitglied sein: Schnell Mitglied werden! (Für Studierende gibt es eine kostenlose Schnuppermitgliedschaft.)

Die Tagung ist kostenlos, auch für Nicht-Mitglieder. Über eine Spende freuen wir uns und danken schon im Voraus.

Hochschule München, Foto: Dagmar Boedicker

Vorträge

Anonymität, Integrität und Vertraulichkeit vs. Strafverfolgung

Dr. Phillip Brunst
Cybercrime Research Institute, Köln

Der Vortrag beleuchtet die aktuellen rechtlichen Entwicklungen im Zusammenhang mit (insbesondere heimlichen) Zugriffen auf Computerdaten und -systeme durch Strafverfolgungsbehörden. Eingegangen wird dabei besonders auf Gefährdungsaspekte für anonyme Handlungen im Internet und Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen.

Konflikte der IT Sicherheit in Unternehmen

Monika Hansmeier

Die Aufgaben eines IT-Sicherheitsbeauftragten und die anderer Unternehmensbereiche (Beispiel Business) können (scheinbar) konkurrieren und Konflikte hervorrufen, denen im Interesse des Unternehmens begegnet und die gelöst werden müssen.

Es kann passieren, dass IT-Projekte ohne Einbeziehung des IT-Sicherheitsbeauftragten den Anforderungen hinsichtlich IT-Sicherheit nicht genügen. Wird der IT-Sicherheitsbeauftragte erst in einer späteren Phase mit hinzugezogen, können die Projektziele *In Time* und *Budget* vielleicht nicht gehalten werden, da Sicherheitsanforderungen dann schwerer umzusetzen sind. Ein typischer Konflikt ist geboren. Frühzeitige Einbindung der IT-Sicherheit und Begleitung in allen Projektphasen reduzieren dieses Risiko und führen bei Projektabschluss zu einem IT-Produkt, das die Anforderungen des Unternehmens hinsichtlich IT-Sicherheit erfüllt. Der IT-Sicherheitsbeauftragte wird vom Disabler zum Enabler.

Der IT-Sicherheitsbeauftragte kann durch einen formellen Prozess unterstützt und entlastet werden, bei dem das Management die Verantwortung übernimmt, wenn Sicherheitslücken aus ökonomischen oder technischen Gründen nicht zeitnah geschlossen werden können.

Der Vortrag illustriert die genannten Konflikte an praktischen Beispielen.

Arbeitsgruppen

AG1: Killerroboter, Cyberwar & Co. – die digitale Aufrüstung geht weiter

Organisation:
Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ralf E. Streibl

Von den Anfängen der Computertechnik und Informatik bis heute werden deren Errungenschaften militärisch genutzt. Ihre vielfältige und umfassende Verwendung in der Rüstungstechnik einerseits und bei der Planung und Organisation von Kriegen andererseits hat völlig neue Formen der Kriegführung ermöglicht und die Bedrohung durch Kriege um einige perfide Komponenten erweitert. Ein Beispiel sind Killerroboter, die programmiert töten und dabei die Illusion nähren, die eigenen Soldaten könnten verschont bleiben. Ein anderes Beispiel ist das, was unter den verniedlichenden Begriff des *CyberWar* fällt: Propaganda, Spionage, Sabotage mit Mitteln der Informations- und Kommunikationstechnik, um militärische und vor allem auch zivile Infrastruktur des Gegners lahmzulegen.

In der Arbeitsgruppe sollen neue Tendenzen der Verflechtung von Informatik und Rüstung zusammengestellt und kritisch erörtert werden. Als eine Konsequenz könnte die Wiederbelebung des überregionalen FIfF-Arbeitskreises RUIN (Rüstung und Informatik) beraten werden.

Die Arbeitsgruppe wird angeboten von Hans-Jörg Kreowski <*kreo@informatik.uni-bremen.de*>, Dietrich Meyer-Ebrecht <*dme@fiff.de*> und Ralf E. Streibl <*res@fiff.de*>.

AG2: Wenn Daten das Unternehmen verlassen Wie können mobile Daten abgesichert werden?

Organisation:
Rainer W. Gerling

Es entspricht dem Stand der Technik, bestimmte Daten zu verschlüsseln, wenn sie auf mobilen Datenträgern gespeichert werden und das Unternehmen verlassen. Das betrifft personenbezogene und als schützenswert klassifizierte Daten, insbesondere auf USB-Sticks, Smartphones und Notebooks. Es muss sichergestellt sein, dass bei einem Verlust des mobilen Datenträgers Unbefugte nicht auf die Daten zugreifen können.

Wie kann man die berechtigten Interessen der Unternehmen am Schutz der mobilen Daten unter einen Hut bringen mit den Interessen der Beschäftigten, nicht ausspioniert zu werden?

Für die Informationssicherheit Zuständige begegnen in der Praxis staatlichen Regelungen und Eingriffen, die die Einhaltung von Sicherheitsstandards schwierig machen, dazu gehören Verschlüsselungsverbote, Verpflichtungen zur Entschlüsselung und die Kontrolle von Datenträgern beim Grenzübertritt.

- Wie erstellt man eine Unternehmens-Policy die allen Anforderungen gerecht wird?

- Wie konfiguriert man einen Rechner so, dass er überall auf der Welt sicher ist?
  Ist das überhaupt möglich?

Die Arbeitsgruppe wird angeboten von Prof. Dr. Rainer W. Gerling, Datenschutz und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft, München.

AG3: Faire Computer Gibts das?

Organisation:
Sebastian Jekutsch

Green-IT kennen wir inzwischen zur Genüge. Computer können aber nicht nur nicht *green* sein, sondern auch unfair und unsozial, von der Rohstoffgewinnung bis zur Verschrottung. Unfair spart nämlich Geld. Dass wir dabei eigennützig Mitmenschen ausbeuten, die für uns diese Computer herstellen, transportieren, verkaufen und entsorgen, ist leider kein so populäres Thema.

Der Gedanke, faire Produkte anzubieten und zu kaufen, ist inzwischen weit verbreitet, allerdings eher bei Kaffee oder Kleidung. Ein Angebot an fairer IT fehlt. Die Industrie hat sich noch nicht auf den Weg gemacht, faire Computer herzustellen. Wir Konsumenten haben nicht die Wahl – verändern können wir aber durchaus etwas.

Der halbtägige Workshop „Faire Computer" beleuchtet in Vorträgen und Filmausschnitten die Wertschöpfungskette von Computern. Wir suchen und diskutieren Verbesserungsmöglichkeiten in der Gruppe. Material zum Thema wird verteilt. Am Ende wissen wir mehr darüber, wie unser Computer hergestellt wurde und auf was wir beim nächsten Kauf achten sollten. Die Arbeitsgruppe wird angeboten von Sebastian Jekutsch *(sj@fiff.de)*.

AG4: Facebook & Co und meine Daten im WWW

Ein Workshop zur Medienkompetenz mit Tom Siegmund

Jugend forscht gern. Und neue Welten mit Social-Media-Plattformen wie Facebook, Google+ und Twitter wollen erforscht sein. Manchmal wissen die Menschen aber nicht, was sie tun, wenn sie posten, googeln oder teilen. Wenn ihnen etwas gefällt, denken sie nicht immer an morgen.

Andere lassen vielleicht ganz die Finger davon, obwohl Netzwerke und Tools die gewünschten Zwecke durchaus erfüllen, wenn man die Vorteile kennt. Es geht also um Medienkompetenz, um Prävention, statt nur vor Nachteilen des Netzes zu warnen:

- Was sind Daten?
- Was sind meine Daten wert, und wo gehen die denn eigentlich überall hin, in diesem Internet?
- Wie kann ich das steuern?
- Was entsteht Gutes durch meine Neugier und wann geht das individuell zu weit?

Ein Forschungs-Workshop am Vormittag für Jung und Alt, Lernende und Lehrende. Fragen im Voraus erwünscht an Tom Siegmund *(www.weberklaerer.de)*. Tom Siegmund ist Netzwerker und Blogger.

AG5: Data-Mining im Internet

Demonstration von Maltego, einem Werkzeug zur Verknüpfung und Auswertung von Daten

Organisation:
Kai Nothdurft

Viele Menschen geben im Internet personenbezogene Informationen über sich preis, ohne sich bewusst zu sein, wie einfach es ist, diese Daten gezielt auszuwerten und zu nutzen. Man liefert Informationen ab für einen bestimmten Zweck, kann aber kaum absehen, für welche weiteren, oft unerwünschten Zwecke diese außerdem genutzt werden. So lassen sich die Ergebnisse von derartigem Data-Mining dazu missbrauchen, Social-Engineering-Attacken vorzubereiten oder gezielt Personengruppen mit bestimmten Zielprofilen zusammenzustellen.

In diesem Workshop wird das Analyse-Werkzeug *Maltego* vorgestellt, mit dem auch technisch wenig versierte Anwender beliebige Daten abschöpfen, verknüpfen und auswerten können. Anhand von konkreten Beispielen soll gezeigt werden, wie einfach es inzwischen ist, personenbezogene Daten aus dem Internet, etwa von Firmenwebseiten und aus Facebook herauszufiltern und welche Risiken daraus entstehen.

Nähere Infos zu Maltego sind auf der Herstellerseite zu finden: *http://www.paterva.com/web5/*. Die Arbeitsgruppe wird angeboten von Iwan Gulenko *(iwan.goolenko@googlemail.com)*.

AG6: EU-Sicherheitspolitik und -forschung

Organisation:
Sylvia Johnigk

In den letzten Jahren wurde ein Weg eingeschlagen, der Europa in die Richtung eines präventiven Polizeistaats führt. Prävention von Verbrechen, Terrorismus und anderem Bösen in der realen wie in der virtuellen Welt steht im Fokus von Politik und Forschung.

Wenige Länder und Organisationen, vorwiegend große Verteidigungs- und Sicherheitsunternehmen und Organisati-

onen der angewandten Forschung, teilen die Fördermittel unter sich auf, das zeigt eine Untersuchung des EU-Parlaments (EP) zur Sicherheitsforschung im Rahmen des Seventh Framework Programme FP7[1].

Ein großer Anteil der Projekte befasst sich mit Überwachungstechnologie, und die Zusammensetzung der Projekte verhindert, so das EP, "eine breite Reflektion der Auswirkungen dieser Technologien auf die Bevölkerung, die von solchen Technologien betroffen sein wird"[2].

Die technische Entwicklung von Videoüberwachung, dem Monitoring von Internetaktivitäten und der Speicherung von Verbindungsdaten geht einher mit einem neuen EUROPOL-Gesetz, das die Exekutive der EU stärkt und Kompetenzen und Einflussmöglichkeiten der Legislative und Judikative beschneidet. Europa wird zur Festung nach außen (besonders auffällig durch den Ausbau der Grenzschutzorganisation FRONTEX) und zum präventiven Überwachungsstaat nach innen.

Wir suchen nach Möglichkeiten und Alternativen, die diesen Trend umkehren zu Sicherheitsforschung und Politik für die Menschen. Wir wollen Forderungen erarbeiten, die die demokratisch-freiheitlichen Rechte der EU-Bürger dabei mindestens erhalten, wenn nicht verbessern, einschließlich unabhängiger Technikfolgenabschätzung.

Die Arbeitsgruppe wird angeboten von Sylvia Johnigk *sylvia@fiff.de*

1 *http://cordis.europa.eu/fp7/security/home_en.html).*
2 *http://www.europarl.europa.eu/activities/committees/studies/download.do?language=de&file=32851#search=%20REview%20of%20security%20measures)*

AG7: KRITIS
Interessenskonflikte im Kontext kritischer Infrastrukturen

Organisation:
Claus Stark und Bernhard C. Witt

„Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden", so die offizielle Definition zu kritischen Infrastrukturen. Bereiche wie Transport und Verkehr, Energieversorgung, Informations- und Telekommunikationstechnik, Wasserversorgung, Finanzwesen, Gesundheitswesen und der Katastrophenschutz zählen zu diesen kritischen Infrastrukturen (KRITIS). Deren Ausfall oder Beeinträchtigung kann beispielsweise durch Naturereignisse, technisches oder menschliches Versagen, durch Sabotage, Terrorismus oder Krieg nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen des gesellschaftlichen Miteinanders oder andere dramatische Folgen haben.

Die – gerade auch im Kontext von KRITIS – eingesetzten IT-Systeme sind hochgradig miteinander vernetzt und durchdringen zunehmend mehr Bereiche des Alltags, insofern gebührt der kritischen Informations- und Kommunikationsinfrastruktur eine besondere Aufmerksamkeit. Ausfälle und Fehlfunktionen von und Angriffe auf kritische Informations- und Kommunikationssysteme können verheerende Folgen für die Gesellschaft haben. Es ist daher von gesellschaftlichem Interesse, dass IKT-Systeme wirksam geschützt werden. Infolge des technischen Fortschritts und des variantenreichen Einsatzes entsprechender Techniken existieren jedoch eine Vielzahl von Angriffsvektoren und Verletzlichkeiten. Gerade der Stuxnet-Angriff auf eine isolierte Atomanlage hat vor Augen geführt, dass wir es mit einer realen Gefahr zu tun haben. Grundsätzlich unterliegen alle kritischen Einrichtungen permanenten Angriffen der Spaß-Guerilla, von Hacktivisten, dem organisierten Verbrechen sowie Terroristen.

Die bisherigen Angriffe auf kritische Einrichtungen haben deutlich gemacht, wie leicht Sicherheitsmaßnahmen von Angreifern umgangen werden können und wie erstaunlich wenig die Informationssicherheit dem oft entgegenzusetzen hat. Die Kreativität der Angreifer, die Komplexität der Systeme und die Arglosigkeit der Menschen scheinen oft alle Schutzbemühungen zu vereiteln. Die aufgebauten Strukturen wirken daher durchaus zerbrechlich. Die Diskussion unter zuständigen KRITIS-Beteiligten wird aufgrund der besonderen Bedeutung i.d.R. nicht öffentlich, sondern vertraulich geführt, eine breite gesellschaftliche Diskussion und Beteiligung sind so nur schwer möglich. Die Folgen der Atom-Katastrophe in Japan zeigen aber auch, dass es vielleicht gerade jetzt an der Zeit ist, über diese Fragen grundsätzlich und öffentlich zu diskutieren.

- Im Workshop sollen aktuelle KRITIS-Aktivitäten vorgestellt und dabei die Rolle der Informationssicherheit kritisch hinterfragt werden.
- Welchen Konflikten sind Manager für die Informationssicherheit kritischer Infrastrukturen in der Praxis ausgesetzt?
- Welche der kritischen Infrastrukturen sind warum und wie schützenswert?
- Können komplexe gesellschaftliche Strukturen mit noch komplexeren Sicherheitsmethoden überhaupt ausreichend geschützt werden?
- Ist ein angemessener Schutz nur auf Kosten einer verstärkten Überwachung des Einzelnen möglich? Oder wäre es unter gewissen Umständen besser, KRITIS-Strukturen wieder so zu vereinfachen, dass sie robuster gegen Störungen sind und eine Fehlfunktion oder ein Angriff nicht zur Katastrophe führen kann?

Die Arbeitsgruppe wird angeboten von Claus Stark *(claus@fiff.de)* und Bernhard C. Witt (Sprecher der GI-Fachgruppe Management von Informationssicherheit, *bcw@bc-witt.de*).

AG8: Europäische Vernetzung

Organisation:
Stefan Hügel, Dietrich-Meyer-Ebrecht, Jens Rinne

Auch wenn sich die politische Berichterstattung immer noch stark auf die nationale Sicht konzentriert – wesentliche Entscheidungen, auch in der Netzpolitik, werden seit längerer Zeit in Brüssel und Straßburg getroffen. Aktuelle Themen wie Vorratsdatenspeicherung, Netzsperren, Datenschutz basieren letztlich auf europäischen (Regierungs-) Initiativen. Die Vorratsdatenspeicherung, deren Umsetzung in Deutschland als verfassungswidrig verworfen wurde, geht auf die europäische Richtlinie 2006/24/EG zurück – für die Nichtumsetzung sieht sich die deutsche Regierung einem Vertragsverletzungs-Verfahren gegenüber. Wenn aber die wesentlichen Entscheidungen auf europäischer Ebene getroffen werden, ist es entscheidend für netzpolitische Initiativen, dass sie sich europaweit vernetzen.

Das ist die Ausgangslage für diesen Workshop. Wir wollen zunächst darstellen, wie auf europäischer Ebene Entscheidungen getroffen werden:

- Welche Organe gibt es?
- Wie arbeiten sie zusammen?
- Wer nimmt Einfluss auf die Entscheidungen – Lobby-Verbände und nationale Regierungen?
- Wie transparent ist diese Entscheidungsfindung?

Um in Europa netzpolitisch mitwirken zu können, wurde bereits 2002 EDRi gegründet – European Digital Rights. Das FIfF ist seit 2004 Mitglied dieses Verbandes. Wir wollen vorstellen, wie EDRi arbeitet, welche Organisationen dort Mitglied sind, und welche Erfolge wir bereits feiern durften.

Unser Ziel ist es, unsere Aktivitäten auf der europäischen Ebene zu verstärken – die EDRi-Arbeit besser zu unterstützen. Das wollen wir nach den einführenden Referaten gemeinsam erarbeiten:

- Welche Möglichkeiten hat das FIfF, auf europäischer Ebene mitzuwirken?

Das FIfF hat viele kompetente Mitglieder, deren Kenntnisse und Fähigkeiten hier gefragt sind.

- Wie können wir dieses Potential besser nutzen, um europäische Initiativen zu unterstützen?
- Welche Informationen benötigen wir dafür?
- Brauchen wir andere Strukturen?
- Und nicht zuletzt: Wer im FIfF kann dabei mitarbeiten, ihre und seine Kompetenz dabei einbringen?

Wir planen dabei auch, Repräsentanten aus anderen Ländern der EU einzuladen und gemeinsam mit ihnen Möglichkeiten der Zusammenarbeit zu diskutieren.

Wenn wir auf Entwicklungen erst reagieren, wenn sie auf der nationalen Ebene angekommen sind, ist es häufig zu spät noch etwas zu bewegen. Deswegen ist ein stärkeres europäisches Engagement für das FIfF sinnvoll und wichtig.

Die Arbeitsgruppe wird angeboten von Stefan Hügel *(sh@fiff.de)*, Jens Rinne *(rinne@fiff.de)* und Dietrich Meyer-Ebrecht *(dme@fiff.de)*.

Einladung zur Mitgliederversammlung 2011

des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e.V.)

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2011 ein.

Sie findet statt am Sonntag, den 13. November 2011, von 11:00 bis 15:00 Uhr
in der Hochschule für angewandte Wissenschaften, Lothstraße 64, München

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl des Vorstands
8. Neuwahl der Kassenprüfer
9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen
10. Berichte aus den Regionalgruppen
11. Anträge an die Mitgliederversammlung
    Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein
12. Verschiedenes

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FIfF

Dialektik der Informationssicherheit

Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit

Vorträge:

»Vorratsdatenspeicherung aus EU-rechtlicher und verfassungsrechtlicher Perspektive«
»Konflikte der IT-Sicherheit in Unternehmen«
»Anonymität, Integrität und Vertraulichkeit vs. Strafverfolgung«

Podiumsdiskussion:
»Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit«

Rainer W. Gerling
Constanze Kurz
Thomas Petri
Enno Rey

Workshops:

Data Mining im Internet
EU Sicherheitspolitik
Fair IT
Kritische Infrastrukturen
Krypto auf Reisen
Rüstung und Informatik (AK Ruin)
Web 2.0

Filmabend:

»Behind the Screen – Das Leben meines Computers«

FIfF-Jahrestagung

in Kooperation mit der

Hochschule München

Lothstraße 64

11. bis 13. November 2011

HOCHSCHULE
FÜR ANGEWANDTE
WISSENSCHAFTEN
MÜNCHEN

Die Tagung ist öffentlich, die Teilnahme ist kostenfrei.
Anmeldung bitte unter 2011@fiff.de
Nähere Informationen unter http://fiff.de/2011

V.i.S.d.P. FIfF – Forum InformatikerInnen
für Frieden und gesellschaftliche Verantwortung e.V.,
Goetheplatz 4, D-28203 Bremen

FIfF

„Das Internet war's!“

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

fassungslos stehen wir vor dem Massaker in Norwegen. Erneut hat sich gezeigt, wozu rechter Terror in der Lage ist. Unsere Gedanken sind bei den Opfern dieses furchtbaren Anschlags.

Gleichzeitig ist es bewundernswert, wie die Menschen in Norwegen damit umgehen. Gerade bei solchen Ereignissen müssen wir dafür sorgen, dass es den Terroristen nicht gelingt, unsere offene, demokratische Gesellschaft zu zerstören.

Das bedeutet selbstverständlich nicht, den Angreifern wehrlos gegenüber zu stehen. Doch Bürgerrechte sind keine Schönwetterrechte. Sie müssen sich gerade dann bewähren, wenn unsere freiheitliche Gesellschaft von jenen angegriffen wird, die dieses Wertesystem ablehnen. Sonst verhilft man ihnen noch nachträglich zum Erfolg.

Doch nicht alle haben diese Botschaft begriffen. Wie *Kavalleriepferde beim Hornsignal* stehen sie bereit, um wieder ihre alten Forderungen vorzutragen: *Schärfere Gesetze! Mehr Überwachung! Härtere Strafen!* So hören wir es (nicht nur) von konservativen Innen- und Sicherheitspolitikern. Und immer wieder im Mittelpunkt: das Internet.

„*Im Internet geboren*“ sei Breiviks Tat, so hören wir, und flugs folgt die Forderung: „*Vorratsdatenspeicherung!*“ Andere fordern, anonymes Auftreten im Internet zu untersagen. Eine Datenbank *auffälliger Personen* müsse eingerichtet werden. Dass der Nutzen der Vorratsdatenspeicherung für eine effektive Strafverfolgung sehr zweifelhaft ist (die verursachte Einschränkung der Bürgerrechte dagegen offensichtlich), und dass so mancher Prediger von Rassismus und rechtem Hass seine Identität durchaus nicht verbirgt – und bei nicht Wenigen Zustimmung findet –, solche Widersprüche zählen nicht.

Sobald irgendetwas passiert – seien es terroristische Anschläge, seien es Ausschreitungen wie in England: Scheinbar war es immer das Internet. Die Täter hätten sich über das Internet koordiniert, sie hätten ihre Taten im Internet angekündigt. Ist das immer noch der Reiz des vermeintlich Neuen, Unbekannten, oder soll der Boden bereitet werden für ein anderes Internet: kontrolliert und von missliebigen Inhalten gereinigt? Schon gibt es Überlegungen für ein *virtuelles Schengen*, eine europäische Internet-Außengrenze, an der unerlaubte Inhalte abgewehrt werden können.

Europa, so ist auch dieses Heft überschrieben. Für einige immer noch ein unbekanntes Wesen, und von manchen immer wieder in Frage gestellt, ist Europa doch die Ebene, auf der die meisten politischen Weichen gestellt werden. Politische Berichterstattung und politisches Engagement scheinen sich aber immer noch stärker im nationalen Rahmen als auf europäischer Ebene zu bewegen. Selbst bei einem europäischen Ereignis wie der Wahl zum Europäischen Parlament werden eher die Auswirkungen auf die nächste Bundestagswahl diskutiert als das Ergebnis der Wahl selbst. *Ralf Bendrath* stellte in den *Blättern für deutsche und internationale Politik* (4/2010) fest, die europäische Öffentlichkeit kranke daran, „dass sie massenmedial aus nationalen Öffentlichkeiten besteht – und nur auf die reagieren nationale Regierungen.“ Er fordert eine europäische Bürgerbewegung – diese Ausgabe der FIfF-Kommunikation will beitragen, den Boden dafür zu bereiten.

Ein Thema, das derzeit sowohl auf europäischer Ebene als auch in Deutschland diskutiert wird, ist der Datenschutz. Die in die Jahre gekommene Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995 soll überarbeitet werden – das FIfF hat sich mit vielen anderen bürgerrechtlichen Organisationen an der öffentlichen Konsultation beteiligt – wir berichteten darüber (*FIfF-Kommunikation 1/2011*). Gleichzeitig wird in Deutschland der Beschäftigtendatenschutz (§32 BDSG) überarbeitet. Letztes Jahr war er zentrales Thema unserer Jahrestagung, die wir gemeinsam mit der *Deutschen Vereinigung für Datenschutz* (DVD) in Köln durchgeführt haben. *Marie-Theres Tinnefeld* hielt damals den Hauptvortrag zu diesem Thema; in dieser Ausgabe stellt sie für uns die entscheidenden Fragestellungen und die aktuellen Entwicklungen seit damals dar. Wir sollten dieses Thema weiter wachsam verfolgen.

Mit dem Datenschutz werden wir uns auch bei unserer Jahrestagung beschäftigen: Sie findet statt vom 11. bis 13. November 2011 an der Hochschule München. *Dialektik der Informationssicherheit – Interessenskonflikte bei Vertraulichkeit, Anonymität, Integrität* ist sie betitelt und verspricht spannende Diskussionen:

> *„Die umfassende Computerisierung der Gesellschaft hat insbesondere durch die allgegenwärtige Nutzung des Internets im Privatbereich, im Geschäftsleben und in Behörden mit ihren Verwaltungsprozessen die Sicherheit von Information zu einer zentralen gesellschaftlichen Herausforderung werden lassen. Interessenskonflikte finden sich auf allen Ebenen. Wir reden darüber.“*

Vielen Dank schon jetzt an die Organisatorinnen und Organisatoren der Tagung, auf die wir uns freuen können.

Mit FIfFigen Grüßen

Stefan Hügel

Raffael Rittmeier

How To FIfF

oder wie das FIfF funktionieren sollte

Unabhängig davon, wie das FIfF funktioniert, haben wir wohl alle eine Meinung darüber, wie es funktionieren sollte, oder? Meiner Meinung nach ist ein gutes Zusammenspiel zwischen den Mitgliedern und den unterschiedlichen Organen des Vereins notwendig. Ein Blick in die Satzung [1] zeigt, dass das FIfF seine Ziele u.a. durch die „fachliche und wissenschaftliche Unterstützung von regionalen Gruppen und Initiativen" erreichen will – es gibt also sowohl regionale als auch inhaltliche Schwerpunkte. Ein integraler Bestandteil des Vereins ist die Geschäftsstelle, die für die organisatorischen Arbeiten zuständig ist und die den Arbeitsgruppen bzw. dem Vorstand zuarbeitet. Darüber hinaus werden in der Satzung auch der Beirat und ein Regionalrat erwähnt – doch dazu mehr in einem späteren Beitrag.

Teil 1: die Regionalgruppen

Regionalgruppen sind ein wichtiger Bestandteil des FIfF. Sie sind regionale Zusammenschlüsse von Menschen, denen die Ziele des FIfF wichtig sind und die sich über entsprechende Themen austauschen wollen. Regionalgruppen müssen nicht auf FIfF-Mitglieder beschränkt sein und sind es in der Regel auch nicht. Andere Organisationen haben eine ähnliche Struktur: der CCC mit seinen Chaostreffs/Erfa-Kreisen und der Arbeitskreis Vorratsdatenspeicherung mit seinen Ortsgruppen.

Aktive Regionalgruppen des FIfF gibt es derzeit in Bremen, Hamburg, Köln und München. Dort treffen Menschen in regelmäßigen oder unregelmäßigen Abständen zusammen, tauschen sich über aktuelle Ereignisse aus, organisieren Veranstaltungen oder Aktionen. In weiteren Regionen gibt es regionale Ansprechpartner.

Doch was, wenn es in Eurer Region keine Regionalgruppe gibt? Wir können Euch bei der Gründung einer Regionalgruppe unterstützen. Wichtig ist, Gleichgesinnte zu finden und ein erstes Treffen zu organisieren. Unsere Geschäftsstelle kann bei der Einladung behilflich sein und diese an die Mitglieder in der Region verschicken. Ihr könnt Euch auch einfach mit Ideen oder Zielen melden: *fiff@fiff.de* oder ruft uns im Büro während der Geschäftszeiten an.

In Teil 2 der Reihe How To FIfF schreibe ich über Initiativen und Arbeitsgruppen im FIfF. Anmerkungen und Kritik sind ebenso gerne gesehen wie eigene Berichte oder Leserbriefe: *redaktion@fiff.de*.

Aktuelles aus der Bremer Regionalgruppe

Am 23. Juni 2011 haben wir eine Veranstaltung mit Diskussion und Kurzvorträgen unter der Überschrift „Ist der Schutz der Privatsphäre technisch und gesellschaftlich überholt?" organisiert. Herbert Kubicek, Bernard Robben und Gilljen Theisohn hatten sich bereit erklärt, kurze Beiträge vorzubereiten. Im Kurzschluss, einem selbst organisierten Café [2], haben sich dann knapp 20 Interessierte eingefunden, u.a. auch Mitglieder vom FoeBuD und dem CCC. Gilljen Theisohn berichtete von ihren datenschutz(un)rechtlichen Erfahrungen als Anwältin. Herbert Kubicek sprach über Soziale Netzwerke und teilte Forschungsergebnisse aus dem Bereich der eID-Funktionalitäten in Ausweisdokumenten mit uns. In der Diskussion wurde unter anderem die Scoring-Branche (Wirtschaftsauskunfteien) für ihre Datensammelwut kritisiert.

Den Beitrag von Bernd Robben drucken wir im Folgenden für Euch ab.

[1] http://fiff.de/about/satzung
[2] http://www.kurzschluss-bremen.de/

Raffael Rittmeier

Raffael Rittmeier hat Computer Security and Forensics an der University of Canterbury in Christchurch, Neuseeland, und Informatik an der Universität Bremen studiert und ist in der Regionalgruppe Bremen und im Vorstand des FIfF aktiv.

Bernd Robben

Ist der Schutz der Privatsphäre technisch und gesellschaftlich überholt?

Um mich der Frage zu nähern, die zum Thema der Veranstaltung gemacht wurde, habe ich überlegt, was da gefragt ist. Was bedeuten die einzelnen Wörter Schutz, Privatsphäre, technisch, gesellschaftlich eigentlich? Meine Reflexionen darüber habe ich in sieben Punkten zusammengefasst.

1

Beginnen möchte ich mit dem letzten Wort der Frage: *überholt*. Gemeint scheint, dass so etwas wie Privatsphäre im Zeitalter von SchülerVZ und Facebook antiquiert ist. Das erinnert mich an eine für mich prägende Lektüre, als ich begann, Informatik zu studieren. Das Buch ist schon älter: Günther Anders: Die Antiquiertheit des Menschen. Anders schrieb die Aufsätze dieses zweibändigen Werks unter dem Eindruck des Abwurfs der Atombomben auf Hiroshima und Nagasaki. Die Menschheit konnte sich durch die eigene, selbst geschaffene Technik völlig vernichten. Die Antiquiertheit des Menschen analysiert Anders in der Haltung einer prometheischen Scham. Der Mensch schämt sich *vor* seinen Produkten (nicht *wegen* der in die Welt gesetzten Produkte). Darin wird der Mensch antiquiert, was Anders an vielen Kategorien zeigt, unter anderem an der Privatheit. 1958 schreibt er:

> *„§1 Nicht nur gilt: Die Welt wird ins Haus geliefert, sondern auch: Das Haus wird der Welt ausgeliefert."*

Er bezieht sich dabei auf Rundfunk und Fernsehen, welche die Welt zum Phantom und zur Matrize machen. Im US-TV laufen schon zu der Zeit Shows, die das Private in die Öffentlichkeit zerren. Aber die Auslieferung des Privaten zeigt sich auch totalitärer:

- Zwischen 1940 und 1957 werden in Los Angeles mehr als 1000 Gebäude mit Abhörinstallationen versehen.
- 1952 beauftragten die Gerichte der Vereinigten Staaten von Amerika die Polizei, 58.000 Personen, Firmen und Vereine abzuhören.
- Offiziell wird geschätzt, dass dies etwa ein Fünftel der „legalen" Abhörungen ausmacht. Hauptsächlich wird also privat untereinander geschnüffelt.

2

George Orwells 1949 erschienener Roman „*1984*" malte die Bedrohung der Privatsphäre durch den *Big Brother* – das überall hinschauende Auge und Ohr des Diktators – im Überwachungsstaat drastisch aus. Im wirklichen Jahr 1984 warnte das FIfF vor dem gläsernen Menschen und organisierte drei Jahre später ziemlich erfolgreich zusammen mit anderen gesellschaftlichen Gruppen eine Kampagne zum Boykott der Volkszählung 1987. Aus der Perspektive von heute wirkt das alles ziemlich überholt – ja dieses Zentralauge des Big Brother erscheint geradezu lächerlich gegenüber den vielfältigen Technologien, die heutzutage in jede einzelne Faser der Privatsphäre eindringen und nach dem terroristischen Anschlag vom 11. September 2001 geradezu hysterisch gefördert und eingesetzt werden, wie die Überwachung und Speicherung aller Flugdaten; das Speichern von Kundendaten im Kaufhaus, woraus mit Techniken des Data Minings genaue Kundenprofile erstellt werden; RFID-Techniken zur Identifizierung von allem und jedem; Gen-Datenbanken und biometrische Datenbanken; E-Mail Überwachung und Internet-basierte Spionage über Cookies und Trojaner; Erstellung genauer Bewegungsprofile, insbesondere durch Handy-Ortung – wie sie gerade flächendeckend in Dresden angesichts einer Anti-Nazi-Demo angewandt wurde.

3

Bisher habe ich Bilder ausgemalt, wie das Private überholt zu sein scheint, weil es Bedrohungen durch die Technik des Menschen ausgesetzt ist, habe aber noch gar nicht erklärt, was Privatsphäre ist. Meine erste Annäherung an Definitionen vollziehe ich immer durch einen Blick in das Grimmsche Wörterbuch der deutschen Sprache. Zum Stichwort *privat* findet sich dort unter anderem: „amtlos, besonder, geheim, unöffentlich, persönlich, häuslich, überhaupt dem amtlichen öffentlichen, allgemeinen, gemeinsamen entgegengesetzt; im 16. Jh. aus lat. *privatus* entlehnt". (Vgl. das lateinische-, Verb: *privare* rauben, befreien). Aufgelistet werden zunächst nicht positive Bestimmungen, in denen das Private anklingt, sondern Abgrenzungen. Mir wird langsam klar: Das Private hat keinen exakt zu definierenden Kern, den man schützen oder bewahren kann. Privatheit lässt sich nur in Differenz zu Öffentlichkeit definieren.

4

Seltsamerweise lässt dieser öffnende Blick in ein altes Wörterbuch die von Katastrophenstimmung geprägte Redeweise von der Antiquiertheit des Menschen selbst etwas antiquiert erscheinen. Dass die Privatsphäre überholt wird, scheint normal zu sein:

> *„Wir sprechen von Öffentlichkeit und Privatsphäre wie von etwas Feststehendem, weil man sich auf diese Weise besser verständigen kann. In Wirklichkeit freilich handelt es sich um komplexe, in dauernder Wandlung begriffene Phänomene."*

analysierte Richard Senett 1977 in seinem Buch „Fall of Public Man". Die deutsche Ausgabe hat den Titel „Verfall und Ende des öffentlichen Lebens – Die Tyrannei der Intimität". Noch bekannter zum Thema ist hier vielleicht Jürgen Habermas' berühmte Studie zum Strukturwandel der Öffentlichkeit.

5

Die Privatsphäre wird technisch und gesellschaftlich in Relation zur öffentlichen Sphäre ständig neu produziert. Das ist ein

Prozess, in dem sich beide gegenseitig überholen. Durch diesen reflexiven Produktionsprozess des sich Wandelns und Transformierens wird die fundamentalistische Redeweise von der Antiquiertheit des Menschen in Scham vor seiner selbst produzierten Technik überholt. Irgendwie steckte hinter dieser Sichtweise die Vorstellung, dass das Eigentliche des Menschen nicht technisch sei – was ein Schmarren ist.

Fruchtbarer finde ich heute Denkansätze, die betonen, dass das technische Medium selbst eine Botschaft ist. Schöner drückt es Walter Benjamin aus:

> *„Innerhalb großer geschichtlicher Zeiträume verändert sich mit der gesamten Daseinsweise der menschlichen Kollektiva auch die Art und Weise ihrer Wahrnehmung."*

Das heißt zugespitzt und holzschnittartig ausgedrückt: In oralen Kulturen der Face-to-Face-Kommunikation, bei der jeder jeden kennt, kann sich eine Öffentlichkeit nur schwer herausbilden. Der private Tratsch durchlöchert sie ständig. In Schriftkulturen mit ihren festgeschriebenen Gesetzen bildet sich die Scheidung zwischen Privatheit und Öffentlichkeit scharf heraus. Dadurch ist unsere Vorstellung der Privatsphäre geprägt.

In der globalen Wissensgesellschaft bildet sich das erste Mal eine globale Privatheit: Anders als bei Brieffreundschaften kann sie im Internet in Echtzeit gelebt werden.

Globalisierte Privatsphären führen aber nicht zur Homogenisierung der Privatsphäre – wie der im Schriftdenken verwurzelte Theoretiker die These sofort missversteht. Etwa die private Gemeinschaft der Briefmarkensammler über das Web 2.0 in China, Argentinien, Philippinen und Finnland bedeutet nicht, dass die Vorstellung von Privatheit und Intimität in diesen Ländern durch derartige gesellschaftliche Transformationen gleich würden. Im Gegenteil: Es bilden sich neue Fraktionierungen und lokal geprägte Welten der Privatheit.

6

Überholen müssen wir die Vorstellung, die richtige und gute Ausbildung der Beziehung zwischen Privatsphäre und Öffentlichkeit sei in erste Linie eine Abwehrschlacht gegen den technisch sich hochrüstenden großen Bruder:

- Web-2.0-Technologien erweitern die Möglichkeiten für private Gemeinschaften. Und es ist sehr die Frage, was zukünftige Arbeitgeber mehr stört, die heißen Fotos von wilden Festen oder das Fehlen von interessanten Einträgen – was doch auf eine langweilige Person mit mangelnder kommunikativer Kompetenz schließen lässt.

- Web-2.0-Technologien sind Basistechnologien zur Mobilisierung von politischen Bewegungen geworden. Beispielhaft galt das für die iranische Oppositionsbewegung anlässlich der letzten Wahlen in diesem Land und gilt vielleicht noch deutlicher für die demokratischen Bewegungen im heutigen Tunesien, Ägypten, Syrien usw.

7

Was folgt aus diesen Überlegungen für das FIfF und für unsere Ausgangsfrage: Ist der Schutz der Privatsphäre technisch und gesellschaftlich überholt?

- Ich wünsche mir für das FIfF eine Haltung wie das Bundesverfassungsgericht sie zum Volkszählungsurteil 1983 eingenommen hat, indem es das informationelle Selbstbestimmungsrecht als eine Ausprägung des allgemeinen Persönlichkeitsrechts und als ein Grundrecht anerkannte. Ich wünsche mir vor allem solche Kreativität bei neuen Situationen, wie sie Wilhelm Steinmüller und Bernd Lutterbeck in den 70er Jahren an den Tag legten, als sie in einem Gutachten den Terminus „informationelles Selbstbestimmungsrecht" erfanden. Sie sahen voraus, dass die Privatsphäre künftig vor den Zugriffen der Informations- und Kommunikationstechnologien anders zu schützen ist als vor den Angriffen einer Bürokratie, die auf Basis von Aktenordnern und Karteikästen arbeitet. Für mich ist also ganz klar, dass der Schutz der Privatsphäre nicht überholt, sondern hoch aktuell ist. Die Frage ist bloß, was wir darunter verstehen.

- Auf jeden Fall gilt, dass das FIfF gesellschaftliche Kämpfe gegen Vorratsdatenspeicherung und allgemeine Videoüberwachung weiterhin zusammen mit anderen organisieren muss. Auf diesem Feld ist das FIfF relativ gut. Meines Erachtens ist aber auch erforderlich, dass das FIfF Vorschläge zur Gestaltung von Informations- und Kommunikationstechnologien erarbeiten muss – etwa zur besseren Nutzbarkeit von Web-2.0-Technologien zur geselligen privaten Nutzung und zum effizienten Einsatz für politische Bewegungen. In diesem zweiten Bereich hat das FIfF einigen Nachholbedarf und muss etwas tun, wenn es nicht von den sich vollziehenden Veränderungen überholt werden will. Auf diesem Feld wirkt das FIfF bisher ziemlich antiquiert.

Bernd Robben

Bernd Robben ist wissenschaftlicher Mitarbeiter in der Informatik-AG *Digitale Medien in der Bildung* der Universität Bremen.

- Von zentraler Bedeutung ist meines Erachtens, zu begreifen, dass die Beziehung zwischen Privatheit und Öffentlichkeit ein Prozess ist, ein Prozess, der sich in zugleich technischen und sozialen Medien bildet. Wenn ich hier davon spreche, dass dieser Prozess sich in den (und nicht durch die) Medien bildet, will ich damit ausdrücken, dass wir alle reflexiv in diesen Prozess eingebunden sind. Er prägt uns, und wir sollten ihn mitgestalten. Aber weil wir ihm unterworfen sind, können wir ihn nicht beliebig manipulieren.

Dieter Wöhrle und Wolfram Thiemann

Appell zur Umbenennung des *Fritz-Haber-Instituts* der Max-Planck-Gesellschaft

In diesem Jahr feiert das ehemalige Kaiser-Wilhelm-Institut für Physikalische Chemie und Elektrochemie *und jetzige* Fritz-Haber-Institut *der Max-Planck-Gesellschaft (MPG) in Berlin sein hundertjähriges Bestehen. Die Bedeutung des Instituts und die wissenschaftlichen Leistungen der Mitarbeiter/innen wurden durch Nobelpreise (zuletzt der Nobelpreis für Chemie 2007 an G. Ertl) und zahlreiche weitere Wissenschaftspreise gewürdigt.*

Jedoch in wenigen anderen Wissenschaftlern vereinen sich Nutzen der Wissenschaft für die Menschheit – die Erfindung der Ammoniaksynthese für die Düngemittelherstellung – und Missbrauch der Wissenschaft in so extremen Maße wie bei Fritz Haber: Mit seinen Forschungsarbeiten und seinen politischen Ambitionen hat Haber eines der schrecklichsten Kapitel der Kriegsführung, die Anwendung chemischer Waffen, eingeläutet.[1] [2]

Es wird Zeit, dass wir als verantwortliche Wissenschaftler auch der dunklen Seite des Nobelpreisträgers Fritz Haber Rechnung zollen: Das Chemiewaffenübereinkommen von 1997 und der Verhaltenskodex der Gesellschaft Deutscher Chemiker lassen den Namen „Fritz-Haber-Institut" nicht mehr länger vertretbar erscheinen. Die Umbenennung des Instituts wäre eine mutige Konsequenz. Für das renommierte Institut könnte das im Oktober dieses Jahres anstehende hundertjährige Jubiläum seiner Gründung ein würdiger Anlass sein. Dafür möchten wir uns einsetzen.

Der Appell zur Umbenennung des Fritz-Haber-Instituts wird inzwischen von vielen Organisationen mitgetragen, so auch vom FIfF. Wenn auch Sie den Appell unterstützen wollen, wenden Sie sich bitte an die Initiatoren *woehrle@uni-bremen.de* oder *thiemann@uni-bremen.de,* FB-02 der Universität Bremen. Links zu Materialien finden Sie auf der Internet-Seite *www.fritz-haber-und-cwaffen.de*.

Anmerkungen

1 *Wöhrle D und Thiemann W: „Der Chemiker Fritz Haber. Anerkannte Wissenschaft und Etablierung eines Massenvernichtungsmittels", Wissenschaft und Frieden 29 (1/2011) S. 45—49*

2 *Wöhrle D: „Fritz Haber und Clara Immerwahr", Chemie in unserer Zeit, 44, S. 30—39*

Stefan Hügel

Ereignis-Log 3/2011

Events, Incidents und **Problems** der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung kann nicht vollständig sein; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

Mai 2011

14. Mai 2011: Im US-Senat haben Senatoren beider Parteien eine neue Fassung des Gesetzes *PROTECT IP (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property)* eingebracht, das die rechtliche Grundlage liefern soll für Internet-Sperren, Beschlagnahme von Domains, Sperrungen von Konten und Zensur bei Web-Dienstleistern und Suchmaschinen. Es sei ein „wichtiger erster Schritt, um der Online-Piraterie und dem Verkauf gefälschter Produkte ein Ende zu bereiten" (Quelle: Heise).

15. Mai 2011: Das US-Repräsentantenhaus soll an einem Gesetzentwurf zur verdachtsunabhängigen Speicherung von Telefon- und Internetdaten arbeiten. Die Daten sollen 18 Monate auf Vorrat gespeichert werden. Das Gesetz richtet sich vor allem gegen die Darstellung von Kindesmissbrauch im Internet. Daten von Handy-Nutzern und IP-Adressen von WLAN-Servern sollen nicht gespeichert werden. Bisher gibt es in den USA das *Quick-Freeze*-Verfahren, bei dem Verbindungs- und Standortinformationen bei konkretem Verdacht für 90 Tage festgehalten werden; eine Vorratsdatenspeicherung wie in der EU gibt es nicht (Quelle: Heise, CNet).

16. Mai 2011: Beim französischen Unternehmen *Trident Media Guard (TMG)* wird ein Datenleck festgestellt, das unter anderem den Zugriff auf Tausende IP-Adressen zulässt. TMG arbeitet eng mit der Behörde *HADOPI (Haute Autorité pour la diffusion des oeuvres et la protection des droits sur l'Internet)* zusammen und überwacht dabei *P2P*-Netzwerke, um verdächtige IP-Adressen im Zusammenhang mit Urheberrechtsverletzungen zu ermitteln (Quelle: netzpolitik.org).

17. Mai 2011: EU und OSZE kritisieren Einschränkungen der Internetnutzung in der Türkei. Sie warnen die türkische Regierung vor einem neuen System der Filterung, durch das die Informationsfreiheit gefährdet werden könnte. Obligatorische Filterpakete würden Inhalte filtern, ohne dass die Kriterien dafür klar seien. In einer anderen Anordnung werden *anstößige* Begriffe für die Verwendung in türkischen Internet-Adressen (mit der Top Level Domain „.tr") verboten. Das Umgehen der Filter soll unter Strafe gestellt werden. In der Türkei gab es dagegen in über 40 Städten Proteste (Quelle: netzpolitik.org, Heise).

18. Mai 2011: In einem Vortrag auf einer Sicherheitstagung hat BKA-Chef Ziercke erneut die Einführung der verdachtsunabhängigen Vorratsdatenspeicherung für sechs Monate gefordert. In 87 % der Fälle des Jahres 2010 hätte das BKA keine Auskunft zu der Person hinter einer IP-Adresse erhalten. Der Arbeitskreis Vorratsdatenspeicherung hat eine kritische Betrachtung dieser Zahlen veröffentlicht (Quelle: Heise, AK Vorratsdatenspeicherung).

18. Mai 2011: In Frankreich soll die Internet-Sicherheit durch höhere Strafandrohung verbessert werden, die auch eine Sperrung des Internet-Zugangs einschließt. Angriffe wie DDoS-Attacken, die auch heute schon unter Strafe stehen, sollen künftig härter sanktioniert werden. Die Strafandrohung richtet sich gegen Angriffe, auf „Informationssysteme einer öffentlichen Einrichtung oder auf eine Privatperson mit einer öffentlichen Aufgabe." Die Maßnahmen orientieren sich am *HADOPI*-Gesetz, das eine *abgestufte Erwiderung* mit Internet-Sperren vorsieht (Quelle: netzpolitik.org, Heise).

20. Mai 2011: In den Verhandlungen zum Fluggastdatenabkommen erheben Vertreter von US-Behörden Forderungen nach langfristiger Speicherung der Fluggastdaten. Es gehe nicht um Wochen oder Monate, sondern es gehe um Dekaden, so der Verhandlungsführer der Innenkommissarin der Europäischen Union. (Quelle: Heise).

20. Mai 2011: Bei einem Hoster in Offenbach werden mehrere Server der Piratenpartei beschlagnahmt. Seither seien einige Web-Sites und Online-Dienste der Partei nicht mehr erreichbar. Die Beschlagnahme basiert auf einem Rechtshilfeersuchen der französischen Behörden. Hintergrund ist offenbar, dass das Piraten-Pad durch die Hackergruppe *Anonymous* genutzt wurde, um DDoS-Angriffe abzustimmen. Die *Etherpad Foundation* zeigt sich aus rechtsstaatlicher Sicht besorgt über die Beschlagnahme. Die Piratenpartei kündigte eine Überprüfung an, ob angesichts der Landtagswahl in Bremen das Grundrecht auf politische Willensbildung verletzt worden sei. Es sei vollkommen unverhältnismäßig, wegen eines Forumsbeitrags die gesamte Kommunikationsinfrastruktur der Partei lahmzulegen, heißt es in einer Beschwerde beim Amtsgericht Darmstadt. Die Server wurden am Folgetag zurückgegeben (Quelle: netzpolitik.org, Piratenpartei, Heise).

21. Mai 2011: Der Arbeitskreis Vorratsdatenspeicherung stellt fest, dass in der Polizeilichen Kriminalstatistik nichts für die Wiedereinführung der verdachtsunabhängigen Protokollierung spreche. Die Zahlen straften „die ständige Leier maßloser Innenpolitiker und Polizeifunktionäre Lügen", dass Ermittlungen ohne die Vorratsdatenspeicherung kaum noch möglich seien. 71 % der Internet-Delikte seien nach Angaben des Bundeskriminalamts (BKA) aufgeklärt worden (Quelle: AK Vorratsdatenspeicherung, Heise).

23. Mai 2011: Menschenrechtler der *Human Rights Law Foundation (HRLF)* werfen dem Unternehmen *Cisco* vor, der chinesischen Regierung bei der Verfolgung missliebiger Personen geholfen zu haben. Von der HLRF vertretene Mitglieder von *Falun Gong* seien dauerhaft festgehalten, gefoltert oder getötet worden, oder seien vermisst. Cisco habe beim Aufbau des *Golden Shield*, auch bekannt als *Great Firewall*, mitgewirkt, durch die das Internet zensiert und Dissidenten ausfindig gemacht werden können (Quelle: Heise).

23. Mai 2011: *Facebook*-Gründer Mark Zuckerberg will Facebook auch für Kinder zugänglich machen, die jünger als 13 Jahre sind. Bisher verbietet der *Children's Online Privacy Protection Act (COPPA)* Unternehmen, persönliche Daten von Kindern zu speichern (Quelle: Heise).

23. Mai 2011: In den USA hat das *Department of Homeland Security* acht Domains stillgelegt. Begründet wurde die Stillegung damit, dass die Seiten „Bezug zur Piraterie" hätten (Quelle: Wired, netzpolitik.org).

27. Mai 2011: US-Senat und US-Repräsentantenhaus haben der Verlängerung des *Patriot Act* um weitere vier Jahre zugestimmt. Damit bleiben die nach den Anschlägen des 11. September 2001 beschlossenen Befugnisse zur Terrorismusbekämpfung bis 2015 in Kraft (Quelle: Heise).

Juni 2011

3. Juni 2011: Frank La Rue, Sonderbeauftragter der Vereinten Nationen zum Schutz der Meinungsfreiheit, spricht sich gegen *Three Strikes* zum Schutz vor Urheberrechtsverletzungen, unverhältnismäßige Netzüberwachung und für Anonymität aus. Der freie Informationsfluss solle so wenig wie möglich beschränkt werden. La Rue zeigte sich besorgt über die zunehmend ausgefeilten Filterverfahren zur Zensur. Solche Verfahren dürften ausschließlich aufgrund gesetzlicher Anordnung angewandt werden. Die Sperrung von Internet-Verbindungen sei in jedem Fall unverhältnismäßig (Quelle: netzpolitik.org, Heise).

8. Juni 2011: Das EU-Parlament fordert in einem Zwischenbericht zum 7. Rahmenforschungsprogramm der Europäischen Union strenge Auflagen für Überwachungsprojekt *INDECT (Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment).* Die EU-Kommission wird aufgefordert, alle Unterlagen des Projekts herauszugeben. Es solle ein „klares und strenges

Mandat für das Forschungsziel, die Anwendung und die Endanwender" festgelegt werden. INDECT ist ein Projekt zum Aufbau eines Informationssystems zur Unterstützung der Suche, der Entdeckung und der Überwachung von Bürgern in städtischen Umgebungen (Quelle: Heise).

8. Juni 2011: Der iranische Blogger Hossein Derakshan ist zu einer langjährigen Haftstrafe verurteilt worden. Unter anderem wird er aufgrund eines Besuchs in Israel 2008 der Spionage beschuldigt. Nachdem wegen Spionage zunächst die Todesstrafe gefordert worden war, wurde Derakshan zu neunzehneinhalb Jahren Haft verurteilt. Die Schriftstellervereinigung PEN bezeichnete das Urteil als *ungeheuerlich* (Quelle: Heise).

8. Juni 2011: Nach Schätzungen ist ein Viertel aller Hacker in den USA als Informanten für das FBI tätig. Auch die Gruppe *Anonymous* sei bereits vom FBI unterwandert. Bekanntes Beispiel ist Adrian Lamo, der Bradley Manning ins Gefängnis brachte. Manning wird verdächtigt, *Wikileaks* Material zugespielt zu haben (Quelle: Guardian, Heise).

8. Juni 2011: Wie erst jetzt bekannt wird, haben sich Unbekannte bereits am 10. Mai durch einfache Manipulation der URL Zugriff auf die Daten hunderttausender Kunden bei der *Citibank* verschafft. Sie hatten dadurch Zugriff auf Namen, Kontonummern und Mailadressen von ca. 1-2 % der 21 Mio. Kreditkartenkunden in Nordamerika (Quelle: Heise).

7. Juni 2011: Das soziale Netzwerk Facebook aktiviert die automatische Gesichtserkennung. Die Artikel-29-Gruppe der europäischen Datenschutzbeauftragten zeigt sich darüber besorgt und will die Funktion auf eine mögliche Verletzung der Privatsphäre überprüfen. Durch die Funktion werden Nutzer beim Upload der Bilder auf möglicherweise abgebildete Personen aus dem Freundeskreis hingewiesen und aufgefordert, die Personen zu kennzeichnen. Um die Funktion für eigene Bilder zu verhindern, muss man sie in den Privatsphäre-Einstellungen ausschalten (Quelle: netzpolitik.org, Heise).

10. Juni 2011: Bei der Ermittlung geblitzter Verkehrssünder greift die Polizei in Hamburg und Nordrhein-Westfalen immer häufiger auf soziale Netzwerke zurück. Fotos werden mit den Persönlichkeitsprofilen im Internet abgeglichen, anstatt wie die Beschuldigten wie bisher vorzuladen oder ihnen einen Besuch abzustatten. Da die Daten frei zugänglich sind, greift der Datenschutz in solchen Fällen nicht (Quelle: netzpolitik.org, Hamburger Morgenpost, Heise).

15. Juni 2011: Das *Schengener Informationssystem (SIS)* ist 2010 um 12,9 % auf 35 Mio. Einträge angewachsen, das geht aus einer Mitteilung der EU-Ratspräsidentschaft hervor. Ursache sei, dass der Personenkreis, der heimlich überwacht oder einer gesonderten Überprüfung unterzogen werde, um 11 % gewachsen ist (Quelle: Statewatch, Heise).

16. Juni 2011: Bundesinnenminister Hans-Peter Friedrich hat in Bonn das nationale Cyber-Abwehrzentrum eröffnet. Das Zentrum steht unter Federführung des Bundesamts für Sicherheit in der Informationstechnik (BSI); weitere Beteiligte sind das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das Bundesamt für Verfassungsschutz, das Bundeskriminalamt, das Zollkriminalamt, die Bundespolizei, der Bundesnachrichtendienst und die Bundeswehr. Friedrich bezeichnete Prävention, Information und Frühwarnung als die zentralen Aufgaben. Es werde geprüft, ob das Zentrum weitere Befugnisse bekommen solle (Quelle: Heise).

19. Juni 2011: Die Dresdner Polizei wertet bei Protesten gegen Aufmärsche von Neo-Nazis Tausende Handydaten aus, wie zunächst bekannt wird. Hintergrund ist nach Angaben der Behörden ein Verfahren wegen schweren Landfriedensbruchs. Später informierte die *taz*, dass Verbindungsdaten auch gegen Personen verwendet worden seien, denen die Störung der Demonstration der Nazis vorgeworfen wird. Die erfolgte Zweckentfremdung der Daten sei juristisch nicht haltbar; der Bundesdatenschutzbeauftragte Peter Schaar forderte, die Funkzellen-Auswertung stärker als bisher einzugrenzen (Quelle: taz, netzpolitik.org, Heise).

20. Juni 2011: Nach Ansicht von *Netzpolitik.org* gibt es in Baden-Württemberg Hinweise, die grün-rote Landesregierung wolle sich für die Wiedereinführung der vom Bundesverfassungsgericht verworfenen Vorratsdatenspeicherung einsetzen. Im Koalitionsvertrag heißt es dazu: „Bei der Vorratsdatenspeicherung setzen wir uns dafür ein, die Vorgaben des Bundesverfassungsgerichts präzise einzuhalten." Die Verlautbarungen der Koalitionspartner dazu sind widersprüchlich (Quelle: netzpolitik.org).

22. Juni 2011: Die EU leitet ein Vertragsverletzungs-Verfahren gegen Deutschland wegen der nicht erfolgten Umsetzung der Vorratsdatenspeicherung ein. Als erste Stufe wurde eine Stellungnahme des Bundesjustizministeriums angefordert (Quelle: Neue Osnabrücker Zeitung, Heise).

22. Juni 2011: Berichten des *mdr* zufolge wurden in Dresden seit 2009 in großem Umfang Kundendaten der Baumarkt-Kette *OBI* und Mobilfunkdaten in der Dresdner Neustadt gespeichert und ausgewertet. Von OBI wurde 162 000 Einkaufsjournale ausgewertet, nachdem offenbar dort gekaufte Artikel in Brandsätzen verwendet worden waren (Quelle: mdr, netzpolitik.org).

26. Juni 2011: In Bayern soll der sogenannte Bayern-Trojaner in den Jahren 2009 und 2010 insgesamt fünf Mal genutzt worden sein, um Rechner von Verdächtigen auszuspähen. Es sollten dabei Straftaten wie banden- und gewerbsmäßiger Betrug oder Handel mit Betäubungs- oder Arzneimittel aufgeklärt werden (Quelle: Heise).

26. Juni 2011: Einem Bericht der *taz* zufolge weitet sich der Datenskandal bei der Anti-Nazi-Demonstration in Dresden immer weiter aus. Inzwischen ist von über 1 Mio. Mobilfunk-Verbindungsdaten die Rede, die bei der Funkzellen-Auswertung erfasst worden seien. Als Grund gibt Justizminister Jürgen Martens (FDP) die Bildung einer kriminellen Vereinigung an; Details werden keine genannt. Der sächsische Innenminister Markus Ulbig (CDU) hält die Auswertung für *verhältnismäßig*. Der Skandal weitet sich im Folgenden weiter aus. Der Dresdner Polizeipräsident wird abberufen, dann aber zum Leiter der sächsischen Landespolizeidirektion befördert. Es stellt sich heraus, dass offenbar auch Gespräche abgehört wurden. Die Demonstrationsteilnehmer bereiten eine Klage vor (Quelle: Polizei Sachsen – *www.polizei.sachsen.de*, netzpolitik.org, taz, Heise).

26. Juni 2011: Die unbekannten Datendiebe, die sich Zugang zu Kundendaten der *Citibank* verschafft hatten, haben mittlerweile rund 2,7 Mio. US-Dollar von den Konten der Citibank-Kunden erbeutet. Dies war offenbar möglich, obwohl die Täter angeblich keinen Zugriff auf Sicherheitscodes, Sozialversicherungsnummern und Geburtsdaten gehabt hätten (Quelle: Heise).

29. Juni 2011: Bundesinnenminister Hans-Peter Friedrich und Bundesjustizministerin Sabine Leutheusser-Schnarrenberger geben bekannt, dass die Anti-Terror-Gesetze, die nach dem 11. September 2001 erlassen worden waren, um weitere vier Jahre verlängert werden sollen. Unter anderem erlauben es die Gesetze Geheimdiensten, Auskünfte von Banken, Fluggesellschaften, Postdienstleistern und Telekommunikationsfirmen zur Terrorbekämpfung einzuholen (Quelle: Heise).

Juli 2011

11. Juli 2011: US-Bürgerrechtler befürchten, dass das Datenerfassungs-Projekt *NGI (Next Generation Identification)* massive Folgen für die Privatsphäre der Bürger haben wird. Im Rahmen des Projekts sollen neue Systeme für Finger- und Handballenabdrücke, Iris-Scans und Gesichtererkennung entwickelt und eine große Datenbank aufgebaut werden. Diese Datenbank soll zur Erkennung von Kriminellen und potenziellen Terroristen im Rahmen der Strafverfolgung und Immigrations-Überwachung dienen, und zusätzlich laut Planung auch eine Schnittstelle für Firmen bereitstellen, um Mitarbeiter überprüfen zu können. Teil des Projekts ist *S-Comm (Secure Communities deportation program).* Entgegen bisherigen Plänen befürchten Bürgerrechtsvereinigungen, dass S-Comm eine erste Komponente zur Erfassung biometrischer Daten von US-Bürgern wird. Es gibt auch Anzeichen, dass die bisher freiwillige Teilnahme an S-Comm obligatorisch werden soll (Quelle: Heise).

15. Juli 2011: Das Verwaltungsgericht Hannover hat entschieden, dass die dauerhafte Videoüberwachung in der Innenstadt von Hannover rechtswidrig ist. Nach Ansicht des Gerichts verstößt die Überwachung mit über 70 fest installierten aufzeichnungsfähigen Kameras gegen Vorgaben des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung. Danach ist eine Videoüberwachung nur als offene Beobachtung zulässig. (Quelle: Heise).

18. Juli 2011: Der umstrittene Elektronische Gehaltsnachweis ELENA soll nach Willen der Bundesregierung endgültig gestoppt werden. Bundeswirtschafts- und -arbeitsministerium haben sich nach einer gemeinsamen Mitteilung auf die schnellstmögliche Einstellung des Verfahrens verständigt. Als Grund geben sie die zu geringe Verbreitung der qualifizierten elektronischen Signatur an, die für ELENA datenschutzrechtlich erforderlich ist. ELENA stand in der Kritik, weil dadurch eine umfangreiche Datenbank mit Gehalts- und anderen Daten der Beschäftigten aufgebaut werden sollte (Quelle: Zeit, Spiegel, netzpolitik.org, Heise).

20. Juli 2011: Das Landgericht München hat entschieden, dass eine Durchsuchung im Frankfurter Bundesbüro des globalisierungskritischen Netzwerks *Attac* rechtswidrig war. Attac hatte ein Gutachten zu Geschäften der Bayerischen Landesbank auf seiner Internet-Seite veröffentlicht. Der Durchsuchungsbeschluss war nach Ansicht des Landgerichts nicht verhältnismäßig; zudem hatte der bayerische Landtag zuvor selbst wesentliche Teile des Gutachtens veröffentlicht (Quelle: Attac, Heise).

25. Juli 2011: Die Anschläge in Oslo und auf der Insel Utøya, die insgesamt 93 Todesopfer gefordert haben, werden von deutschen Innenpolitikern dazu genutzt, die Vorratsdatenspeicherung und weitere Überwachungsmaßnahmen wieder ins Gespräch zu bringen. Hans-Peter Uhl (CDU) forderte die Überwachung von Internetverkehr und Telefongesprächen. Er begründete das damit, dass die Tat „im Internet geboren" sei. Der Vorsitzende der Gewerkschaft der Polizei, Bernhard Witthaut, forderte, neben der Anti-Terror-Datei für *Gefährder* auch eine Datei für auffällig gewordene Personen einzurichten (Quelle: netzpolitik.org, Heise).

30. Juli 2011: Die Schweizerische Justizministerin Simonetta Sommaruga fordert die erhebliche Ausweitung der Überwachung des Internet. Die Polizei soll die Möglichkeit erhalten, neben dem Abhören von Telefongesprächen und der Überwachung von E-Mails auch weitere Aktivitäten wie Chats, das Abrufen von Videos und Recherchen mit Suchmaschinen in Echtzeit zu überwachen. Die Bürgerrechtsorganisation *Digitale Gesellschaft* schließt aus den Formulierungen, dass auch die Einführung einer zeitlich nicht näher befristeten, verdachtsunabhängigen Vorratsdatenspeicherung geplant ist. Diese sei ein „schwerwiegender Eingriff in die verfassungsmäßig garantierten Grundrechte" und bedürfe zumindest einer klaren rechtlichen Grundlage. Nach „Gutdünken der Überwachungsbehörden" würden „Befugnisse erweitert und Grundrechte beschnitten" (Quelle: Heise).

31. Juli 2011: Auch SPD-Chef Sigmar Gabriel fordert nach den Terroranschlägen von Norwegen die schärfere Überwachung des Internet (Quelle: Bild am Sonntag, Heise).

August 2011

2. August 2011: Der Hamburgische Datenschutzbeauftragte Johannes Caspar fordert die Löschung biometrischer Daten bei Facebook. Er bezeichnet die Funktion als einen „schweren Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen" (Quelle: Heise).

3. August 2011: Nach Ansicht des Bundesdatenschutzbeauftragten Peter Schaar haben sich Befürchtungen bestätigt, dass die einheitliche Steueridentifikationsnummer als personenbezogenes Merkmal zunehmend in anderen Bereichen verwendet wird. Sie drohe ein allgemeines Personenkennzeichen zu werden, so Schaar. Gegen ein solches Kennzeichen bestehen verfassungsrechtliche Bedenken; bisherige Klagen wurden aber vom Finanzgericht Köln zunächst abgewiesen (Quelle: Heise).

3. August 2011: Industrieanlagen-Steuerungen sind unter Umständen ungeschützt im Netz erreichbar. Es sei gelungen, über Google die ungeschützte Steueroberfläche des Transformators in einem britischen Umspannwerk zu finden. Die Steuerung war nicht durch Passwort geschützt und hätte übernommen werden können, um beispielsweise einen Stromausfall auszulösen (Quelle: Heise).

7. August 2011: In einem Interview mit dem Nachrichtenmagazin *Spiegel* hat Bundesinnenminister Hans-Peter Friedrich (CSU) die Anonymität im Internet in Frage gestellt. Er fordert, dass Blogger wie *Fjordman* – auf den sich der norwegische Attentäter Anders Behring Breivik bezieht – ihre wahre Identität offenbaren sollten. Sebastian Nerz, Vorsitzender der Piratenpartei, warf Friedrich darauf vor, einen der „Grundpfeiler unserer Demokratie" anzugreifen. Dieter Wiefelspütz (SPD) wertete die Aussagen als „Ausdruck von Hilflosigkeit" (Quelle: Spiegel, Heise, Kölner Stadt-Anzeiger).

8. August 2011: Der *Blackberry*-Hersteller *RIM* hat angekündigt, im Zusammenhang mit den Ausschreitungen in England die Behörden zu unterstützen. Mögliche Unterstützung ist das Entschlüsseln von Kurznachrichten. Der Hersteller bewirbt den Blackberry als besonders sicher, hat aber bereits in der Vergangenheit Daten an Behörden übergeben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte bereits 2005 wegen Datenschutzbedenken eine Warnung veröffentlicht (Quelle: netzpolitik.org).

Marie-Theres Tinnefeld

Der Beschäftigtendatenschutz – eine unendliche Geschichte?

Zu den wesentlichen Reformen im Datenschutz gehört die geplante Regelung des Beschäftigtendatenschutzes. Sie wird seit den siebziger Jahren des 20. Jahrhunderts gefordert und wird seitdem von der jeweiligen Bundesregierung als rechtspolitisches Ziel anerkannt. Der Gesetzgeber selbst stuft die 2009 eingefügte eigenständige Bestimmung zum Beschäftigtendatenschutz (§ 32 BDSG) als Zwischenlösung ein, die gegenüber der bisherigen Rechtslage keine grundlegenden Neuerungen bringt. Sie beschränkt sich im Wesentlichen auf die Festschreibung von Prinzipien und Regeln, die von der arbeitsgerichtlichen Rechtsprechung seit Jahrzehnten entwickelt worden sind.

Im Spätsommer 2010 hat die Bundesregierung einen Gesetzentwurf zum Beschäftigtendatenschutz vorgestellt, der sowohl von den Arbeitgeberverbänden als auch von den Gewerkschaften heftig kritisiert wird. Inzwischen ist dieser Gesetzentwurf fortentwickelt worden. Auch Differenzen zwischen Sachverständigen selbst und innerhalb der Bundesregierung bestehen fort.[1] Die heiklen Konfliktfelder des Gesetzentwurfs werden hier dargestellt, um erforderliche Lösungen anzustoßen. Die Ausführungen beruhen auf Analysen des Gesetzes, die die Autorin in Zusammenarbeit mit Thomas Petri und Stefan Brink u.a. mit Unterstützung von Prof. Düwell (Vorsitzender Richter am BAG und Professor an der Universität Konstanz) in Anknüpfung an einen eigens erstellten Fragenkatalog zum geplanten Gesetz erstellt hat.[2]

Im Folgenden sollen die aktuellen Herausforderungen punktuell und unter Berücksichtigung neuer Technologien (Videoüberwachung, Kommunikation im Internet, Ortungssysteme usw.) dargelegt werden, um notwendige Nachbesserungen des Entwurfs anzustoßen. Denn wir waren uns einig, dass der Gesetzentwurf grundsätzlich auf einem tragfähigen Konzept beruht, der allerdings eine weitere faire Ausbalancierung widerstreitender Interessen in umstrittenen Fällen erforderlich macht. In engem Zusammenhang dazu stehen die seit den Datenskandalen angewachsenen Compliance-Anforderungen an Unternehmen, welche diese auch zur Sicherstellung datenschutzrechtlicher Vorschriften ergreifen müssen.

Insbesondere sollen an dieser Stelle sieben umstrittene Fragestellungen unter Einbeziehung der Ausführungen von Tinnefeld/Petri/Brink aus dem Jahre 2011 näher betrachtet werden. Vorausgestellt wird eine kurze Erläuterung des verfassungsrechtlichen Erforderlichkeitsprinzips, das Teil der Verhältnismäßigkeit ist: Neue Fragen lassen sich mit diesem Instrument im Beschäftigungsverhältnis analysieren, diskutieren und häufig auch beantworten. Abstrakt belehrt das Prinzip darüber, dass keine Daten auf Vorrat erhoben und verwendet werden dürfen; die Zulässigkeit endet an den „erforderlichen" Daten für das jeweilige Beschäftigtenverhältnis.

1. Erforderlichkeitsgrundsatz

Schon § 32 Abs. 1 Satz 1 BDSG knüpft die Rechtmäßigkeit einer Verarbeitung der Beschäftigtendaten an deren Erforderlichkeit für die Begründung, Durchführung oder Beendigung eines Beschäftigtenverhältnisses. Als Beispiele wurden in den Entstehungsmaterialien insbesondere die bekannten Entscheidungen des Bundesarbeitsgerichts zum Fragerecht des Arbeitgebers an-

Marie–Theres Tinnefeld

Prof. Dr. **Marie-Theres Tinnefeld** ist Juristin und Publizistin mit Schwerpunkt Datenschutz- und Wirtschaftsrecht. Sie ist Mitglied im wissenschaftlichen Beirat des FIfF.

geführt. Die Hervorhebung des Erforderlichkeitsprinzips ist verfassungsrechtlich zum Schutz des Grundrechts auf Privatheit und informationelle Selbstbestimmung (Datenschutz) geboten. Dies bedeutet, dass widerstreitende Positionen der Vertragsparteien im Wege der praktischen Konkordanz auszugleichen und nur solche Eingriffe in das Grundrecht der schwächeren Partei, also des Beschäftigten, hinzunehmen sind, die tatsächlich für den Arbeitgeber bzw. Dienstherrn erforderlich sind. Mit anderen Worten: Die Erhebung und Verwendung von Beschäftigtendaten muss geeignet und zugleich das relativ mildeste Mittel sein, um den unternehmerischen Interessen Rechnung zu tragen (Beispiele: zulässige Fragen bei Begründung des Beschäftigungsverhältnisses nach Qualifikationen, beruflichem Werdegang, Drogenabhängigkeit usw. des Beschäftigten; ausgeschlossen sind dagegen Fragen nach genetischen Eigenschaften oder der sexuellen Orientierung des Beschäftigten).

2. Umstrittene Fragen

a. Kollektive Vereinbarungen

Die Arbeitgeberseite hat häufig kritisiert, dass der Entwurf die notwendige Flexibilität im Rahmen von Datenverarbeitungsprozessen beeinträchtige. Sie seien zwar nicht immer zur Abwicklung des Beschäftigungsverhältnisses im Sinne des Gesetzes „erforderlich", aber trotzdem für die betrieblichen Abläufe notwendig. Der Vorwurf zielt vor allem auf Beschränkungen in Dienst- und Betriebsvereinbarungen.

Bereits vor Inkrafttreten des § 32 BDSG kam dem kollektiven Arbeitsrecht eine zentrale Stellung im Beschäftigtendatenschutz zu. Arbeitgeber und Betriebsrat sind nach § 75 Abs. 2 Satz 1 BetrVG verpflichtet, die freie Entfaltung der Persönlichkeit der Beschäftigten zu schützen und zu fördern.

Im Entwurf werden kollektive Vereinbarungen weiterhin als Rechtsvorschriften (vgl. § 4 Abs. 1 S. 2) anerkannt. Er sieht aber im letzten Teil (§ 32l Abs. 5) vor, dass jedwede Regelung an datenschutzgesetzliche Mindeststandards gebunden ist. Ziel der Kollektivvereinbarungen ist es, das vertrauensvolle Verhältnis der Betriebspartner zu fördern, gesetzliche Vorgaben und betriebliche Praxis in Einklang zu bringen. Eine datenschutzrelevante Vereinbarung kann als zulässig angesehen werden, „wenn sie im Rahmen einer *wertenden Gesamtbetrachtung* ein Datenschutzniveau bietet, das mindestens dem gesetzlichen Schutzniveau entspricht. Die Betriebspartner würden auf diese Weise die Möglichkeit zu flexiblen, betriebsnahen Lösungen erhalten, ohne dass das vom Gesetzgeber gewollte Datenschutzniveau unterschritten wird."

b. Bedeutung der Einwilligung im Beschäftigtenverhältnis

Die Einwilligung des Beschäftigten muss auf der „freien Entscheidung" des Betroffenen beruhen (§ 4a Abs. 1 Satz 1 BDSG). Je abhängiger eine Person ist, desto weniger kann sie ihre Rechte im Rahmen einer Einwilligung selbst gestalten. Der Entwurf will die Einwilligung daher nur in bestimmten Fällen zulassen (§ 32l Abs. 1). Es wird kritisiert, dass diese Einschränkung zu weit gehe. Nach Düwell könne der Gesetzgeber jedoch in Fällen von Praxisproblemen „nach dem *trial-and-error*-Prinzip wieder nachjustieren". Bei realitätsnaher Betrachtung ist auch denkbar, die Einwilligungsfähigkeit des Beschäftigten durch eine Ergänzung des Gesetzes (§ 32l Abs. 5) mithilfe von Betriebs- bzw. Dienstvereinbarungen zu erweitern.

c. Betriebliche Videoüberwachung

Die Videoüberwachung wird als Instrument eingesetzt, um das Verhalten des Beschäftigten am Arbeitsplatz zu kontrollieren. Sie wird offen, aber auch heimlich eingesetzt. Nach dem noch geltenden § 32 Abs. 1 Satz 1 BDSG soll die offene Videoüberwachung in nicht öffentlich zugänglichen Räumen dann eingesetzt werden dürfen, wenn sie erforderlich ist. Wegen der hohen Intensität des Eingriffs genügt eine präventive Videoüberwachung ohne konkreten Grund den gesetzlichen Anforderungen nicht. Nach dem Entwurf (§ 32f) ist die verdeckte personenbezogene Videoüberwachung im Beschäftigtenverhältnis nicht gestattet. Eine offene Videoüberwachung wird dagegen nach der Vorschrift erlaubt, wenn sie zu bestimmten Zwecken erforderlich ist (siehe abschließenden Katalog in § 32f Abs. 1). Der Kommunikationswissenschaftler Thomas Knieper hat überzeugend dargelegt, dass „die Aussagekraft von Bildern unterschätzt werde. Videobilder seien letztlich Konstruktionsleistungen, die dem Betrachter eine nicht unerhebliche Bilddeutungskompetenz abverlangten. Das werfe die Frage auf, wer für die Auswertung von Bildern zuständig sein solle. Darüber hinaus sei klar zu bestimmen, welche Zonen als privat von der Bildüberwachung auszuschließen seien. Unterschätzt werde auch die technische Entwicklung im Zusammenhang mit der hochauflösenden Videoüberwachung". Knieper weist in diesem Zusammenhang auf die Folgen der dreidimensionalen und der Videoüberwachung mithilfe von Wärmekameras hin. Es bestehe das Risiko, „dass schützenswerte gesundheitliche Beschäftigtendaten heimlich erkannt und bearbeitet werden können". Bereits diese Ausführungen zeigen, dass die heimliche Beobachtung des Beschäftigten mit Videokameras kein geeignetes Kontrollinstrument ist. Generell solle auch bei der Bewertung von offener Videoüberwachung zwischen der Beobachtung und der Aufzeichnung unterschieden werden. Das oben dargelegte Erforderlichkeitsprinzip verlangt darüber hinaus den Nachweis, dass alternative Methoden nicht zu dem erwünschten Erfolg führen können. In keinem Fall dürfen Daten aus der Qualitätskontrolle zweckentfremdet für die Leistungs- und Verhaltenskontrolle von Arbeitnehmern genutzt werden.

d. Ortung durch Mobilfunkdaten

Ein besonderes datenschutzrechtliches Problem ist im Spannungsfeld zwischen der geplanten Regelung für Ortungssysteme nach § 32g Abs. 1 und derjenigen für die Nutzung von TK-Diensten nach § 32i Abs. 1 erkennbar, wenn sich der Arbeitgeber Zugriff auf geografische Informationen des Nutzers über Telekommunikationsverkehrsdaten verschafft. Die geplante Neuregelung (§ 32g Abs. 1) bezieht sich ausdrücklich auf „elektronische Einrichtungen zur Bestimmung eines geografischen Standortes" und beschränkt für diesen Fall den Zugriff auf Situationen, in denen eine Ortung zur Sicherheit des Beschäftigten oder zur Koordinierung seines Einsatzes erforderlich ist. Die Be-

gründung spricht in diesem Zusammenhang von Ortungssystemen, die die Standortermittlung ermöglichen, etwa bei Mobiltelefonen oder durch GPS, das als Navigationssystem in einem Kraftfahrzeug eingebaut ist. In beiden Fällen kann der aktuelle Standort eines Gerätes und damit auch in vielen Fällen derjenige des Beschäftigten ermittelt werden.

Zu berücksichtigen ist nach Phillip Brunst, „dass standortbezogene Daten nicht nur aufgrund einer unmittelbaren und ausdrücklichen Anforderung übertragen werden, sondern dass – insbesondere bei Mobiltelefonen – derartige Informationen auch im Rahmen der Verkehrsdatenaufzeichnung beim Telekommunikationsprovider anfallen". Über die Handy-Ortung kann ein genaues Bewegungsprofil des Beschäftigten erstellt werden. Der Zugriff des Arbeitgebers auf Verkehrsdaten wird ggf. von § 32i Abs. 1 erfasst und kann möglicherweise auch zu einem späteren Zeitpunkt Aufschluss über den Standort oder die Reiseroute des Arbeitnehmers geben. Da das Fernmeldegeheimnis nach Art. 10 GG und § 88 TKG nicht nur die Telekommunikation an sich, sondern auch ihre näheren Umstände wie den Standort schützt, ist eine strenge Handhabung angezeigt. Eine Ortung des Beschäftigten kann nur zu dessen Sicherheit oder für den Schutz äußerst wertvoller Gegenstände erforderlich sein. Der Entwurf will den Schutz verstärken (§ 32g Abs. 1 Satz 3).

e. „Whistleblowerklausel"

Der Entwurf (§ 32l Abs. 4) sieht vor, dass Beschäftigte sich an die Aufsichtsbehörde wenden können, wenn tatsächliche Anhaltspunkte für einen Datenschutzverstoß des Arbeitgebers vorliegen und dieser einer darauf gerichteten Beschwerde des Beschäftigten nicht abgeholfen hat. Diese Vorschrift wird allseitig zu Recht kritisiert. Sie verstößt auch gegen EU-Recht (vgl. Vorgaben des Art. 28 Richtlinie 95/46/EG).[3]

Die Vorschrift regelt nicht das Recht und die Pflicht des verantwortungsbewussten Whistleblowers, schwerwiegende Missstände im Unternehmen in einem geordneten Verfahren anzeigen zu können. Vor diesem Hintergrund ist es aus Gründen der Rechtssicherheit notwendig, den gegenwärtigen Entwurf durch eine allgemeine Whistleblowerklausel zu ersetzen, die den Whistleblower einerseits und den Angezeigten andererseits schützt. Ohne eine entsprechende Regelung besteht die Gefahr von datenschutzwidrigen anonymen „Anzeigen". Eine solche Regelung ist auch geboten, um entsprechende Compliance-Anforderungen zu gestalten, insbesondere für weltweit operierende Unternehmen.[4] Es wäre nicht sinnvoll, wenn der Gesetzgeber die geplante Regelung nicht verbessern, sondern ganz entfallen lassen würde.

f. Konzernprivileg

Der Entwurf enthält keine Regelung zum *Konzerndatenschutz*, obwohl der praktische Bedarf an einer gesetzlichen (Neu-) Regelung wohl unbestritten ist, insbesondere auch hinsichtlich der Auftragsdatenverarbeitung. Im Gegensatz zum Beschäftigtendatenschutz will die EU eine Richtlinie zum Konzerndatenschutz erlassen, die für die Datenverarbeitung im Konzern sowie grenzüberschreitend äußerst notwendig ist. Aufgabe des nationalen Gesetzgebers ist es dann, diese Regelung in der vorgegebenen Frist umzusetzen. Der deutsche Gesetzgeber plant neuerdings auch eine eigene Regelung im Beschäftigtendatenschutzgesetz.

g. Beschäftigtendaten im Internet

Facebook ist überall; der Nutzen ist der Inhalt, nach dem auch Arbeitgeber suchen, ohne dass Betroffene davon Kenntnis haben. Das Internet bietet eine Fundgrube von Informationen, um von Bewerbern ein Profil zu erstellen, z. B. durch eine *Google-Recherche*. Sie wird von vielen Personalabteilungen bei Einstellungsverfahren genutzt. Die geplante Vorschrift zur rechtlichen Zulässigkeit der Datenerhebung aus sozialen Netzwerken bzw. (sonstigen) allgemein zugänglichen Quellen (§ 32 Abs. 6 S. 2) ist daher umstritten. Einer Regelung (§ 32 Abs. 6), wonach der Arbeitgeber den Bewerber vorher von einer Recherche informieren soll, kommt daher eher eine symbolische Bedeutung zu, da de facto die Datenerhebung nicht überwacht werden kann. Daher ist es wichtig, dem Arbeitgeber prozedurale Pflichten der Informations- und Offenlegung aufzuerlegen: Informationen, die er im Internet recherchiert hat, sollte er bereits vor der Ablehnung einer Bewerbung dem Betroffenen zur Kenntnis bringen, damit dieser dazu Stellung beziehen kann.

3. Fazit und aktuelle Anmerkungen

Es konnten an dieser Stelle einige kritische Punkte im geplanten Reformgesetz angesprochen werden, die unbedingt überdacht werden müssen. Ein weiteres schwerwiegendes Defizit des Regierungsentwurfs ist auch die im Einzelnen ungeklärte Frage der privaten Nutzung betrieblicher TK-Dienste. Hier wären prozedurale Lösungen und Ansätze der Selbstregulierung zu diskutieren. Es ist Aufgabe der Bürger und Bürgerinnen, sich für den dringend notwendigen Beschäftigtendatenschutz so zu engagieren, dass die bestehenden Mängel im laufenden Gesetzesverfahren noch behoben werden können. Dies ist umso notwendiger, als sich nach aktuellen Informationen die Fronten im Ringen um ein angemessenes Beschäftigtendatenschutzgesetz wieder verschärft haben. Insbesondere ist die Frage des Screenings bzw. der Rasterfahndung im Beschäftigtenverhältnis wieder zur größten Baustelle geworden. Der geltende § 32 Abs. 1 Satz 2 BDSG schließt zwar ein anlassloses Screening ausdrücklich aus. Neuerdings wird jedoch das anlasslose Screening mit Hilfe aller beim Arbeitgeber vorhandenen Daten wieder ernsthaft verhandelt. Das könnte zu dem absurden Ergebnis führen, die schwerwiegenden Skandale bei der Telekom, Lidl oder der Bahn nachträglich zu rechtfertigen. Auch die Frage der Freiwilligkeit einer Einwilligung im Beschäftigtenverhältnis ist wieder auf den Prüfstand gestellt worden. Es wird arbeitgeberseitig teilweise die Ansicht vertreten, dass grundsätzlich von einer Freiwilligkeit der Einwilligung im Beschäftigtenverhältnis auszugehen sei, die allerdings durch Positiv- bzw. Negativlisten eingegrenzt werden solle, um einer möglichen Fremdbestimmung im Abhängigkeitsverhältnis vorzubeugen. Diese Ansicht widerspricht den Erfahrungen der Arbeitsgerichte und dürfte auch einer Überprüfung vor dem Europäischen Gerichtshof für Menschenrechte nicht standhalten.

Anmerkungen

1 Die Stellungnahmen der Sachverständigen zum Beschäftigtendatenschutz im Anhörungsverfahren der Bundesregierung sind abrufbar unter: http://www.bundestag.de/bundestag/ausschuesse177/a04/Anhoerungen/Anhoerung08/Stellungnahmen_SV/index.html.

2 Tinnefeld/Petri/Brink, Aktuelle Fragen zur Reform des Beschäftigtendatenschutzes. Ein Update, MMR 7/2011, 427-432; dies., MMR 2010, 727-735.

3 Vgl. Tinnefeld, Whistleblowing, FIfF-Kommunikation 3/2010, 30-34.

4 Unter gewissen Umständen (etwa bei sehr großen oder besonders exponierten Unternehmen) kann sich bereits aus den in § 130 OWiG geregelten Aufsichtspflichten von Unternehmensinhabern eine faktische Rechtspflicht zum Betrieb eines angemessenen und datenschutzkonformen Hinweisgebersystems ergeben, vgl. etwa Wybitul, Handbuch Datenschutz im Unternehmen, 2011, Rn. 186 ff.

Jens Rinne

EDRi-Corner

*Das FIfF ist eine von aktuell 28 Mitgliedsorganisationen der 2002 gegründeten Vereinigung für Europäische Digitale Rechte, kurz: EDRi (**E**uropean **D**igital **Ri**ghts). EDRi und seine Mitgliedsorganisationen haben sich zum Ziel gesetzt, die Bürgerrechte in der Informationsgesellschaft zu verteidigen. Bei Interesse an Mitarbeit bitten wir um Nachricht an rinne@fiff.de. Diese EDRi-Ecke erhebt nicht den Anspruch, die komplexen Abläufe in Brüssel zu erklären, sondern sie soll ein paar Schlaglichter als ‚Appetitanreger' auf die aktuellen Themen werfen, über die im EDRi-gram berichtet wird.*

Das EDRi-gram erscheint alle zwei Wochen und hat zirka 20 Seiten. In den letzten sechs Ausgaben (#9.10 bis #9.15) wurden wieder die Dauerbrenner Vorratsdatenspeicherung, Netzsperren, Zensur, Netzneutralität, Urheberrechte und Copyright behandelt. Zum Online-Mitlesen erscheint es in Deutsch unter *www.unwatched.org/taxonomy/term/1* und als englisches Original unter *www.edri.org/edrigram.*

Zwei Themen beschäftigen uns zur Zeit besonders. Das eine ist der *OSZE-Bericht* zu den Themen Netzzugang und Menschenrechte. Dem Bericht der OSZE (Organisation für Sicherheit und Zusammenarbeit in Europa) vom 8. Juli 2011 zufolge sollte ein freies Internet beibehalten und der *Zugang zum Internet als Menschenrecht* betrachtet werden (#9.14). Diesem Thema widmet sich ausführlich der Artikel von *Andreas Krisch* auf Seite 40-41 in diesem Heft, und wir können es deshalb hier bei diesem Hinweis belassen.

Das zweite Thema sind die Verhandlungen zum Fluggastdatenabkommen. Anfang Juli 2011 wurde in einer Plenarsitzung des Europäischen Parlaments (EP) über den aktuellen Stand bei den Verhandlungen über die *Fluggastdatenabkommen* (*Passenger Name Record, PNR)* mit den USA, Kanada und Australien diskutiert (#9.11, 9.13, 9.14). Die Kommissarin *Cecilia Malmström* erklärte, die Abkommen mit den USA, Kanada und Australien befänden sich in einem fortgeschrittenen Stadium, einige wichtige Entscheidungen stünden aber noch aus. Nach Klärung dieser Punkte solle ein multi-lateraler Ansatz anstelle des bisherigen länderweisen Vorgehens gewählt werden. Sie führte aus, die Daten seien im Kampf gegen den Drogenschmuggel und den Menschenhandel nützlich gewesen, konnte aber nicht verdeutlichen, was es nütze, wenn die Ermittler wüssten, was die Menschenhändler zu Abend gegessen hätten. Von den Parlamentariern wurde die Neuverhandlung der Abkommen gefordert, wobei sichergestellt werden müsse, dass diese im Einklang mit den EU-Datenschutzbestimmungen stünden.

Im Mai warnte der Juristische Dienst der Europäischen Kommission den Generaldirektor für Inneres, dass der Entwurf zum EU/US-Abkommen über den Austausch von Fluggastdaten nicht mit den Grundrechten vereinbar sei. Auch von Seiten der Europäischen Grundrechtsagentur (FRA) ist an dem PNR-Vorschlag der EU vernichtende Kritik geübt worden. Aber die Europäische Kommission ist trotz dieser Kritik und selbst unter den nationalstaatlichen Bedenken bezüglich Speicherfristen und Bestimmungen zur Übermittlung der Daten an Drittstaaten offensichtlich nicht bereit, die Verhandlungen neu aufzunehmen.

Datenschutzaktivisten von EDRi und anderen Organisationen haben sich Ende Mai in Brüssel getroffen, um eine rechtliche, technische und politische Analyse auszuarbeiten, ihre Aktivitäten für die nächste Zeit zu koordinieren und eine langfristige Zusammenarbeit zu diesem Thema zu planen. Eine Postkartenaktion wurde gestartet, mit der dazu aufgerufen wird, Urlaubspostkarten an die Europaparlamentarier zu schicken und diese aufzufordern, sich persönlich gegen die PNR-Abkommen einzusetzen.

Jens Rinne

Jens Rinne ist Diplom-Informatiker und studierte in Bonn. Seit 2007 im FIfF-Vorstand und seit 2009 stv. Vorsitzender. Derzeit im AK Zensus gegen die Volkszählung für das FIfF aktiv.

Göde Both

6th Gender & ICT in Umeå (Schweden)

Konferenzbericht

Unter dem diesjährigen Motto Feminist Interventions in Theories and Practices *trafen sich vom 8. bis 10. März 2011 InformatikerInnen und SozialwissenschafterInnen, um aus feministischen Perspektiven Informationstechnologien zu kritisieren und ihre eigene Verstrickung zu reflektieren. Ausgerichtet wurde die Konferenz vom Institut für Informatik an der Universität Umeå. Sie bildet ein wichtiges Vernetzungs- und Austauschmedium für feministische WissenschaftlerInnen, die im Bereich der männlich dominierten Informationstechnologien arbeiten oder forschen. Die Beiträge speisten sich aus feministischer und postkolonialer Technikforschung, Frauenforschung und partizipativem Design. Die TeilnehmerInnen kamen aus Bangladesh, Deutschland, Finnland, Großbritannien, Holland, Norwegen, Österreich, Schweden, Spanien und den USA. Die Zusammensetzung spiegelte sowohl die national unterschiedlichen Institutionalisierungen der feministischen Technikforschung als auch die ökonomischen Privilegien wider, welche die Voraussetzungen für eine Teilnahme an der Konferenz bildeten. In diesem Beitrag möchte ich von einer Auswahl von Vorträgen berichten, die ich auf der Konferenz mitverfolgt habe.*

Ein Großteil der Konferenzbeiträge zeigte, dass die Praktiken und Theorien der Informatik immer lokal, situiert und verkörpert sind. Dies steht im Widerspruch zu ihrem Selbstbild einer (geschlechts-)neutralen und universalistischen Wissenschaft. Es trifft im übrigen auch auf diesen Artikel zu, der von einer *weißmännlichen* Position aus geschrieben wurde. Es ist notwendig, auf unterschiedliche Positionierungen aufmerksam zu machen, weil sie mit Privilegien verbunden sind. Spezifisch für eine feministische Herangehensweise ist die Analyse von (Handlungs-) Macht. Wer kann sprechen, gestalten und entscheiden? InformatikerInnen tragen Verantwortung nicht nur daran, wie Menschen gegenwärtig leben, sondern beteiligen sich im zunehmenden Maße daran, welche Zukünfte imaginiert und realisiert werden: Wer hat die Möglichkeit zu träumen?

Fragwürdige Innovationen

Tiina Suopajärvi und Johanna Ylipulli berichteten von ihrer Studie zur *Ubiquitous City Oulu*, einer Kooperation von Universität, Privatwirtschaft und Stadtverwaltung zum Aufbau einer Informationsinfrastruktur in Oulu (Finnland). Hierzu führten sie Interviews mit Projektverantwortlichen und -beteiligten durch. In ihrem Vortrag gehen sie der Frage nach, welche AkteurInnen die Entscheidungen treffen, wessen Visionen so verwirklicht werden und wer davon profitiert. Das Projekt ist nach dem Konzept eines *living lab* angelegt und soll die NutzerInnen aktiv in den Gestaltungsprozess einbinden. Im Stadtgebiet befinden sich große Touchscreen-Displays und drahtlose Netzwerke, die von EinwohnerInnen und TouristInnen genutzt werden können, um aktuelle und kontextabhängige Informationen abzurufen. Suopajärvi und Ylipulli stellen fest, dass die Vorteile der Technologien von den AkteurInnen als selbstverständlich angesehen werden. Damit gibt es für die Projektverantwortlichen keinen Grund, sie näher zu untersuchen oder zu hinterfragen. NutzerInnen-Studien wurden nur im eingeschränkten Maße und kurz vor der Fertigstellung durchgeführt. Suopajärvi und Ylipulli kommen zum Schluss, dass die ausschließlich männlichen Informatiker die relevanten Entscheidungen treffen. Ohne ausführliche NutzerInnen-Studien orientieren sich die Informatiker an ihren eigenen Interessen. Damit richtet sich die Gestaltung hinsichtlich technisch interessierter Männer aus. Dies verdeutlicht sich u.a. an einem Wettbewerb, in dem nach neuen Anwendungen für die Displays gesucht wird. Diese müssen von Teilnehmenden selbst entwickelt werden. So werden alle BürgerInnen ausgeschlossen, die nicht über die Fähigkeiten und Ressourcen verfügen, um Anwendungen zu programmieren. Suopajärvi und Ylipulli kritisieren Ubiquitous Oulu als technikgetriebenes Projekt, welches den Informatikern mehr Handlungsmacht einräumt als allen anderen AkteurInnen. Da die NutzerInnen weder ausreichend noch gleichberechtigt involviert werden, droht das Projekt, sich einseitig an den Interessen der Informatiker auszurichten. Die geringe Akzeptanz bei BürgerInnen kündigt ein Scheitern auf breiter Linie an.

Johanna Sefyrin hinterfragt in ihrem Beitrag die Visionen der mobilen Internetnutzung. Diese versprechen zu „jeder Zeit und an jedem Ort" den Zugriff auf das Internet zu ermöglichen. Diese Vision, welche bereits von Kleinrock im Jahre 1969 formuliert wurde, ist ungemein wirkmächtig. Das Subjekt dieser Visionen ist privilegiert, autonom und kann sich frei über nationale Grenzen bewegen. Dieser Lebensstil erfordert erhebliche Ressourcen und eine Infrastruktur. Bestimmte Menschen müssen dafür arbeiten, dass diese extensiven Reisen und der von Zeit und Raum unabhängige Zugriff für andere möglich sind. Im Gegensatz zu den Visionen sind die Praktiken der Herstellung und Gestaltung immer lokal und situiert. Sefyrin schlägt eine modifizierte Lebenszyklus-Betrachtung vor. Es müssten nicht nur die Auswirkungen für die Umwelt berücksichtigt werden, sondern auch die AkteuerInnen und die Orte an denen sie sich befinden. So geraten die Konsequenzen in den Blick, die AkteurInnen erfahren, weil sie in den Lebenszyklus eines IT-Produkts oder einer Dienstleistung eingebunden sind. Sie hebt hervor, dass bereits der Abbau der Rohstoffe für Informationstechnologien in Konflikt mit den Interessen der lokalen Gemeinschaften stehen kann. Sie verweist auf den Bergbau in Nord-Australien und im Kongo. Die im Kakadu National Park (Australien) lebenden Mirrar zum Beispiel wurden solange bedroht, schikaniert und bestochen, bis sie ihren Widerstand gegen eine Mine aufgaben und einem Unternehmen die Schürfrechte verkauften. Sefyrin for-

dert diejenigen auf, die in der IT-Industrie arbeiten oder davon profitieren, Verantwortung für die Probleme zu übernehmen.

Postkoloniale Perspektiven

Naziat Hossain Choudhury hat die Facebook-Nutzung weiblicher User in Bangladesh erforscht. Sie wirft damit ein Schlaglicht auf die interpretative Flexibilität von Technologien. Nur eine privilegierte Minderheit hat in Bangladesh regelmäßig Zugang zum Internet. Dem gegenüber stehen eine Million Facebook-Anmeldungen aus Bangladesh. Weibliche User greifen mehrheitlich über Mobiltelefone darauf zu. Choudhury unterstreicht, dass die Nutzung über die Pflege von Freundschaften hinaus geht. Facebook diene als Infrastruktur für gegenseitige Unterstützung und stärke so die Handlungsmacht der weiblichen User im Alltag. Die Aneignung der Technologien durch die Nutzerinnen geht so über die vom Unternehmen intendierten Szenarios hinaus.

Pirjo Elovaara berichtete von ihrer Beteiligung an einem IT-Projekt mit einer Frauen-Kooperative in Ruanda. Es wurde im Rahmen der Entwicklungszusammenarbeit von der schwedischen Regierung finanziert. In ihrem Vortrag hinterfragt sie das Projekt und ihr ursprüngliches Anliegen. Welche Gemeinsamkeiten haben *weiße* Wissenschaftlerinnen aus Schweden und die Mitglieder der Kooperative? Elovaara kommt zu dem Schluss, dass die universalistische Kategorie „Frau" nicht greift, indem sie auf die zahlreichen Privilegien verweist, die sie in Ruanda genossen hat. Ferner kritisiert sie den Fortschrittsglauben auf dem Technologietransfer basiert. So gerät außer Blick, dass Informationstechnologien aus den Länder des Nordens bestimmte Formen von Wissen ein- oder ausschließen. Wie passen sie zu den lokalen Formen von Wissen und Wissenspraktiken in der Kooperative? Elovaara stellt fest, dass ihr kritischer Impetus zur Projektlaufzeit in den Hintergrund geriet und durch die unmittelbaren Probleme in der Durchführung überschattet wurde.

Vergeschlechtlichte Normen

Frederik Sjögren beschäftigt sich mit der Frage, wie Geschlecht in zwischenmenschlichen Interaktionen hergestellt wird. Hierzu untersucht er ethnographisch Schwedens Elite-Informatik-Forschungszentren. Seine männlichen Informanten behaupten, Geschlecht spiele keine Rolle innerhalb der Informatik, weil nur „objektive" Leistungen gewürdigt würden. Sjörgrens Studie zeigt auf, wie Männlichkeit und Kompetenz in der Informatik ko-konstruiert werden. Technische Kompetenz wird durch Computer-Nerds verkörpert, eine Verkörperung die weitgehend nur „Männern" offen steht.

Maja van der Velden berichtete von den Fallstudien des Forschungsprojekts *Autonomy and Automation*. Es untersucht, wie norwegische PatientInnen das Web 2.0 nutzen, um an medizinische Informationen zu gelangen und ihre Erfahrungen mit anderen Betroffenen zu teilen. Van der Velden schlägt dabei vor, *privacy*[1] nicht als Eigenschaft oder Besitz eines autonom gedachten Individuums aufzufassen, sondern als materiell-diskursive Aktivität der NutzerInnen. Van der Velden greift zahlreiche feministische Kritiken auf, die privacy als ein individualistisches, rationalistisches und inhärent männliches Konzept zurückweisen. Diesen Kritiken zu Folge dienen Autonomie und privacy in erster Linie männlichen Interessen und werten weiblich konnotierte Werte wie Fürsorge ab. Zum Beispiel wurde häusliche Gewalt bis in 1970er Jahre als „private" Angelegenheit verhandelt. Ihre InformantInnen äußern eine Auffassung von „relationaler" Autonomie, welche durch ihre Wahl an Technologien gestaltet wird. Trotz ihrer Skepsis gegenüber „Privatsphäre-Einstellungen", wie beispielsweise bei Facebook, erfahren die InformantInnen es als ein Zuwachs an Kontrolle und Selbstbestimmung, wenn sie ihre persönlichen Informationen mit einem teilweise unbekannten Publikum teilen. Die Offenheit, über die eigenen Erfahrungen zu sprechen, erzeugt jenes Vertrauen, welches die NutzerInnen bei der Vernetzung anstreben. Van der Velden schließt daraus, dass die Nutzung von Sozialen Netzwerken nicht als Verhandlungen entlang starrer Grenzen von öffentlich/privat und Autonomie/Fremdbestimmung analysiert werden muss, sondern als dynamische, materiell-diskursive Grenzziehungen in denen Materialität und Bedeutung produziert werden. Privacy und Autonomie sind so ein Effekt der spezifischen Praktiken von Mensch und Maschine und nicht eine Eigenschaft eines rationalen, männlichkonnotierten Individuums.

Wer die Vorträge nachlesen oder sich über weitere Themen informieren möchte, kann dies unter dem Menüpunkt *Programme* auf der Konferenz-Website tun: *https://gict2011.informatik.umu.se/*.

Anmerkungen

1 Privacy kann je nach Kontext mit Datenschutz, Intimsphäre, Privatsphäre, Vertraulichkeit und informationeller Selbstbestimmung übersetzt werden.

Göde Both

Göde Both hat 2011 sein Informatik-Studium an der Humboldt-Universität zu Berlin abgeschlossen. In seiner Diplomarbeit führt er aktuelle Ansätze aus der Informatik, Geschlechterforschung und Technik- und Wissenschaftsforschung zur Analyse von informatischen Artefakten zusammen. Er strebt eine Promotion im Feld der feministischen Technikforschung an.

Armin Schmid

Neue Aktionsform „Callshop Meeting“ gegen Vorratsdatenspeicherung

Oder: Was kann man eigentlich gegen EU-Richtlinien tun?

Deutsche und europäische Politik sind untrennbar miteinander verbunden. Doch im Gegensatz zur nationalen Ebene beschäftigen sich nur wenige Menschen mit der EU-Ebene. Und das, obwohl hier viele Richtungsentscheidungen getroffen werden. Das deutsche Gesetz zur Vorratsdatenspeicherung (VDS) wurde 2010 als verfassungswidrig verworfen. Die Richtlinie besteht aber weiterhin und wird seit April 2011 evaluiert [1]. Diese Evaluierung ist die vielleicht letzte Gelegenheit, die Richtlinie wieder abzuschaffen oder sie im Kern zu verändern.

Drei Punkte sind bei den Aktivitäten zur Evaluierung der Richtlinie zur Vorratsdatenspeicherung besonders auffällig:

Zum Ersten ist festzustellen, dass zum Personal der EU-Ebene nur wenige erfahrene Aktivisten Zugang finden. Im AK Vorrat gibt es zwar einen *Action Plan*, dieser zielt jedoch auch darauf ab, dass Personen einzeln Kontakt aufnehmen zu nationalen NGOs, Wirtschaftsverbänden, Datenschutzbeauftragten und Regierungen [2].

Die zweite Beobachtung ist, dass die Rechte des EU-Parlamentes zwar gestärkt wurden, dies sich jedoch nicht in einem gesteigerten Interesse an der Arbeit der EU-Abgeordneten widerspiegelt.

Und als Drittes fällt auf, dass wenige öffentliche Aktionen und Proteste gegen EU-Vorhaben stattfinden. Da diese in Brüssel wohl nur wenigen Amtsträgern auffallen würden, fehlt offensichtlich die Motivation dazu.

In Deutschland haben aber gerade die dezentralen Aktionstage und Veranstaltungen der lokalen Ortsgruppen und der Bündnisgruppen im AK VDS der letzten Jahre einen wesentlichen Anteil an der guten Stellung und an der Vielzahl der Überwachungskritiker innerhalb der nationalen Diskussion. Das *Callshop Meeting* ist eine Möglichkeit, sich vor Ort in die Evaluierung der EU-Richtlinie aktiv einzubringen, die Debatte europaweit in breitere Bevölkerungsteile hinein zu tragen und der personellen Verengung beim Kampf um die EU-Richtlinie entgegen zu wirken.

Bei dieser Aktionsform trifft man sich in einem Internetcafé und telefoniert von dort aus öffentlich und Seite an Seite mit verantwortlichen Personen des Parlamentes, der Kommission oder der nationalen Regierung(en). Bei einem ersten Testlauf in Regensburg kamen bei einer zweistündigen Aktion auf der einen Seite etwa 25 Telefonate (vier direkt mit Abgeordneten) zustande, sowie auf der anderen Seite eine reaktivierte Ortsgruppe, mehrere Presseberichte und ein Pressevideo. Eine Folgeveranstaltung mit dem lokalen EU-Abgeordneten ist in Vorbereitung. Mit der Aktion lassen sich tatsächlich drei Fliegen mit einer Klappe schlagen: Einbindung neuer AktivistInnen, direkter Kontakt mit politisch Verantwortlichen und Öffentlichkeitsarbeit vor Ort.

Einziger Haken ist, dass die Anzurufenden in Brüssel telefonisch nur zu den Arbeitszeiten erreichbar sind. Deshalb kommen als Teilnehmer für die Aktion vor allem Schüler, Studenten und Selbstständige in Betracht, die selbst ihre Arbeitszeiten variieren können.

Ein besonderer Reiz der Aktion ist es hingegen, dass via Skype und zum Beispiel der Software Callgraph leicht Mitschnitte der Telefonate gemacht werden können. So erhält man Zitate für die Pressemitteilung [3]. Ob man mitschneiden darf, muss vorher natürlich immer gefragt werden. Für Vertreter von Radio und Fernsehen kann es interessant sein, sich direkt in das Gespräch per Kabel einzuklinken und so selbst Live-Mitschnitte der Telefonate mit Abgeordneten anzufertigen.

Mit dem Callshop Meeting steht der Versuch im Raum, mit einer leicht durchführbaren, dezentralen und öffentlichen Aktion Druck auf die Evaluation der EU-Richtlinie zur Vorratsdatenspeicherung auszuüben. Als Ortsgruppe Regensburg im AK Vorrat bieten wir dauerhaft ein umfangreiches zweisprachiges How-To zu dieser neuen Aktionsform an und freuen uns natürlich sehr über Nachahmer, Anregungen und Verbesserungsvorschläge [4]!

Abschließend gilt der Dank dem FIfF e.V. für die Betreuung einer Praktikumsstelle zur Durchführung und Nacharbeitung des Testlaufes!

Referenzen

[1] AK Vorrat: AK Vorrat fordert europaweites Vorratsdatenspeicherungs-Verbot (18.04.2011) http://www.vorratsdatenspeicherung.de/content/view/445/135/lang,de/

[2] AK Vorrat: Data Retention action plan, http://wiki.vorratsdatenspeicherung.de/DR-Action-Plan

[3] AK Vorrat: Premiere der Callshop Meetings in Regensburg (06.05.2011), http://www.vorratsdatenspeicherung.de/content/view/451/135/lang,de/

[4] AK Vorrat Regensburg: How-To Callshop Meeting, http://wiki.vorratsdatenspeicherung.de/Ortsgruppen/Regensburg/Planungen/CallshopMeetingDoku

Armin Schmid

Armin Schmid, Student der Politikwissenschaft an der Universität Regensburg und Aktivist im AK Vorrat. Im Rahmen eines Praktikums hat er zusammen mit der Regensburger Ortsgruppe im AK Vorrat für das FIfF die Idee eines „Callshop Meetings“, als neue Protestform für die politische Ebene der EU, in einem Probelauf realisiert und dokumentiert.

Stefan Hügel

IT- und Bürgerrechtspolitik in Europa

Ein Überblick über einige europäische Entwicklungen

In Brüssel sitzt ein Ungeheuer
das in Rätseln zu mir spricht
(Dota Kehr, „Utopie")

Europa bestimmt unsere Politik – und kaum jemand hört zu. Diesen Eindruck kann man bekommen, wenn man die aktuelle politische Berichterstattung verfolgt. Selbst über Ereignisse, die auf europäischer Ebene stattfinden – beispielsweise die Wahlen zum europäischen Parlament –, wird immer noch häufig aus nationaler Sicht berichtet: „Was bedeutet das Ergebnis für die nächsten Bundestagswahlen?" Gleichzeitig scheint es für den oder die Einzelne schwierig, auf europäische Politik Einfluss zu nehmen – Sprachbarrieren, große Entfernungen und unterschiedliche Kulturen stehen dem häufig entgegen.

Dieser Beitrag soll einen Überblick über europäische Debatten geben – aktuelle wie Debatten der letzten Jahre. Dabei geht es um drei Bereiche der Netz- und Bürgerrechtspolitik: Regulierung, Überwachung, Datenschutz. Ein weiterer Themenbereich ist die Innen- und Sicherheitspolitik, die ebenfalls im Zusammenhang mit Bürgerrechtspolitik betrachtet werden muss.

Regulierung

Netzneutralität

Grundlage eines freien und allgemein zugänglichen Internet ist die Netzneutralität: Die Zusicherung, dass jedes Datenpaket im Internet gleich behandelt wird. Diese Regel, die in den Anfangsjahren des Internet nicht angezweifelt wurde, gerät unter Druck: Für Dienste, die eine hohe Bandbreite erfordern, etwa Internet-Fernsehen, soll eine *Überholspur* eingerichtet werden. Unterschiedliche Nutzer sollen unterschiedliche Bandbreiten zur Verfügung gestellt bekommen, abhängig beispielsweise von ihrer Finanzkraft.

Die Bedeutung der Netzneutralität ergibt sich aus den möglichen Folgen, wenn sie verletzt wird[1]:

- Einschränken des Zugangs zum Netz eines Netzbetreibers auf wenige oder einen Servicebetreiber gegen Bezahlung,
- Einschränken von Diensten, um sich oder Partnerunternehmen Marktvorteile zu verschaffen (das Unternehmen Apple verhindert beispielsweise die Nutzung von Skype auf dem iPhone und verschafft damit seinem Partner T-Mobile – und weiteren Partnern, die Telefonie-Dienste anbieten – einen Vorteil),
- Unterbinden oder Einschränken bestimmter Dienste wie Filesharing,
- Einschränken des Angebots in einzelnen Ländern, möglich beispielsweise durch Vergabe getrennter IP-Adressgruppen.

Offensichtlich können Einschränkungen und Filter auch für bestimmte Inhalte festgelegt werden, beispielsweise nach politischen Kriterien.

Zur Durchsetzung der Einschränkungen müssen die Datenpakete klassifiziert und dazu auf ihre Eigenschaften geprüft werden. Dabei eingesetzte Verfahren der *Deep Packet Inspection* stellen eine Gefahr für die Privatsphäre dar.

Netzneutralität hat also sowohl wirtschaftliche als auch politische und bürgerrechtliche Aspekte. Während das Thema in Deutschland heftig umstritten ist – in der Enquête-Kommission *Internet und digitale Gesellschaft* des Deutschen Bundestages konnte bei der Erarbeitung des Zwischenberichts zunächst keine Einigung erzielt werden – führen nun die Niederlande als erstes Land der EU ein Gesetz ein, das die Netzneutralität für Provider zur Pflicht macht[2,3].

Ein bereits im April veröffentlichter Bericht der Kommission bestätigt die ungleiche Behandlung des Internet-Verkehrs und führt dabei die Ergebnisse einer Studie an, die *BEREC (Body of European Regulators for Electronic Communications),* das Gremium der EU-Telekomregulierer, zu Beginn des Jahres 2010 in etlichen EU-Staaten durchgeführt hat[4]: Es komme zu Geschwindigkeitsbeschränkungen für das P2P-Filesharing oder das Streamen von Videos und Sperren oder Extragebühren für die Bereitstellung von *Voice-over-Internet-Protocol-Diensten (VoIP)* in mobilen Netzwerken durch eine Reihe von Anbietern.

Dennoch wird die Kommission „… das Jahr 2011 damit verbringen, gemeinsam mit nationalen Telekomregulatoren einen genauen Blick auf gängige Marktpraktiken zu werfen." Danach will Kommissarin Neelie Kroes „… Ergebnisse vorstellen und öffentlich Provider benennen, die sich an zweifelhaften Praktiken beteiligen".

Im Juli 2011 hat der Europäische Rat eine Grundsatzerklärung zur Netzneutralität veröffentlicht[5], in der er die Notwendigkeit eines offenen und neutralen Internet betont[6]. Gleichzeitig fordert er einen digitalen Markt, der erschwingliche und sichere Kommunikation mit hoher Bandbreite und umfangreiche Inhalte und Dienste anbietet.

ACTA

Ein stark diskutiertes Thema auch auf europäischer Ebene ist die Debatte um die Immaterialgüter-Rechte: das *geistige Eigentum* – ein Thema, bei dem verschiedene Interessen aufeinanderprallen.

Aktuell debattiertes Abkommen ist das *Anti-Counterfeiting Trade Agreement – ACTA*. ACTA ist ein Handelsabkommen, das auf *TRIPS (Trade-Related aspects of Intellectual Property rightS)* basiert und Regelungen vorgibt für:

- Internationale Kooperation,
- Abstimmung des Gesetzesvollzugs,
- Schaffung neuer Gesetze zur Verwertung geistigen Eigentums[7].

Eine wesentliche Eigenschaft von ACTA ist, dass auch Anbieter für Urheberrechts-Verletzungen ihrer Kunden als Störer haftbar gemacht werden können. Das führt dazu, dass sie den Internet-Verkehr ihrer Kunden überwachen und bei Verletzungen des Urheberrechts gemäß dem *Three-Strikes*-Prinzip den Zugang zum Internet sperren müssen. Überwachung und Sperrung werden von Bürgerrechtsvereinigungen als Verletzung von Privatsphäre und Grundrechten heftig kritisiert. Der Vertrag erlaubt es Regierungen, „einen Online-Service-Provider anzuweisen, ausreichende … Informationen preiszugeben, um einen Kunden, der der Verletzung des Marken- oder Urheberrechts oder verwandter Rechte beschuldigt wird, identifizieren zu können"[8]. Damit führt ACTA nicht nur durch die Sperrung des Internet-Zugangs zu Eingriffen in die Grundrechte, sondern gefährdet durch die erforderliche Überwachung des Datenverkehrs auch die Privatsphäre.

Darüber hinaus wurde das Zustandekommen der Vereinbarungen kritisiert: Die Verhandlungen fanden lange Zeit unter Ausschluss der Öffentlichkeit statt; im März 2010 forderte das Europäische Parlament die EU-Kommission auf, über die Verhandlungen zu ACTA zu informieren.

Vor allem die US-Regierung macht aber Druck, dass ACTA noch im Jahr 2011 vom Europäischen Parlament verabschiedet wird. Dagegen wehrte sich beispielsweise der mexikanische Senat.

Software-Patente

Breit diskutiert und kritisiert wurde vor einigen Jahren die damals geplante Richtlinie zu Software-Patenten – bis das europäische Parlament ihr mit deutlicher Mehrheit ein Ende setzte. Gegner hatten damals vor allem davor gewarnt, dass es durch die Patentierung kaum noch möglich sein würde, Software zu erstellen, ohne eine Vielzahl von Patenten zu verletzen. Bedingt würde das insbesondere durch Trivialpatente, bei denen bereits simple Ideen – beispielsweise der Fortschrittsbalken in der Benutzeroberfläche eines Software-Systems – patentiert werden konnten. Die Kritiker verwiesen auf die in den USA bereits übliche Praxis. Die daraus resultierende Rechtsunsicherheit stelle ein massives Innovationshemmnis dar. Außerdem begünstige es große Unternehmen gegenüber kleinen, die keine teuren Patentanwälte beschäftigen könnten[9].

Doch möglicherweise ist das Thema noch nicht erledigt – in Form des europäischen Patents könnte es durch die Hintertür zurückkehren. Nach einer Empfehlung des Rechtsausschusses (JURI) hat sich das Europäische Parlament am 15. Februar 2011 über eine verbesserte Zusammenarbeit bei der Entwicklung eines einheitlichen Patentsystems in der EU geeinigt[10].

Die *Free Software Foundation Europe* (FSFE) kritisiert in dem Zusammenhang,, dass „Software-Patente die Innovation beeinträchtigen und eine unnötige Belastung für europäische Softwareentwickler darstellen. … Der Gesetzgeber muss die Führung übernehmen und sicherstellen, dass das Patentsystem zum Gemeinwohl beiträgt. Wie das Europäische Patentamt festgestellt hat, kann diese Entscheidung nicht der Bürokratie oder der Justiz überlassen werden[11]."

Netzsperren

Netzsperren werden derzeit in zwei Varianten diskutiert:

- Netzsperren als Sperrung einzelner Websites und Domains, um den Zugriff auf illegale Inhalte zu verhindern. Begonnen hat diese Debatte mit den Plänen, Seiten mit pornografischen Darstellungen von Kindern zu verhindern. Um diese Netzsperren soll es hier gehen.

- Netzsperren für Einzelpersonen, um deren Internet-Zugriff zu unterbinden. Diese Variante wird – meist als *Three-Strikes*-Regelung im Zusammenhang mit Urheberrechts-Verletzungen (siehe beispielsweise oben zu ACTA) diskutiert.

In Deutschland kennt man das Thema Netzsperren vor allem im Zusammenhang mit dem durch die damalige Bundesfamilienministerin Ursula von der Leyen initiierten *Zugangserschwerungsgesetz,* einem Gesetz, das in Netzkreisen heftig kritisiert wurde und letztendlich – obwohl vom Bundestag beschlossen – nicht zur Anwendung kam. *Löschen statt sperren* gilt nun als der richtige Weg, das Internet von kriminellen Inhalten zu befreien. Mittlerweile ist das Gesetz auch formal vom Tisch: Am 5. April 2011 haben sich die Koalitionsparteien CDU/CSU und FDP darauf geeinigt, das Zugangserschwerungsgesetz fallen zu lassen.

Nachdem in Deutschland weitgehende Einigkeit darüber herrschte, dass das Zugangserschwerungsgesetz nicht nur schädlich für die Bürgerrechte, sondern auch nutzlos für den angestrebten Zweck ist, kam eine neue Initiative von der EU: Innenkommissarin Cecilia Malmström propagierte eine Richtlinie, die genau die in Deutschland gerade verworfenen Netzsperren wieder in die Diskussion brachte.

In Frankreich sorgt das Gesetz *Loppsi 2* (*Loi d'orientation et de programmation pour la performance de la sécurité intérieure*) für die Einführung von Netzsperren[12]. Es wurde am 8. Februar 2011 verabschiedet und ermöglicht ohne richterliche Genehmigung die Sperrung von Internet-Zugängen zu Seiten mit angeblich *offensichtlich* kinderpornografischen Inhalten .

Auch im Zusammenhang mit der Sicherheit des Cyberspace werden Netzsperren diskutiert. So wurden Forderungen nach einem *virtuellen Schengen* laut; an virtuellen Zugangspunkten sollen Internet-Provider unerlaubte Inhalte auf Basis einer EU-Blacklist abwehren[13].

Auf europäischer Ebene werden Netzsperren durch das Projekt *CIRCAMP – COSPOL Internet Related Child Abusive Material Project* – vorangetrieben. Das Projekt hat das Ziel, die kommerzielle und organisierte Verbreitung dokumentierten Kindes-

missbrauchs zu bekämpfen. Es ist eins von vielen Projekten des Programms *COSPOL – Comprehensive Operational Strategic Planning for the Police* – zur Bekämpfung grenzübergreifender Kriminalität in Europa.

Überwachung

Fluggastdaten-Abkommen

Begründet mit der Bekämpfung des Terrorismus fordern vor allem US-Behörden den Zugriff auf die *Passenger Name Records (PNR)*. Dieser Zugriff wird durch das Fluggastdaten-Abkommen geregelt. Es geht dabei um einen umfangreichen Satz teilweise sensibler, personenbezogener Daten; damit ist die Privatsphäre von Fluggästen von einem solchen Abkommen massiv betroffen. Dagegen wird angezweifelt, dass die Übermittlung der Daten tatsächlich einen Mehrwert bei der Verfolgung von Terroristen bringe[14].

Die Diskussion über das Fluggastdaten-Abkommen dauert seit Längerem an. Das frühere Abkommen wurde 2004 durch den EuGH zurückgewiesen[15]. Zuletzt debattierte das Europäische Parlament in seiner Sitzung am 4. Juli 2011 über das Thema[16]. Zuvor hatte bereits der Juristische Dienst der Europäischen Kommission davor gewarnt, dass der vorliegende Entwurf zum Abkommen nicht mit den Grundrechten vereinbar sei[17].

Richtlinie zur Vorratsdatenspeicherung

Auf eine europäische Richtlinie geht auch die Vorratsdatenspeicherung zurück[18]. Mit Datum vom 15. März 2006 wurde die Richtlinie 2006/24/EG ausgefertigt, *über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden*[19]. Bereits am 14. Dezember 2005 hatte das EU-Parlament die Richtlinie mit 387 Ja- gegen 204 Nein-Stimmen beschlossen[20], der Europäische Rat (Ministerrat der Innen- und Justizminister) zog am 21. Februar 2006 nach[21].

Am 19. März 2008 hatte dann ein Eilantrag in Verbindung mit einer Verfassungsbeschwerde gegen die Vorratsdatenspeicherung teilweise Erfolg[22]: Zwar wurden die Daten weiterhin auf Vorrat erhoben, die Verwendung wurde aber auf bestimmte Straftaten eingeschränkt.

Und auch im Hauptverfahren wurde der Verfassungsbeschwerde – zumindest ihren Buchstaben nach – vollständig stattgegeben[23]. Die Vorratsdatenspeicherung an sich wurde aber – entgegen den Hoffnungen Vieler – nicht verworfen; das Bundesverfassungsgericht hält eine verfassungsmäßige Umsetzung für möglich. Darauf berufen sich auch die immer wieder aufkommenden Forderungen nach einer erneuten Umsetzung immer dann, wenn ein vorangegangenes Ereignis eine erhöhte Akzeptanz für derartige Forderungen vermuten lässt.

Die Umsetzung der Vorratsdatenspeicherung wurde in mehreren weiteren Mitgliedsstaaten durch deren Verfassungsgerichtshöfe für nicht verfassungsgemäß erklärt, so zum Beispiel in Rumänien, Zypern und Tschechien. Gleichzeitig strengte die EU Vertragsverletzungs-Verfahren bei nicht erfolgter Umsetzung an. Auch der europäische Datenschutzbeauftragte Peter Hustinx hat mittlerweile in einer Stellungnahme die Datenschutzkonformität der Richtlinie angezweifelt[24].

Eine Untersuchung, die das Bundeskriminalamt am 26. Januar 2011 veröffentlicht hatte, kommt ebenfalls zu dem Schluss, dass eine Vorratsspeicherung von Telekommunikationsdaten bei der Verfolgung schwerer Straftaten nicht von Nutzen ist. Eine vom *Arbeitskreis Vorratsdatenspeicherung* veröffentlichte Analyse hat offenbart, dass die Vorratsdatenspeicherung, solange sie in Kraft war, die Aufklärung schwerer Straftaten nicht verbessert hat[25].

INDECT

Auch im Bereich der universitären Forschung wird an der Überwachung der europäischen Bürger gearbeitet: Das Projekt INDECT – *Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment* – zielt darauf, den Sicherheitsbehörden neue Werkzeuge zur effizienten und effektiven Überwachung und Strafverfolgung zur Verfügung zu stellen[26].

Die Projektziele auf der offiziellen Homepage wirken im englischen Original etwas gestelzt formuliert und lauten übersetzt[27]:

- Entwicklung einer Plattform für die Erfassung und den Austausch von Betriebsdaten, Sammlung von Multimedia-Inhalten, intelligente Verarbeitung von allen Informationen und automatisches Entdecken von Bedrohungen und Erkennung von abnormalem Verhalten oder Gewalt,
- Entwicklung eines Prototyps für ein integriertes, netzwerkzentriertes System, das die operative Polizeiarbeit unterstützt, Bereitstellen von Techniken und Werkzeugen zur Überwachung verschiedener mobiler Objekte,
- Entwicklung eines Suchmaschinen-Typus, der die direkte Suche nach mit Wasserzeichen markierten Bildern und Videos mit der Speicherung von Metadaten verbindet.

Zu INDECT siehe auch den Beitrag von *Sylvia Johnigk* und *Kai Nothdurft* auf Seite 50 in diesem Heft.

SWIFT-Abkommen

Das SWIFT-Abkommen sieht vor, dass *SWIFT – Society for Worldwide Interbank Financial Telecommunication* – Finanztransaktionsdaten an die USA übermittelt, wo sie im Rahmen des *Programms zur Aufdeckung der Terrorfinanzierung (TFTP)* genutzt werden.

Am 8. Juli 2010 hatte das Europäische Parlament das heute gültige Abkommen gebilligt, nachdem es eine erste Fassung zunächst abgelehnt hatte. Bei einer Überprüfung der Umsetzung des Abkommens ist nun aufgefallen, dass keine Kontrolle der Datenübermittlung stattgefunden hat[28]. Im Widerspruch zum Abkommen waren die Anfragen abstrakt formuliert und betrafen mehrere Arten von Daten. Außerdem wurden viele Infor-

mationen nur mündlich ausgetauscht, ohne schriftliche Anfrage, wodurch eine effektive Überprüfung der Datenschutzbestimmungen unterlaufen wird.

Nacktscanner

Heftige Diskussionen löste anfangs die Einführung von Nacktscannern – akzeptanzfördernd auch Bodyscanner genannt – aus. Bis hin zu den Kirchen wurde der durch die Geräte vorgenommene Eingriff in die Menschenwürde kritisiert. Befürworter verwiesen auf gesteigerte Sicherheit. Mittlerweile wurden einige Praxistests an Flughäfen durchgeführt; in Deutschland beispielsweise am Flughafen Hamburg[29].

Die Abgeordneten des Europäischen Parlaments befürworten den Einsatz von Nacktscannern auf freiwilliger Basis. Voraussetzung dafür ist, dass die Geräte weder die Privatsphäre der Passagiere beeinträchtigen noch ihre Gesundheit gefährden[30].

Datenschutz

Bereits 1995 wurde die europäische Datenschutz-Richtlinie erlassen: Die Richtlinie 95/46/EG regelt seither den Datenschutz in der Europäischen Union; in Deutschland umgesetzt durch das Bundesdatenschutzgesetz (BDSG). Der Niederländer Peter Hustinx wacht als Datenschutzbeauftragter über die Einhaltung.

Aktuell ist eine Reform der Datenschutzrichtlinie geplant. Dazu wurde Ende 2010 eine öffentliche Konsultation durchgeführt, bei der Bürger und Organisationen ihre Anforderungen an eine neue Datenschutzrichtlinie mitteilen konnten.

In einer Stellungnahme weist EDRi unter anderem auf folgende Probleme im Zusammenhang mit der Datenschutzrichtlinie hin[31]:

- Rückläufige Datenverarbeitungskosten führen zur Sammlung und Verarbeitung von immer mehr Daten. Gesetzliche Bestimmungen müssen einen gerechten Ausgleich schaffen, sonst würde diese Entwicklung immer größere Risiken für personenbezogene Daten mit sich bringen.

- Das Vorgehen der Mitgliedsstaaten bei der staatlichen Verarbeitung personenbezogener Daten müsse in Einklang stehen mit der Handhabung, wie sie von privaten Unternehmen erwartet wird, es gebe aber viele Gegenbeispiele: Fälle von elektronischen Patientenakten, E-Government- und Bezahlsysteme im Bereich des öffentlichen Verkehrs, wo das Prinzip des eingebauten Datenschutzes und der Datensparsamkeit sowie andere elementare Grundsätze keine Berücksichtigung fänden.

- Kritisiert wird die breite Akzeptanz der Empfehlung über Profiling, wodurch im Grunde gebilligt würde, dass europäische Regierungen das wichtigste Grundprinzip des Datenschutzes und des Schutzes der Privatsphäre aufgäben.

- Bei der Datenverarbeitung durch Unternehmen begrüßt EDRi, dass etwa die Datensparsamkeit, das Recht auf Vergessen, das Recht auf Zugang und Löschung zu Daten vorgesehen sind, stellt aber fest, dass viele dieser Rechte bereits jetzt gesetzlich festgelegt sind. Zu klären sei nun, warum diese Rechte bisher nicht durchgesetzt werden konnten.

Auch das FIfF hat eine Stellungnahme bei der Konsultation abgegeben[32].

Innen- und Sicherheitspolitik

Alle fünf Jahre werden Programme zur Weiterentwicklung der gemeinsamen europäischen Innen- und Sicherheitspolitik aufgesetzt. Aktuelles Programm ist das *Stockholm-Programm*, das während der schwedischen Ratspräsidentschaft 2009 entwickelt wurde. „Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger" – so ist das Fünfjahresprogramm überschrieben, das die Innen- und Justizpolitik der Europäischen Union bis 2014 vorgeben soll.

Leitbild soll der *Aufbau eines Europas der Bürger* sein; als politische Prioritäten werden im Text des Programm genannt:

- Förderung der Rechte der Bürger – Europa als Garant der Grundrechte und Grundfreiheiten,

- Erleichterungen für die Bürger – Europa als Raum der justiziellen Zusammenarbeit,

- Schutz der Bürger – ein Europa, das Schutz bietet,

- Förderung des gesellschaftlichen Zusammenhalts – ein Europa der Solidarität.

Schaut man sich das Programm genauer an, so findet man unter anderem Instrumente wie Ausweisregistrierung, Internet-Überwachung, Grenzübergangssysteme mit Nutzung biometrischer Daten und Profile zur Risiko-Einschätzung von Einzelpersonen[33]:

- Zentrales Instrument der Asyl- und Einwanderungspolitik ist die Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen (FRONTEX). Über FRONTEX soll die operative Zusammenarbeit unter den Mitgliedsstaaten zur Grenzsicherung verbessert werden. Wesentlicher Teil davon ist der übergreifende Datenaustausch; Werkzeuge dafür sind das Visa-Informationssystem (VIS) und das Schengener Informationssystem der zweiten Generation (SIS II).

Stefan Hügel

Stefan Hügel ist Vorsitzender des FIfF, arbeitet als IT-Berater und lebt in Frankfurt am Main

- Einen *echten Mehrwert* bietet die EU nach Ansicht der Kommission, wenn es um die Bekämpfung *bestimmter Bedrohungsarten* geht: Organisierte Kriminalität und Terrorismus. Dazu soll die übergreifende Zusammenarbeit weiter ausgebaut werden: beispielsweise durch die Weiterentwicklung der Europäischen Polizeiakademie (CEPOL), durch Polizei- und Zollkooperationen an den Binnengrenzen und durch gemeinsame Ermittlungsgruppen auf Grundlage vor allem des EU-Rechtshilfeabkommens.

- Information sei der Schlüssel zum Schutz der zunehmend vernetzten Welt. Das Programm antwortet darauf mit dem Prinzip der Verfügbarkeit: Der Informationsaustausch zwischen den damit befassten Behörden und damit die Verfügbarkeit der Informationen zur Kriminalitätsbekämpfung.

Das Stockholm-Programm wurde im Dezember 2009 beschlossen[34].

Anmerkungen

1 Wikipedia, Stichwort Netzneutralität, http://de.wikipedia.org/wiki/Netzneutralität (Abruf aller Internet-Quellen am 9. August 2011)
2 The Netherlands – first EU country to launch net neutrality, EDRi-gram 9.13, 29. Juni 2011, http://www.edri.org/edrigram/number9.13/net-neutrality-netherlands (alle Artikel des EDRi-gram finden sich auch in deutscher Übersetzung unter http://www.unwatched.org)
3 The Netherlands first country in Europe to launch net neutrality, Pressemitteilung, Bits of Freedon, 22. Juni 2011, https://www.bof.nl/2011/06/22/press-release-–-the-netherlands-first-country-in-europe-to-launch-net-neutrality/
4 European Commission's Net Neutrality report, EDRi-gram 9.8, 20. April 2011, http://www.edri.org/edrigram/number9.8/european-commission-net-neutrality-report
5 Draft Council Conclusions on Net Neutrality, Council of the European Union, http://register.consilium.europa.eu/pdf/en/11/st12/st12950.en11.pdf
6 Draft Council conclusions on Net Neutrality, EDRi-gram 9.15, 27. Juli 2011, http://www.edri.org/edrigram/number9.15/net-neutrality-council-conclusions
7 Wikipedia, Stichwort ACTA, http://de.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement
8 The US pressures the EU to pass ACTA before the end of 2011, EDRi-gram 9.4, 23. Februar 2011, http://www.edri.org/edrigram/number9.4/us-pushes-acta-european-parliament
9 Software-Patente, FIfF-Kommunikation 4/2003, Schwerpunktthema
10 Is the EU going to have a new common patent law? EDRi-gram 9.4, 23. Februar 2011, http://www.edri.org/edrigram/number9.4/towards-a-european-patent-law
11 Is the EU going to have a new common patent law? EDRi-gram 9.4, 23. Februar 2011, http://www.edri.org/edrigram/number9.4/towards-a-european-patent-law
12 France: Loppsi 2 adopted – Internet filtering without court order, EDRi-gram 9.4, 23. Februar 2011, http://www.edri.org/edrigram/number9.4/web-blocking-adopted-france-loppsi-2
13 The „Virtual Schengen Border" or „The Great Firewall of Europe", EDRi-gram 9.9, 4. Mai 2011, http://www.edri.org/edrigram/number9.9/virtual-schengen-border
14 Konsens für Passagierdatenspeicherung in der EU gesucht, Heise.de, 14. Juli 2011, http://heise.de/-1279257
15 Urteil: Keine Rechtsgrundlage für Fluggastdatenweitergabe an USA, Heise.de, 30. Mai 2006, http://heise.de/-128128
16 EP discussions in international agreements on passenger name records, EDRi-gram 9.14, 13. Juli 2011, http://www.edri.org/edrigram/number9.14/pnr-debates-european-parliament
17 EU-US PNR agreement found incompatible with human rights, EDRi-gram 9.13, 29. Juni 2011, http://www.edri.org/edrigram/number9.13/us-eu-pnr-breaches-human-rights
18 2006/24/EG. Wenn Politik auf Grundgesetz trifft, Stefan Hügel, FIfF-Kommunikation 2/2010, 30-33
19 Richtlinie 2006/24/EG des europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG. Amtsblatt der Europäischen Union L 105 vom 13. April 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF
20 EU-Parlament beschließt massive Überwachung der Telekommunikation. Heise.de, 14.12.2005, http://www.heise.de/newsticker/meldung/EU-Parlament-beschliesst-massive-ueberwachung-der-Telekommunikation-157997.html
21 EU-Rat nickt Richtlinie zur Vorratsdatenspeicherung ab. Heise.de, 21.02.2006, http://www.heise.de/newsticker/meldung/EU-Rat-nickt-Richtlinie-zur-Vorratsdatenspeicherung-ab-177825.html
22 1 BvR 256/08 vom 11. März 2008, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html
23 1 BvR 256, 263, 586/08 vom 2. März 2010, http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html
24 EDPS: Data Retention Directive fails to meet data protection requirements, EDRi-gram 9.11, 1. Juni 2011, http://www.edri.org/edrigram/number9.11/data-retention-directive-failure-edps
25 German study finds the data retention ineffective, EDRi-gram 9.3, 9. Februar 2011, http://www.edri.org/edrigram/number9.3/telecom-data-retention-ineffective-german-study
26 INDECT – Ein weiterer Schritt zum Orwellschen Überwachungsstaat? Sylvia Johnigk und Kai Nothdurft, FIfF-Kommunikation 1/2010, 62-65
27 http://www.indect-project.eu
28 Implementation of the SWIFT agreeement under review, EDRi-gram 9.8, 20 April 2011, http://www.edri.org/edrigram/number9.8/review-implementation-swift
29 Nacktscanner-Test am Hamburger Flughafen startet am 27. September, Heise.de, 16. September 2010, http://heise.de/-1080628
30 MEPs approve body scanners on a voluntarily basis, EDRi-gram 9.11, 1. Juni 2011, http://www.edri.org/edrigram/number9.11/body-scanners-airports-ep
31 EDRi responds to data protection consultation, EDRi-gram 9.2, 26. Januar 2011, http://www.edri.org/edrigram/number9.2/edri-data-protection-legislation
32 Novellierung der Datenschutz-Richtlinie, Stellungnahme zur EU-Konsultation, FIfF-Kommunikation 1/2011, 5-10
33 Stockholm Programme – The New EU Dangerous Surveillance Systems, EDRi-gram 7.12, http://www.edri.org/edri-gram/number7.12/stockholm-programme-eu-surveillance
34 Mehr Sicherheit um jeden Preis. Das Stockholmer Programm der Europäischen Union, Christine Wicht, Blätter für deutsche und internationale Politik 3/2010, 91-98, auch unter http://www.eurozine.com/pdf/2010-03-24-wicht-de.pdf

Alexander Alvaro MdEP

Aktuelle Herausforderungen europäischer Netzpolitik

Das Internet hat das Leben der Menschheit in den letzten Jahren so stark verändert, wie kaum eine Erfindung zuvor. Nicht nur in unserem täglichen Leben, sondern auch bei politischen Umbrüchen, wie dem „Arabischen Frühling" spielt die Kommunikation über das Internet eine entscheidende Rolle. Diese Entwicklung ist gleichzeitig eine Chance und Herausforderung für die Politik und die Gesellschaft als Ganzes. Beispielhaft hierfür sind vor allem die Themen Vorratsdatenspeicherung, Internetsperren und der Datenschutz im Internet.

Ungefähr 99% der 14-29jährigen benutzen Umfragen zufolge regelmäßig das Internet[1]. In der gleichen Altersgruppe lässt sich zunehmend ein steigender Grad an Politikverdrossenheit beobachten. Die Politik hat es bisher nicht ausreichend vermocht, sich dieser Entwicklung entgegenzustellen. Im Gegenteil: Viele Bürger resignieren aufgrund unverständlicher Entscheidungsprozesse oder mangelnder Kommunikation. Werden Entscheidungen immer öfter als „alternativlos" dargestellt, um jeglichen Diskurs zu vermeiden, trägt das nicht nur zur weiteren Frustration der Bevölkerung über die Politik bei, sondern behindert auch den öffentlichen Diskurs, von dem eine gesunde Demokratie lebt. Das Internet kann hier einen großen Beitrag leisten, um den Kontakt zwischen Bevölkerung und Politik wieder zu verstärken. Sicherlich ist das Internet nicht der Heilige Gral, der alle Probleme der Politik löst, aber es ist durchaus zu beobachten, dass eine große Zahl der Bürger sich über soziale Netzwerke und andere Plattformen organisiert, wodurch die Möglichkeit und Bereitschaft zur politischen Diskussion gefördert wird.

Aufgrund dieser immer stärkeren Stellung des Internets wird es zunehmend wichtiger, dass wir das Internet nicht als einen rechtsfreien Raum begreifen – was es auch nicht ist. Es ist wichtig, dass Bürger auch im Internet geschützt werden, ohne jedoch die Freiheit der Internetnutzer, aus der das hohe innovative Potential dieses Mediums stammt, ungerechtfertigt einzuschränken. Am großen Widerstand der Bevölkerung gegen die europäische Richtlinie zur Vorratsdatenspeicherung konnten wir beobachten, wie wichtig den Menschen ihre Rechte in dieser Hinsicht sind.

Das Bundesverfassungsgericht hat, wie mehrere Verfassungsgerichte in anderen Mitgliedsstaaten der EU, die nationale Umsetzung der Richtlinie für verfassungswidrig erklärt. Auch der Evaluierungsbericht der Europäischen Kommission zur Umsetzung und den Auswirkungen der Richtlinie hat gezeigt, dass weder ein Sicherheitsgewinn noch eine Harmonisierung der Rechtslagen innerhalb der Union zu beobachten ist. Wenn jetzt ein Vertragsverletzungsverfahren wegen Nichtumsetzung der Richtlinie gegen Deutschland eingeleitet wird, noch bevor eine Revision auf europäischer Ebene geschehen ist, grenzt das an Realitätsverweigerung seitens der Europäischen Kommission. Dogmatik vor Pragmatik lautet die Botschaft aus der Kommission.

Bei der Bekämpfung von Kindesmissbrauch im Internet hingegen konnte sich das effektivere und praktikable Vorgehen des „Löschen statt Sperren" durchsetzen.

Gutachten haben gezeigt, dass eine Zensur verdächtiger Inhalte weder technisch sinnvoll ist, noch sicherstellt, dass betroffene Seiten aus dem Internet verschwinden[2]. Wenn man den Opferschutz und die Bekämpfung der Kinderpornografie wirklich ernst nimmt, muss man dafür sorgen, dass die Inhalte aus dem Internet entfernt werden und vor allen Dingen gegen die Verantwortlichen vorgegangen wird. Viele der Server, auf denen sich kinderpornografisches Material befindet, liegen in den USA und Westeuropa und somit durchaus in unserem Einflusskreis. Der Innenausschuss des Europäischen Parlaments hat sich dieser Auffassung angeschlossen und wir konnten so in den Verhandlungen zur Richtlinie zur Kindesmissbrauchsbekämpfung durchsetzen, dass die Mitgliedsstaaten verpflichtet werden, Seiten mit kinderpornografischem Inhalt zu löschen, wenn sich die Server in ihrem eigenen Hoheitsgebiet befinden, sowie sich dafür einzusetzen, dass gegen diese Seiten auf Servern in Drittstaaten vorgegangen wird.

Neben der Vorratsdatenspeicherung und den Internetsperren muss weiterhin auch die Revision der Datenschutzrichtlinie genau beobachtet werden. Der technische Wandel hat sich gerade in den letzten Jahren rasant vollzogen und soziale Netzwerke und digitale Kommunikationsmittel haben Einzug in unser aller Leben gefunden. Mit dem Fortschreiten der Technik ist es nur richtig, dass die Datenschutzrichtlinie aus dem Jahre 1995 aktualisiert wird. Es muss sichergestellt sein, dass persönliche Daten der Bürger vor Missbrauch geschützt werden und Unternehmern Rechtssicherheit geboten wird. Um dieser Herausforderung mit einem guten gesetzlichen Rahmen begegnen zu können, ist es von größter Bedeutung, dass drei Hauptkriterien erfüllt werden: Zum einen muss die neue Richtlinie technikneutral formu-

Alexander Alvaro

Alexander Alvaro ist seit 2004 Mitglied des Europäischen Parlaments und seit 2009 Vizepräsident des Haushaltsausschusses, sowie innenpolitischer Sprecher der FDP im Europäischen Parlament. Seit 2011 ist er Mitglied des Präsidiums der FDP.

liert sein, um Flexibilität zu gewährleisten, sie muss sich an langfristigen Zielen orientieren und zeitgemäß sein.

Es gilt also, den richtigen Rahmen dafür zu schaffen, dass sich jeder Bürger frei, aber sicher im Netz bewegen kann und das Internet weiterhin eine Quelle des gesellschaftlichen Fortschritts bleibt.

Anmerkungen

1 *ARD-ZDF Online Studie 2011, www.ard-zdf-onlinestudie.de*

2 *Arbeitskreis gegen Internet-Sperren und Zensur, www.ak-zensur.de*

Jan-Philipp Albrecht MdEP

Rechtsdurchsetzung im Internet

Zahlreiche politische Reaktionen, die angesichts der Attentate in Norwegen ohne Schonfrist in der Europäischen Union und insbesondere in Deutschland aufkamen, zeigen Unkenntnis und Unvermögen, wenn es darum geht, als Staat die Herausforderungen einer globalisierten und digitalisierten Gesellschaft zu bewältigen. Symbole der Auseinandersetzung sind vor allem die folgenden drei: Die anlasslose Vorratsdatenspeicherung aller Telekommunikationsdaten, die Sperrung von Internetseiten mit illegalen oder gefährlichen Inhalten und die Reduzierung der Möglichkeiten anonymen Handelns im weltweiten Netz. Die politische Rechte und die Innenpolitiker von Union und SPD verbreiten den Eindruck, dass diese drei Maßnahmen die Radikalisierung und die Gewalteskalation einzelner verhindern könnten. Dass sich diese These schon seit vielen Jahren als falsch herausgestellt hat, spielt in den Köpfen dieser Politiker offenbar keine Rolle. Auf Kosten der Freiheit und auf Kosten der Sicherheit in Europa und der Bundesrepublik. Denn statt sich mit den wahren Ursachen der gegenwärtigen Probleme zu befassen, werden die Prioritäten in der Innen- und Sicherheitspolitik komplett falsch gesetzt. Noch dazu vor dem Hintergrund einer massiven Erosion staatlicher Regelungsgewalt, die sich sicherlich nicht durch deutsche Gesetze für das weltweite Netz wird verhindern lassen.

Die eingeforderten Vorhaben sind ebenso sehr umstritten wie sie von einer Lösung des Problems entfernt sind. Sie sind der populistische Griff in die Werkzeugkiste des Polizeistaates. Dabei stellen Globalisierung und Digitalisierung die Polizeiarbeit und die innere Sicherheit vor Herausforderungen, die weitaus komplexere Antworten erfordern. Es können noch so viele Sicherheitsagenturen und Überwachungsmaßnahmen auf EU-Ebene verabschiedet werden; wenn die Polizei vor Ort in einigen Dienststellen nicht einmal eine ausreichende Ausstattung mit guten Internetanschlüssen oder IT-Forensik hat, wird es auch in Zukunft keine bessere Aufklärungsquote bei Straftaten mit Internetbezug geben. Das Internet ist keine neue Welt, sondern eine Erweiterung der Bestehenden, die zwar grenzübergreifende Regeln, aber keine neuen Erfindungen von Politikern braucht. Und wenn die Mittel für die Streifenpolizei gerade im ländlichen Raum immer weiter gekürzt werden, um auf Bundes- und EU-Ebene noch mehr Gelder in die wenig hinterfragte Bekämpfung des internationalen Terrorismus zu stecken, rückt eine Senkung der realen Kriminalitätsraten in weite Ferne. Gerade auf europäischer Ebene müssen endlich neue Wege gedacht werden, um den Ursachen von Kriminalität im digitalen Zeitalter besser vorzubeugen und Straftaten schneller aufzudecken und zu verhindern. Auch in der noch immer bestehenden analogen Welt funktioniert effektive Polizeiarbeit ohne generelle Platzverbote, Nummernschilder auf der Stirn und Totalüberwachung.

Die Innenminister von Union und SPD haben seit Jahren eine Politik der schnellen Effekte und der falschen Prioritätensetzung betrieben. Es ist kein Wunder, dass immer mehr Menschen diese Parteien nicht mehr als Vertreter einer sinnvollen Politik der inneren Sicherheit sehen. Sie wollen eine Gesellschaft, die tatsächlich sicher ist und keinen Überwachungsstaat mit Sicherheitsgefühl. Statt teure Körperscanner an Flughäfen oder immer neue Datensammlungen anzulegen, muss endlich wieder in

Jan Philipp Albrecht

Jan Philipp Albrecht gehört zum Jahrgang 1982 und ist damit der jüngste deutsche Abgeordnete im Europäischen Parlament. Der ehemalige Sprecher der Grünen Jugend hat sich dort insbesondere mit seinem Einsatz für Datenschutzthemen binnen kurzer Zeit als Grüner Innen- und Justizexperte hervorgetan. Albrecht hat von 2003 bis zu seiner Wahl 2009 Rechtswissenschaften in Bremen, Brüssel und Berlin sowie Rechtsinformatik in Hannover und Oslo studiert. Bereits seit 1999 hat sich Albrecht auf verschiedensten Ebenen bei den Grünen engagiert. Der gebürtige Braunschweiger vertritt die norddeutschen Grünen im Europaparlament und hat Regionalbüros in Hamburg, Hannover und Kiel.

wahre Kriminalitätsbekämpfung investiert werden. Und statt einer Auslagerung vermeintlicher Polizeiarbeit an Internetprovider und Zensurbehörden brauchen wir nicht weniger, sondern mehr Geld und Wertschätzung für den Einsatz gegen menschenverachtendes Gedankengut und die Gestaltung alternativer und sinnstiftender Angebote von Kultur, Medien und Informationsaustausch im Netz. Das heißt konkret: Eine bessere Ausbildung für angehende Polizisten, eine gute Ausstattung der Polizeidienststellen vor Ort und die Stärkung einer aufmerksamen und solidarischen Zivilgesellschaft, in der Anonymität keinen Verdacht auslöst sondern die Schwelle zur Beteiligung senken soll. Absolute Sicherheit ist und bleibt auch nach den schrecklichen Taten in Norwegen eine Illusion. Die reale Senkung von Kriminalitätsraten allerdings wäre zum Greifen nahe. Dazu bedarf es allerdings der richtigen politischen Entscheidungen. In ganz Europa und damit auch in Deutschland.

Tobias Lönnies

Digitale Bürgerrechtsorganisationen in Europa

In vielen gesellschaftlichen Bereichen fallen heute Entscheidungen in den Institutionen der EU, so auch beim Datenschutz, Urheberrecht, der freien Meinungsäußerung im Netz und ähnlichen Themen, die sich unter dem Begriff Digitale Bürgerrechte *zusammenfassen lassen. Um in diesen Institutionen effektiver seine Positionen vertreten zu können, ist das FIfF Mitglied von* **European Digital Rights (EDRi)***, einem Dachverband für Organisationen aus ganz Europa, die sich für digitale Bürgerrechte einsetzen.*

In EDRi sind inzwischen 28 europäische Organisationen zusammengeschlossen, die das gemeinsame Ziel haben, die digitalen Bürgerrechte zu schützen [1]. Das sind vor allem, aber nicht ausschließlich, das Recht auf Privatsphäre, der Schutz der eigenen Daten und das Recht auf freien Informationszugang. EDRi selbst ist in der *FIfF-Kommunikation* 2/2009 beschrieben, dieser Artikel bietet eine Übersicht über die Mitglieder.

Die EDRi-Mitglieder unterscheiden sich in Mitgliederzahl, Organisationsform und Aktivitäten. EDRis mitgliederstärkste Organisation ist beispielsweise *Electronic Frontier Finland* mit über 2000 Mitgliedern [2], andere Organisationen in EDRi haben lediglich drei Mitglieder. Diese Organisationen sind dann nicht als Vereine, sondern meist als Stiftungen organisiert und finanzieren ihre Arbeit über Spenden anstatt über Mitgliedsbeiträge. Eine dritte Organisationsform ist die gemeinnützige Firma, die zu ermäßigten Preisen anderen Organisationen Internet-Dienstleistungen zur Verfügung stellt.

Die Aktivitäten der EDRi-Mitglieder richten sich an zwei Adressaten: In Kampagnen klären sie die Öffentlichkeit auf und lenken die Aufmerksamkeit auf die häufig stark technisch geprägten Probleme der Informationstechnologie. Um dasselbe bei politischen Vertretern zu erreichen, arbeiten viele der Organisationen in politischen Gremien und Kommissionen ihrer Länder mit und teilen dort ihr Expertenwissen. Beide Aktivitäten setzen auf langfristige Überzeugungsarbeit. Wesentlich direkter ist der juristische Weg, jedoch ist er meist nicht einfach zu gehen. Das liegt vor allem am Zeit- und Personalaufwand, der Komplexität der juristischen Verfahren und den zahlreichen nationalen Eigenheiten der europäischen Justizsysteme.

European Digital Rights

Seit EDRis Gründung im Jahr 2002 sind eine Reihe neuer Mitglieder beigetreten. Neben 28 Organisationen als ordentlichen Mitgliedern gibt es mehrere Einzelpersonen mit Beobachterstatus. Die Beobachter repräsentieren mitunter auch Gruppen, die aufgrund ihrer Struktur bzw. ihres juristischen Status nicht ordentliche Mitglieder werden können. Weil EDRi die Anliegen der Mitglieder in den europäischen Institutionen vertritt, befindet sich die Geschäftsstelle in Brüssel. EDRi befasst sich mit wichtiger EU-Gesetzgebung zur Informationstechnologie und dem Internet. Explizit zu nennen sind dabei die Vorratsdatenspeicherung, aber auch Reformen des Urheberrechts und unterschiedlichste Ansätze zu Netzsperren, die Auswirkungen der neuen Technologien auf die Gesellschaft, beispielsweise im Bereich des E-Government oder des Datenschutzes.

Lobbyarbeit im Europa-Parlament ist ein Schwerpunkt, dazu gehört auch die Mitarbeit in den Gremien und Kommissionen der EU-Institutionen. Die Aufklärung der Öffentlichkeit dagegen findet vor allem in Form von Petitionen und offenen Briefen statt. EDRi veröffentlicht einen eigenen zweiwöchentlichen Newsletter auf ihrer Webseite, *EDRi-gram*. Außerdem gibt es im Netz In-

Tobias Lönnies

Tobias Lönnies schreibt zur Zeit seine Abschlussarbeiten in Informatik und Politikwissenschaft an der Uni Bremen. Er war im April und Mai 2011 Praktikant beim FIfF.

formationsmaterial, etwa einen Aufklärungs-Comic zum Thema Datenschutz sowie Broschüren zu weiteren Themen. Weil einem Dachverband eigene Mitglieder fehlen, sind Aktionen mit persönlicher Präsenz selten, es gab aber beispielsweise Demonstrationen auf mehreren europäischen Flughäfen gegen die Weitergabe von Passagierinformationen. Finanziert wird EDRi durch Mitgliedsbeiträge und Spenden [3], vor allem durch eine Großspende des *Open Society Institute* [4].

Dachverbände in Europa und der Welt

EDRi ist der wohl bedeutendste Dachverband dieser Art in Europa, aber auch weitere Organisationen sind europa- und weltweit für digitale Bürgerrechte aktiv.

European Regional At-Large Organization (EURALO) ist der *Internet Corporation for Assigned Names and Numbers (ICANN)* angeschlossen. ICANN ist weltweit zuständig für die Regulierung von Top-Level-Domains und hat mehrere regionale Beratergremien. Diese stellen ein zivilgesellschaftliches Gegengewicht in der von kommerziellen und staatlichen Interessen dominierten ICANN dar. Das FIfF ist dort ebenfalls Mitglied. EURALO beschäftigt sich mit Themen, die die Verwaltung des Internets betreffen, wie der Reform des Domain-Systems und der Herstellung von Transparenz in den ICANN-Entscheidungprozessen [5].

Ebenfalls eine Stimme der Zivilgesellschaft stellt der **Civil Society Information Society Advisory Council (CSISAC)** dar, jedoch der OECD (*Organisation für wirtschaftliche Zusammenarbeit und Entwicklung*) angeschlossen und mit einem breiteren Themenrahmen. Die CSISAC-Mitgliedsorganisationen stammen größtenteils aus den Ländern der OECD und beschäftigen sich neben Themen der Netzpolitik, wie Schutz von Meinungsfreiheit und Privatsphäre, auch mit der Umwelt- und Entwicklungspolitik [6].

In **Association for Progressive Communications (APC)**, haben sich die Mitglieder mit dem Ziel zusammengeschlossen, möglichst vielen Menschen einen Zugang zum Internet zu ermöglichen [7]. **Computer Professionals for Social Responsibility (CPSR)** ist eine US-amerikanische Vereinigung von kritischen Informatikern, wie das FIfF ursprünglich gegründet aus Sorge vor einem möglichen Atomkrieg; inzwischen sind zahlreiche Themen hinzugekommen. Sie ist eine Schwesterorganisation des FIfF und hat in mehreren Ländern und Regionen Ableger, darunter auch in Europa [8].

Die Electronic Frontier Foundation (EFF) und die Internet Society (ISOC) haben in Europa Nachahmer gefunden, wobei die nach EFF Benannten von der US-amerikanischen Zentrale unabhängig und lediglich von ihrer Idee inspiriert sind, während die in den europäischen Ländern gegründeten ISOC-Filialen vom *Open Society Institute* bzw. der *Soros Foundation* finanziert werden. Diese beiden Organisationen sind Teil des gemeinnützigen Stiftungsnetzwerks von Hedgefond-Milliardär *George Soros*, das zahlreiche Bürgerrechtsorganisationen auf der ganzen Welt unterstützt [9].

Electronic Frontier Foundation (EFF) in Europa

Ebenfalls in Brüssel befindet sich das europäische Büro der US-amerikanischen **Electronic Frontier Foundation (EFF)**, das mit EDRi eng zusammenarbeitet. Diese Zusammenarbeit bezieht sich neben den europäischen Themen wie Vorratsdatenspeicherung und Netzsperren auch auf transatlantische Themen wie Urheberrecht, Softwarepatente und das internationale Handelsabkommen ACTA [10]. Im Heimatland USA ist EFF mit zahlreichen Projekten aktiv, darunter *TOSBack*, einem Projekt zur Überwachung von Änderungen in den Nutzungsbedingungen von Webangeboten, *Patent Busting*, bei dem Softwarepatente auf ihre tatsächliche Patentierbarkeit geprüft werden, und der *Takedown Hall of Shame*, die besonders krasse Fälle der Einschränkung der Meinungsfreiheit durch Urheberrechtsklagen anprangert. Des weiteren führt EFF in den USA Aufklärungskampagnen zum Thema Urheberrecht und dem Schutz der eigenen Daten durch, betreibt Lobbyarbeit für eine gesetzliche Regelung der Rechte von Bloggern, insbesondere ihre Gleichstellung mit traditionellen Journalisten, und klärt Programmierer über die juristischen Probleme ihrer Arbeit zum Beispiel beim Aufspüren von Sicherheitslücken auf [11].

Die Mitglieder von EDRi

Im Folgenden werden die Mitgliedsorganisationen von EDRi vorgestellt, ausgenommen die zuvor vorgestellte EFF und das FIfF. Die Informationen stammen von den Organisationen

Name	Liga voor Mensenrechten (LvM) [12]	Bits of Freedom (BoF) [13]	Vrijschrift [14]
Gründungsdatum	1979	2000	2003
bei EDRi seit	2010	2002	2008
Mitgliederzahl	400	250	8
Land (Geschäftsstelle)	Belgien (Gent)	Niederlande (Amsterdam)	Niederlande (Workum)
Themen	Recht auf Privatsphäre (Überwachung am Arbeitsplatz, Videoüberwachung)	Datenschutz, Recht auf Privatsphäre, Meinungsfreiheit, Recht auf Internetzugang	Informationsfreiheit, Urheberrecht, Freie Softwarestandards
in den internationalen Organisationen			

selbst, entweder von ihren Webseiten oder aus Antworten auf Anfragen per E-Mail.

Liga voor Mensenrechten (LvM) aus Belgien ist die älteste Organisation unter den EDRi-Mitgliedern. Sie beschäftigt sich nicht nur mit digitalen Bürgerrechten, sondern auch mit Themen wie Diskriminierung, Rassismus und den Rechten von Strafgefangenen. Im digitalen Bereich konzentrieren sie sich vor allem auf das Thema Schutz der Privatsphäre gegen Eingriffe von staatlicher und privatwirtschaftlicher Seite. Neben Petitionen gegen die Vorratsdatenspeicherung und Aufklärungsarbeit zur Überwachung am Arbeitsplatz haben sie sich dem Thema Videoüberwachung verschrieben. Mit Hilfe der Öffentlichkeit erstellen sie durch *Camera Spotting* eine Karte über alle Überwachungskameras im öffentlichen Raum in Belgien. Sie organisieren die belgische Version der *BigBrotherAwards*.

Bits of Freedom (BoF) war nach eigener Aussage von 2006 bis 2009 inaktiv, wurde aber durch eine Großspende zu neuem Leben erweckt und hat nun drei bezahlte Mitarbeiter. Seitdem hat die Organisation eine Reihe von Erfolgen errungen, beispielsweise eine erfolgreiche Kampagne gegen den Plan, eine Abgabe für das nicht-kommerzielle Einbinden von Videos zu erheben (*Embed Tax*), und eine Kampagne für mehr Transparenz bei Abhörmaßnahmen. Eine weitere öffentlichkeitswirksame Aktion war das *Multatuli Projekt* [15], bei dem gezeigt wurde, wie einfach es ist, Webseiten mit ungerechtfertigten Urheberrechtsbeschwerden zu entfernen. Zur Zeit führt Bits of Freedom Kampagnen gegen die Vorratsdatenspeicherung, für Netzneutralität und gegen einen Zentralspeicher für alle niederländischen Bankdaten durch.

Vrijschrift bedeutet im Niederländischen soviel wie „freies Skript" und folglich setzt sich die Organisation vor allem für freie Software und offene Standards ein. Zu ihren Aktivitäten gehören Kampagnen gegen Softwarepatente und für eine benutzerfreundliche Urheberrechtsreform. Außerdem betreiben sie Projekte für kostenlose Schulbücher, die Übersetzung freier Software ins Niederländische und die Etablierung offener Standards in Behörden.

Open Rights Group (ORG) aus England ist eine der mitgliederstärksten und einflussreichsten digitalen Bürgerrechtsorganisationen in Europa. Sie arbeitet vor allem mit Kampagnen, beispielsweise in der Vergangenheit gegen den Einsatz von DRM, übertriebene Markenschutzklagen der BBC und die Verlängerung des Urheberrechts auf Musik. Aktuelle Kampagnen setzen sich für mehr Datenschutz bei Internet-Werbediensten ein und gegen Netzsperren für Urheberrechtsverletzungen. ORG nimmt an einer Regierungskommission zur Reform des Urheberrechts teil und betreibt Projekte, die staatlich erhobene Daten der Öffentlichkeit zur Verfügung stellen, wie die digitale Bereitstellung des Geburtenregisters für Familienforschung.

Foundation for Information Policy Research (FIPR) ist eine britische Stiftung, die Politikberatung betreibt. Ursprünglich beschäftigte sie sich mit den Auswirkungen neuer Technologien auf Staat und Wirtschaft und dem Urheberrecht, doch wegen der Einschränkung von Bürgerrechten durch Anti-Terrorismus-Gesetze kamen Überwachung und akademische Freiheit als Themen hinzu. In diesen Bereichen hat FIPR auch die bisher größten Erfolge erzielt: die Begrenzung von Überwachungsgesetzen auf schwere Verbrechen und Ausnahmen von der Exportkontrolle für die Wissenschaft.

GreenNet (GN) ist ein gemeinnütziger britischer Internet Service Provider, der bei der Bereitstellung seiner Dienstleistungen ethische und ökologische Maßstäbe anlegt. Neben dem auch für Privatnutzer ermöglichten Internetzugang bietet er spezielle Spam-Filter, Website-Hosting und -Design für gemeinnützige Organisationen.

Digital Rights Ireland (DRI), die führende irische digitale Bürgerrechtsorganisation, ist vor allem durch ihre Klage gegen die Vorratsdatenspeicherung international bekannt. DRI arbeitet vor allem über ein Blog, in dem sie die Öffentlichkeit aufklärt und auf Probleme aufmerksam macht. Dabei berichtet sie ausführlich über Skandale, etwa den Missbrauch der Telefonüberwachung für private Zwecke oder die Weitergabe von Daten aus der Sozialbehörde an private Versicherungen.

Imaginons un Réseau Internet Solidaire (IRIS) setzt vor allem auf die Mobilisierung der Öffentlichkeit. Sie hat zu den meisten französischen Gesetzesvorhaben in ihrem Themenbereich Petitionen und Unterschriftensammlungen gestartet, um so öffentlichen Druck aufzubauen, und organisiert Konferenzen und Gipfel mit.

La Quadrature du Net will keine formale Organisation sein, sondern eine Bewegung, weshalb sie auch nicht Mitglied bei EDRi

Open Rights Group (ORG) [16]	Foundation for Information Policy Research (FIPR) [17]	GreenNet (GN) [18]	Digital Rights Ireland (DRI) [19]
2005	1998	1985	2005
2006	2002	2005	2006
1400	35	8	6
Großbritannien (London)	Großbritannien (Sandy, Bedfordshire)	Großbritannien (London)	Irland (Tipperary)
Datenschutz, Recht auf Privatsphäre, Urheberrecht, staatliche Transparenz	Recht auf Privatsphäre, Urheberrecht, Auswirkungen neuer Technologien, Forschungsfreiheit	Recht auf Internetzugang, friedliche und ökologische Nutzung von Technik	Datenschutz, Recht auf Privatsphäre, Auswirkungen neuer Technologien
CSISAC		CSISAC, APC	

Name	Imaginons un Réseau Internet Solidaire (IRIS) [20]	La Quadrature du Net [21]	Comunicació per a la Cooperació (Pangea) [22]
Gründungsdatum	1997	2008	1993
bei EDRi seit	2002		2007
Mitgliederzahl	6	-	400
Land (Geschäftsstelle)	Frankreich (Paris)	Frankreich (-)	Spanien (Barcelona)
Themen	Urheberrecht, Auswirkungen neuer Technologien, Recht auf Internetzugang	Datenschutz, Recht auf Privatsphäre, Urheberrecht	Recht auf Privatsphäre, Auswirkungen neuer Technologien, Geschlechterfragen
in den internationalen Organisationen	CSISAC		CSISAC, APC

ist. Jedoch hat ihr Mitgründer Jérémie Zimmerman Beobachterstatus. Er ist auch einer von drei Sprechern, die als Einzige im Namen der Bewegung sprechen dürfen. An den Projekten der Gruppe kann und soll sich jede/r Interessierte beteiligen. Dazu gehören neben einem Wiki mit Informationen zu netzpolitischen Themen eine Mediendatenbank, ein Werkzeug zum Vergleich von Gesetzestexten und eine Datenbank über das Abstimmverhalten der Mitglieder des Europa-Parlaments.

Comunicació per a la Cooperació (Pangea) und **Nodo50.org** stellen anderen Organisationen und Aktionsbündnissen ihre Internet-Dienstleistungen und Technik zur Verfügung. Beide verbreiten zur Verfügung gestellte Aufrufe ihrer Kunden über Aktionen oder Demonstrationen sowie Stellungnahmen und Artikel darüber auf ihrer jeweiligen Website. Das Ziel ist eine weitere Vernetzung der Organisationen der Kunden untereinander.

Associação Nacional para o Software Livre (ANSOL) bedeutet soviel wie *Nationale Vereinigung für freie Software*. Ihr Fokus liegt auf der Werbung für und dem Schutz von freier Software. Sie setzt sich ein für den Einsatz von freier Software in der öffentlichen Verwaltung und den Schulen und gegen Softwarepatente.

Der **Chaos Computer Club (CCC)** ist wohl die bekannteste deutsche digitale Bürgerrechtsorganisation. Das liegt zum Einen an der Faszination der Medien für *Hacker* – eine Kultur, in der der CCC seine Wurzeln hat – und zum Anderen daran, dass der CCC die treibende Kraft hinter vielen erfolgreichen Kampagnen ist, wie dem Einsatz gegen unsichere Wahlcomputer und gegen alle Arten von Netzsperren. Eine aktuelle Kampagne behandelt den großflächigen Einsatz von Biometrie z. B. im neuen Reisepass. Auch international ist der CCC aktiv, mit Veröffentlichungen von Anleitungen und Werkzeugen zur Umgehung der *Great Firewall of China* [28].

FoeBuD ist Gründer und Hauptorganisator der deutschen *BigBrotherAwards* und kann auf eine lange Geschichte erfolgreicher Projekten zurückblicken. Hervorzuheben sind die Übersetzung der Anleitung für die PGP-Verschlüsselung ins Deutsche, die Kampagne für mehr Datenschutz bei der Payback-Karte und die Beteiligung am jugoslawischen *ZaMir Transnational Net*, das Netzzugang für zivilgesellschaftliche Gruppen während des Krieges bereitstellte. Aktuell arbeitet padeluun für den FoeBuD mit in der Enquête-Kommission *Internet und digitale Gesellschaft* des deutschen Bundestags [29]. FoeBuD beteiligt sich an den deutschen Arbeitskreisen (AK Vorrat, AK Zensur, etc.), engagiert sich gegen die Verbreitung von RFID und hilft mit einem Projekt *PrivacyDongle* beim anonymen Surfen [30].

FITUG bietet eine Plattform zur Unterstützung ihrer Mitglieder bei deren individuellen Aktivitäten, darunter die Mitarbeit bei EURALO und dem AK Zensur.

Die **Digitale Gesellschaft (DG)** ist die jüngste unter den deutschen digitalen Bürgerrechtsorganisationen. Sie hat den Platz des **Netzwerk Neue Medien** übernommen, dessen Vorsitzender DG-Mitgründer Markus Beckedahl, bekannt durch sein Blog

Name	Förderverein Informationstechnik und Gesellschaft (FITUG) e.V. [27]	Digitale Gesellschaft [31]	quintessenz [32]
Gründungsdatum	1996	2011	1994
bei EDRi seit	2002	2011	2002
Mitgliederzahl	10	20	k.A. [33]
Land (Geschäftsstelle)	Deutschland (Jena)	Deutschland (Berlin)	Österreich (Wien)
Themen	Datenschutz, Auswirkungen neuer Technologien, Förderung freier Software	Datenschutz, Recht auf Privatsphäre, Urheberrecht, staatliche Transparenz	Recht auf Privatsphäre, Urheberrecht, Förderung freier Software
in den internationalen Organisationen	EURALO		

Nodo50.org [23]	Associação Nacional para o Software Livre (ANSOL) [24]	Chaos Computer Club (CCC) e.V. [25]	FoeBuD [26]
1994	2001	1981	1987
2006	2007	2002	2005
8	62	2342	460
Spanien (Madrid)	Portugal (Lissabon)	Deutschland (Hamburg)	Deutschland (Bielefeld)
Auswirkungen neuer Technologien, Nutzung des Internets für soziale Bewegungen	Förderung freier Software	Datenschutz, Recht auf Privatsphäre, Meinungsfreiheit, Auswirkungen neuer Technologien	Datenschutz, Recht auf Privatsphäre, Kommunikationsfreiheit
			EURALO

Netzpolitik.org, war. Die DG plant hauptsächlich, öffentlichkeitswirksame Kampagnen zu organisieren, und nennt Greenpeace als ihr Vorbild.

quintessenz veröffentlichte zunächst das erste regelmäßig erscheinende elektronische Magazin im deutschsprachigen Raum. Damals ebenfalls *quintessenz* genannt, wurde es inzwischen in *q/depesche* umbenannt. Sie sind an der Ausrichtung der österreichischen *BigBrotherAwards* beteiligt und helfen bei der Veranstaltung der Linuxwochen mit Vorträgen und Workshops zum Thema Linux und freie Software. Neben mehreren Aufklärungskampagnen gibt es noch ein besonderes Projekt, das quintessenz Kunst-IT-Interface, das Künstler technisch unterstützt.

VIBE!AT ist Gründungsmitglied von EDRi. Es war an der Durchsetzung eines Spam-Verbots in Österreich und ist an der Ausrichtung der österreichischen *BigBrotherAwards* beteiligt.

IT-Politisk Forening (IT-Pol) hat die Förderung von freier Software und den Schutz der Privatsphäre in ihrem erfolgreichsten Projekt verbunden, einer Live-CD mit Programmen zum Schutz der Privatsphäre namens *Polippix*. Neben diesem Projekt setzt IT-Pol auf Mitarbeit im politischen Prozess und Aufklärung der Öffentlichkeit zu Themen wie Überwachung und Zensur.

Electronic Frontier Norway (EFN) ist eine der von EFF inspirierten Organisationen und entstand, als sich eine Mailing-Liste zum Thema digitale Bürgerrechte eine formale Struktur gab, um mehr Gehör in der Öffentlichkeit zu finden. Obwohl Norwegen nicht Mitglied der EU und somit nicht an EU-Richtlinien gebunden ist, ist auch für EFN Vorratsdatenspeicherung eines der dominanten Themen. Ein großer Erfolg der Organisation war die Freilassung des norwegischen Manns, der inhaftiert worden war, weil er den DVD-Kopierschutz geknackt hatte.

Electronic Frontier Finland (EFFi) ist die mitgliederstärkste EDRi-Mitgliedsorganisation und nach eigener Aussage die einzige digitale Bürgerrechtsorganisation in Finnland. In ihren ersten Jahren konzentrierte sie sich auf öffentlichkeitswirksame Kampagnen, bis hin zu Fernsehwerbung, doch in den letzten Jahren hat sich der Fokus eher in Richtung Mitarbeit in parlamentarischen Kommissionen verschoben. Aufgrund einer Besonderheit des finnischen Rechtssystems, das kein Verfassungsgericht kennt, spielt juristisches Vorgehen in ihrer Arbeit keine Rolle.

Panoptykon Foundation ist eine relativ junge polnische Stiftung, bei uns durch ihre Zusammenarbeit mit dem deutschen *AK Vorrat* bekannt. Panoptykon veranstaltet Seminare und Vortragsreihen zu Themen wie Datenschutz und Sicherheit im Internet und hat mit finanzieller Unterstützung des Open Society Institute eine eigene Denkfabrik zum Thema Internet-Regulierung ins Leben gerufen. Sie ist auch außerhalb der digitalen Sphäre für Bürgerrechte aktiv, beispielsweise gegen die schlechte Behandlung von Flüchtlingen durch die EU-Grenzschutzorganisation FRONTEX [41] oder gegen obligatorische gynäkologische Untersuchungen im Rahmen einer Regierungskampagne gegen Gebärmutterhals- und Brustkrebs.

VIBE!AT [34]	The IT-Political Association of Denmark (IT-Pol) [35]	Electronic Frontier Norway (EFN) [36]	Electronic Frontier Finland (EFFI) [37]
1999	2002	1995	2001
2002	2008	2008	2002
60	250	900	2000
Österreich (Wien)	Dänemark (Kopenhagen)	Norwegen (Oslo)	Finnland (-)
Datenschutz, Recht auf Privatsphäre, Meinungsfreiheit, Spam-Bekämpfung	Recht auf Privatsphäre, Meinungsfreiheit, Urheberrecht, Softwarepatente	Recht auf Privatsphäre, Meinungsfreiheit, Recht auf Netzzugang	Recht auf Privatsphäre, Meinungsfreiheit, Urheberrecht

Name	Panoptykon Foundation [38]	Iuridicum Remedium (IuRe) [39]	Associazione per la libertà nella comunicazione elettronica interattiva (ALCEI) [40]
Gründungsdatum	2009	2003	1994
bei EDRi seit	2010	2005	2006
Mitgliederzahl	3	3	6
Land (Geschäftsstelle)	Polen (Warschau)	Tschechien (Prag)	Italien (Mailand)
Themen	Datenschutz, Schutz der Privatsphäre, FRONTEX	Schutz der Privatsphäre, Auswirkungen neuer Technologien	Schutz der Privatsphäre, Meinungsfreiheit
in den internationalen Organisationen		CSISAC	

Bei **Iuridicum Remedium (IuRe)** ist der Name Programm, in etwa: „Das Juristische Heilmittel". Ihre wichtigsten Erfolge sind Klagen vor tschechischen Gerichten, die zur Rücknahme oder Einschränkung von Überwachungsgesetzen führten wie der Vorratsdatenspeicherung und der automatischen Zustimmung zur Videoüberwachung durch Betreten eines öffentlichen Raums. Außerdem arbeitet sie gegen die Verbreitung von RFID-Chips in Dokumenten, fördert *Creative Commons* beispielsweise mit der Übersetzung der Lizenzen ins Tschechische und richtet die tschechischen *BigBrotherAwards* aus.

ALCEI aus Italien setzt sich vor allem gegen Zensur durch Netzsperren ein und gegen die Überwachungsmöglichkeiten der Anti-Terrorismus- und Anti-Mafia-Gesetzgebung.

Association for Technology and Internet (ApTI) ist im Kampf gegen Spam-Mails in Rumänien sehr aktiv und betreibt die nationale schwarze Liste für E-Mail-Adressen unter *abuse.ro*. Sie arbeitet im Rahmen von EURALO bei der Verwaltung der rumänischen Internet-Domain mit und hat die Creative Commons ins Rumänische übersetzt. Daneben beteiligt sie sich am von der EU finanzierten Projekt *Consent*, das untersucht wie die Nutzer sozialer Netzwerke ihre Daten freigeben.

Internet Society Bulgaria (ISOC BG) ist die einzige ISOC in Europa in EDRi. Sie arbeitet in verschiedenen internationalen Projekten zur Förderung von freier und Open Source Software mit, beispielsweise *tOSSad*, einem Projekt zur Verbreitung von freier Software im öffentlichen Dienst, und *FLOSSworld*, einem Forschungsprojekt über die Effekte des Einsatzes von freier Software. Sie hat Creative Commons ins Bulgarische übersetzt und beteiligt sich an der Verwaltung der bulgarischen Internet-Domain.

Metamorphosis war ursprünglich ein Projekt des Open Society Institute, wurde später jedoch als unabhängige Organisation ausgegliedert. Offizielle Mission ist die „Förderung von Demokratie und Wohlstand durch die wissensbasierte Wirtschaft und Informationsgesellschaft". Dazu hat sie zahlreiche Projekte gestartet, die sich beispielsweise mit Gesetzen zu freier Software, dem Schutz der Privatsphäre und dem Schutz der Umwelt vor Elektro-Schrott beschäftigen. Ganz besonders befasst sie sich mit der speziellen Entwicklung einer Informationsgesellschaft in einem jungen, weniger entwickelten und multi-ethnischen Staat wie Mazedonien.

Anmerkungen

[1] http://www.edri.org/
[2] Den aktuellsten Zahlen nach ist nun der CCC die mitgliederstärkste Organisation der EDRi.
[3] Die Zahlen für 2010 sind im EU Transparency Register zu finden: http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=16311905144-06
[4] Mehr zum Open Society Institute: http://www.soros.org/
[5] https://community.icann.org/display/EURALO/
[6] http://csisac.org/
[7] http://www.apc.org/
[8] http://cpsr.org/
[9] George Soros ist aufgrund seiner Vergangenheit als Währungsspekulant und seiner Unterstützung zahlreicher politischer Gruppen eine sehr kontroverse Person, mehr dazu auf Wikipedia: http://de.wikipedia.org/wiki/George_Soros und http://en.wikipedia.org/wiki/George_Soros_conspiracy_theories
[10] Die europäischen Aktivitäten von EFF: https://www.eff.org/issues/eff-europe
[11] https://www.eff.org/
[12] http://www.mensenrechten.be/
[13] https://www.bof.nl/
[14] https://www.vrijschrift.org/
[15] Mehr zu diesem Projekt und seinen Resultaten: http://yro.slashdot.org/story/04/10/09/1929259/Censoring-The-Net-With-A-Hotmail-Account
[16] http://www.openrightsgroup.org/
[17] http://www.fipr.org/
[18] http://www.gn.apc.org/
[19] http://www.digitalrights.ie/
[20] http://www.iris.sgdg.org/
[21] http://www.laquadrature.net/en/
[22] http://www.pangea.org/
[23] http://info.nodo50.org/
[24] http://ansol.org/
[25] http://www.ccc.de/
[26] http://www.foebud.org/
[27] http://www.fitug.de/
[28] Mehr zu diesem Projekt und der Great Firewall of China: http://chinesewall.ccc.de/
[29] Eine Enquête-Kommission ist eine langfristige Arbeitsgruppe aus Experten und Abgeordneten des deutschen Bundestags oder eines Landtags. Mehr zur erwähnten Enquête-Kommission: http://www.bundestag.de/internetenquete/

Association for Technology and Internet (APTI) [42]	Internet Society Bulgaria (ISOC BG) [43]	Metamorphosis [44]
2005	1995	2004
2005	2003	2005
25	7	8
Rumänien (-)	Bulgarien (Sofia)	Mazedonien (Skopje)
Datenschutz, Recht auf Privatsphäre, Spam-Bekämpfung	Förderung freier Software, Recht auf Internetzugang	Demokratie- und Wohlstandsförderung
EURALO, CSISAC	EURALO	CSISAC, APC

[30] http://privacydongle.de/
[31] http://digitalegesellschaft.de/
[32] http://www.quintessenz.org/
[33] Gemäß ihrem Motto „Datenschutz ist Menschenrecht" lehnte quintessenz die Veröffentlichung ihrer Mitgliederzahl ab.
[34] https://www.vibe.at/
[35] http://www.itpol.dk/
[36] http://www.efn.no/
[37] http://www.effi.org/
[38] http://www.panoptykon.org/node/112
[39] http://www2.iure.org/
[40] http://www.alcei.it/
[41] Mehr zum Engagement gegen FRONTEX: http://no-racism.net/article/3370/
[42] http://www.apti.ro/apti-english
[43] http://www.isoc.bg/index_en.html
[44] http://www.metamorphosis.org.mk/en

Andreas Krisch

Netzpolitik: Lassen wir die Fakten sprechen

Vom Grundrecht auf Internetzugang über Nutzerüberwachung durch Internet Service Provider bis zur „Evaluierung" der Vorratsdatenspeicherungs-Richtlinie: Die netzpolitischen Themen und Diskussionsverläufe auf europäischer und internationaler Ebene sind vielfältig. Was aber zählt sind die Fakten.

Das Internet sollte frei bleiben und der Zugang zum Internet als Menschenrecht anerkannt werden. Zu diesem Ergebnis kommt eine im Juli diesen Jahres veröffentlichte Studie der OSZE (Organisation für Sicherheit und Zusammenarbeit in Europa) zur freien Meinungsäußerung im Internet in den OSZE Teilnehmerstaaten.

Die Studie kritisiert den europäischen Trend zu einem regulierten, kontrollierten und zensurierten Internet und das Ausmaß der in der OSZE-Region festgestellten Internet-Sperrmaßnahmen. Sie zeigt, dass Filter- und Sperrmaßnahmen in den meisten Fällen nicht mit dem Recht auf freie Meinungsäußerung und dem freien Informationsfluss vereinbar sind.

Aus Sicht der OSZE sollte der Zugang zum Internet als Grundrecht betrachtet werden und in gleicher Weise respektiert werden, wie das Recht auf freie Meinungsäußerung. „Jeder sollte das Recht haben an der Informationsgesellschaft teilzunehmen und Staaten haben die Verantwortung, sicherzustellen, dass der Zugang der Bürger zum Internet sichergestellt ist", so die Studie.

Zu ganz ähnlichen Ergebnissen kam der UN Sonderberichterstatter für die Stärkung und den Schutz der Rechte auf Meinungsfreiheit und die freie Meinungsäußerung, Frank La Rue, im Juni diesen Jahres. Dieser stellte in seinem Bericht an den UN Menschenrechtsrat fest, dass das Recht Informationen zu suchen, zu empfangen und zu verbreiten, sowie das Recht sich frei zu äußern – also Rechte, die das Wahrnehmen einer Reihe anderer Rechte erst ermöglichen – in der Online-Kommunikation zunehmend durch Hürden beschränkt werden.

Der Bericht verweist auf zahlreiche Belege dafür, dass die internationale Internet-Politik sowie die nationalen Regelungen die veränderte Struktur des öffentlichen Raums, in dem das Recht auf freie Meinungsäußerung praktiziert wird, nicht angemessen berücksichtigen und erinnert die Regierungen an ihre Verpflichtung, diese Rechte auch im digitalen Raum zu schützen. Unter anderem verweist der Sonderberichterstatter auch auf den beunruhigenden Trend der Staaten, private Akteure dazu zu verpflichten oder zu drängen, Informationen ihrer Benutzer herauszugeben.

In tiefer Sorge über die zunehmende Anzahl von Gesetzen, die das Überwachen, Filtern und Kontrollieren von Online-Inhalten ermöglichen, fasst der Sonderberichterstatter zusammen, dass diese oftmals nicht mit den vorgeblichen Zielen übereinstimmen. Zunehmend werden ausgeklügelte Sperrmechanismen für vermeintlich illegale Inhalte ohne Gerichtsbeschluss oder Beiziehung einer Aufsichtsbehörde eingesetzt. Mechanismen zur Verhinderung von Missbrauch und zur Überprüfung von möglichen Missbrauchsfällen fehlen oft. Dies kann zur Zensur einer signifikanten Anzahl von legalen Online-Inhalten führen, so der Bericht.

Den zunehmenden Druck auf Internet-Service-Provider und Anbieter von Online-Diensten hat European Digital Rights (EDRi) bereits Anfang des Jahres gegenüber verschiedenen europäischen Institutionen thematisiert und anhand konkreter Beispiele aus diversen Gremien in einer Publikation exemplarisch zusammengefasst.

Hierbei konnte wiederholt festgestellt werden, dass die Anbieter zu Selbstregulierungsmaßnahmen gedrängt werden, die darauf abzielen, die Nutzungsmöglichkeiten der Internetnutzer einzuschränken und unerwünschtes Verhalten auf Basis von allgemeinen Geschäftsbedingungen zu sanktionieren. Diese Vorgehensweise ermöglicht es den jeweils treibenden Kräften, Regelungen mit Marktmechanismen durchzusetzen, die im Rahmen eines geordneten Gesetzgebungsverfahrens nur schwer oder gar nicht durchsetzbar wären.

Unklare bzw. lückenhafte Regelungen zur Verantwortung von Internet Service Providern und Anbietern von Online-Diensten dienen hierbei als Ausgangspunkt für die „Überzeugungsarbeit" bezüglich der Notwendigkeit einer „freiwilligen" Selbstregulierung, bei deren Ausbleiben sonst zu – selbstverständlich strengeren – gesetzlichen Maßnahmen gegriffen werden müsste.

Dass dieses Gesetzgebungsverfahren schlussendlich nicht notwendigerweise die gewünschte strenge Regelung hervorbringt, zeigt die langjährige Debatte um die Sperrung von kinderpornografischen Internet-Inhalten.

Anhand harter Fakten aus der Praxis der Strafverfolgungsbehörden konnte in Deutschland nachgewiesen werden, dass eine Sperrung von Inhalten nicht erforderlich ist, da in der überwiegenden Anzahl von Fällen innerhalb kurzer Frist eine Löschung der Inhalte erreicht werden kann. Im Einklang mit dem daraus resultierenden politischen Umdenken in Deutschland konnte in weiterer Folge auch der Bürgerrechtsausschuss des Europäischen Parlaments davon überzeugt werden, dass Netzsperren für die Bekämpfung von kinderpornografischen Inhalten im Internet keine zwingend erforderliche Maßnahme ist. Entsprechend hat sich der Ausschuss am 12. Juli 2011 mit fünfzig zu null Stimmen erneut gegen die Einführung von verpflichtenden Internetsperren in der Europäischen Union ausgesprochen.

Rückwirkend betrachtet wurde diese Entwicklung erst dadurch möglich, dass sich die deutsche Internetwirtschaft – anders als ihre Kollegen in Dänemark, Schweden und dem Vereinigten Königreich – mutig dazu entschlossen hat, eine demokratische Vorgehensweise und die Verabschiedung eines Gesetzes zu verlangen, als sie aufgefordert wurde „freiwillig" Internetsperren einzuführen.

Harte Fakten aus der täglichen Realität sollten die Basis sein für Entscheidungen der Politik. Das gilt insbesondere dann, wenn

Grund- und Menschenrechte eingeschränkt werden sollen, um höherwertige Ziele – wie beispielsweise die effektive Bekämpfung von Terrorismus und schwerer Kriminalität – zu erreichen.

Ein Bereich in dem diese Notwendigkeit der faktenbezogenen Entscheidungsfindung aktuell besonders deutlich wird, ist die verdachtsunabhängige Datenspeicherung von Telekommunikationsverbindungen (Vorratsdatenspeicherung; VDS).

Entsprechend der in der VDS-Richtlinie festgelegten Verpflichtung hat die Europäische Kommission im April diesen Jahres ihren Evaluierungsbericht zu dieser Richtlinie verabschiedet.

Wie aus den Vorbereitungsarbeiten der Kommission bereits abgeleitet werden konnte, zeichnet sich der Bericht dadurch aus, die zahlreichen Fehler und Unzulänglichkeiten der durch die Richtlinie vorgeschriebenen Maßnahmen zu verschleiern und stattdessen eine Nützlichkeit der durch die Richtlinie vorgeschriebenen Grundrechtseingriffe zu suggerieren.

Da diese Ergebnisse bereits im Vorfeld absehbar waren, hat EDRi sich dazu entschlossen, aufbauend auf dem methodischen Rahmen der Europäischen Kommission einen faktenbasierten Bericht über die Nützlichkeit der Vorratsdatenspeicherungs-Richtlinie zu erstellen und diesen einen Tag vor dem Bericht der EU-Kommission zu veröffentlichen.

Im Wesentlichen wird anhand dieser beiden Berichte deutlich, dass die Kommission ganz klar daran gescheitert ist, die Notwendigkeit und Effektivität der Vorratsdatenspeicherung nachzuweisen. Vielmehr tritt zu Tage, dass es trotz des politischen Wunsches die Vorratsdatenspeicherungs-Richtlinie aufrecht zu erhalten nicht möglich war ausreichende Tatsachenbeweise zu finden, die diesen politischen Wunsch stützen.

So behauptet die Kommission beispielsweise, dass ihr Evaluierungsbericht den Wert der VDS für die Strafverfolgungsbehörden zeigt. Was sie dabei vergisst zu erwähnen ist, dass die überwiegende Mehrheit der von den Strafverfolgungsbehörden verwendeten Kommunikationsdaten nicht auf Basis der VDS sondern aufgrund anderer Rechtsgrundlagen gespeichert wurden.

Weiters behauptet die Kommission, dass die Anschläge in Madrid und London die Notwendigkeit der VDS gezeigt hätten. Tatsächlich waren Kommunikationsdaten nützlich beim Madrid-Anschlag, jedoch waren diese Daten für Verrechnungszwecke und nicht auf Basis der VDS gespeichert.

Darüber hinaus stellt die Kommission fest, dass die verdachtsunabhängige Speicherung von Kommunikationsverbindungsdaten eine notwendige Maßnahme darstellt. Tatsächlich hat die Kommission weder nach Beweisen gefragt, noch welche erhalten, die belegen, dass die zusätzlichen Daten, die auf Basis der VDS gespeichert wurden, entweder notwendig oder zumindest nützlich waren.

Auch die Behauptung der Kommission – um abschließend einen letzten Punkt aus einer langen Liste von Argumenten zu erwähnen – dass die Verfassungsgerichte die Vorratsdatenspeicherung selbst nicht kritisiert hätten ist falsch. Das rumänische Verfassungsgericht hat dies aus gutem Grund sehr wohl getan. Nach Einschätzung des Europäischen Datenschutzbeauftragten handelt es sich bei dieser Richtlinie um die am meisten in die Privatsphäre eindringende Maßnahme, die in der Europäischen Union jemals beschlossen wurde.

Enttäuscht von der Evaluierung der VDS-Richtlinie zeigte sich kürzlich auch der niederländische Senat. In einem Schreiben an den niederländischen Minister für Sicherheit und Justiz vom 31. Mai bezeichnete der Senat den Evaluierungsbericht als „unzufriedenstellend", „nicht überzeugend" und „enttäuschend" und fragte den Minister, ob die Richtlinie nicht besser aufgehoben werden sollte. Bemerkenswerter Weise stellte auch der Senat fest, dass der Bericht die Notwendigkeit und Verhältnismäßigkeit der Richtlinie nicht ausreichend demonstriert, und dass er es verabsäumt, eine „dringende gesellschaftliche Notwendigkeit" nachzuweisen, da die E-Privacy Richtlinie ohnehin bereits die Speicherung bestimmter Verkehrsdaten zu Verrechnungs- und Marketingzwecken vorsieht.

Andreas Krisch

Magister **Andreas Krisch** studierte Wirtschaftsinformatik an der Universität Wien und der Technischen Universität Wien. Er ist Präsident von European Digital Rights (EDRi, www.edri.org) sowie Obmann des Vereins für Internet-Benutzer Österreichs (VIBE!AT) und setzt sich in diesen Funktionen auf nationaler und europäischer Ebene für eine Stärkung des Datenschutzes ein. Seine Expertise zu Datenschutz, RFID und dem Internet der Dinge stellte er wiederholt Institutionen wie dem Europäischen Parlament, dem Europarat und der OECD zur Verfügung. Die Europäische Kommission berät er in Datenschutzfragen im Rahmen der Expertengruppen zu RFID und dem Internet der Dinge.

Andreas Krisch ist ausgebildeter Datenschutzbeauftragter und geschäftsführender Gesellschafter des Datenschutzunternehmens mksult GmbH (www.mksult.at). Als akkreditierter technischer Experte erstellt er technische Gutachten für das Europäische Datenschutzgütesiegel (EuroPriSe). Sein Unternehmen trägt darüber hinaus mit dem Datenschutzportal www.unwatched.org zu Bewusstseinsbildung und Information der breiten Öffentlichkeit bei.

Interessant ist im Zusammenhang mit der Vorratsdatenspeicherung auch die unterschiedliche Geschwindigkeit mit der die EU Kommission bei der Durchsetzung von Richtlinien vorgeht. Während das Vertragsverletzungsverfahren gegen Österreich wegen Nichtumsetzung der Vorratsdatenspeicherungs-Richtlinie bereits nach rund drei Jahren mit einer Verurteilung endete, dauerte es beispielsweise über zehn Jahre, bis Deutschland wegen der mangelnden Unabhängigkeit bestimmter Datenschutzaufsichtsbehörden verurteilt wurde. Ein ähnliches Verfahren gegen Österreich ist nach wie vor noch nicht abgeschlossen.

Wie anhand dieser ausgewählten Beispiele aus der aktuellen europäischen Netzpolitik deutlich wird, ist es sowohl für die Grundrechte der Bürger, als auch für die Erreichung der übergeordneten Ziele, die eine Einschränkung von Grundrechten möglicherweise rechtfertigen können, von grundlegender Bedeutung, politische Entscheidungen aufgrund harter, nachvollziehbarer Fakten zu treffen. Dazu gehört auch ein tatsächlicher Nachweis der Effektivität und Notwendigkeit dieser Maßnahmen in einer demokratischen Gesellschaft, wie es von der Europäischen Menschenrechtskonvention gefordert wird.

Referenzen

OSCE Report – Freedom of Expression on the Internet – Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States (8.07.2011) http://www.osce.org/fom/80723

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. Frank La Rue http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf

EDRi report: The slide from „self-regulation" to corporate censorship, http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf

ENDitorial: Why it was good to propose web blocking for child abuse images, http://www.edri.org/edrigram/number9.14/blocking-debate-good

EDRi Schattenbericht zur VDS Evaluierung, http://www.edri.org/data-retention-shadow-report

Dutch Senate „disappointed" with Data Retention Directive evaluation, http://www.edri.org/edrigram/number9.14/dutch-senate-data-retention-evaluation

Monika Ermert

Netzneutralität

Handeln? Oder abwarten und Tee trinken?

Das Ringen um eine Absicherung von Netzneutralität für das Internet der Zukunft ist einer der Hauptkampfplätze moderner Netzpolitik. Gleich zweimal hat die Enquête-Kommission des Deutschen Bundestages zum Thema Internet und Digitale Gesellschaft die Verabschiedung von Handlungsempfehlungen zur Netzneutralität verschoben. Erst nach der Sommerpause will man einen erneuten Anlauf machen, dabei stehen sich – wie in anderen Ländern auch – Befürworter einer Marktlösung und einer Regulierungslösung gegenüber. Im Nachbarland Niederlande hat man sich für eine explizite gesetzliche Priorisierung der Neutralitätspflicht entschieden, der deutsche Gesetzgeber zögert.

Von Netzneutralität reden, heißt, erst einmal eine Diskussion über die Definition zu führen. Die Arbeitsgruppe Netzneutralität der Internet-Enquête, die seit über einem Jahr an dem Thema arbeitet, hat es sich im nicht verabschiedeten Bericht leicht gemacht. Diskriminierungsfreiheit wird als zentrales Merkmal von Netzneutralität bezeichnet, die wiederum das Internet zu dem Innovationsmotor gemacht habe, als das wir es kennen.

Während in den Anfangszeiten des Netzes eine agnostische Behandlung (ohne Ansehen von Anwendung oder Inhalt) von Internet Protokoll-Paketen selbstverständlich war, bestehe heute die Gefahr, so schreibt die Enquête-Kommission, dass Pakete je nach Nutzer, Inhalt, Volumina, gebuchter Qualitätsklasse, Diensteanbieter oder sogar einzelnen Programmen, Applikationen oder Dienste bevorzugt oder gebremst transportiert werden. Das Risiko der Diskriminierung neuer – insbesondere besonders wettbewerbsfähiger – Anwendungen ist, laut den Befürwortern von Netzneutralitätsregeln, heute offensichtlich.

Mobiles Internet ja, aber über meinen Dienst!

Eins der ersten Beispiele dazu, wie Einschränkungen der Netzneutralität aussehen könnten, lieferte das US-Unternehmen *Comcast* vor mehreren Jahren: Ungefragt verlangsamte es Datenverkehre des p2p-Anbieters *Bittorrent*. Auch aktuell ist es ein US-Verfahren vor der *Federal Communications Commission (FCC),* das zeigt, wohin die Reise ohne Regeln gehen könnte. Im Juni schlug die für Informations-, Meinungs- und Medienfreiheit streitende Organisation *Free Press* Alarm und reichte bei der FCC eine Beschwerde gegen den größten US-Anbieter von Breitband-Mobilfunk *Verizon Wireless* ein. Verizon habe *Google* veranlasst, den mobilen Internetzugang vom Laptop – oder einem anderen Gerät – via Smartphone und über das Breitband-Mobilnetz von Verizon zu blockieren. (Die Verbindung von Mobiltelefon und Computer für den Internet-Zugang wird *Tethering* genannt.)

Für Verizon-Kunden musste Google die vom Android-Betriebssystem zur Verfügung gestellten *Tethering-Applikationen* blo-

ckieren. „Kauft ein Kunde etwa ein HTC Thunderbolt Smartphone, um es in Verizons LTE (Netz der 4. Mobilfunkgeneration) zu nutzen, kann dieser Nutzer bestimmte Tethering-Anwendungen nicht von Android herunterladen", beschreibt Free Press das Vorgehen.

Ein starkes Motiv aus Sicht des Netzanbieters: Er möchte den mobilen Zugang zusätzlich zum Mobilfunkvertrag selbst verkaufen. 30 Dollar verlangt Verizon laut der eingereichten Klage für den Tethering-Dienst (zusätzlich zur normalen Monats-Flatrate für mobiles Internet), während er anderweitig frei oder deutlich preiswerter zu haben ist.

Durch Rückmeldungen an die Kunden, „dieses Produkt ist über ihren Netzbetreiber nicht erhältlich", wird den Nutzern teilweise suggeriert, dass sie die Dienste überhaupt nicht nutzen können, obwohl sie sich diese außerhalb des *Android Market* durchaus beschaffen können. Die in Stanford lehrende Juristin und Informatikerin Barbara van Schewick schrieb im Rahmen des FCC-Verfahrens zu der Tethering-Blockade: „Verizons Praxis und die Beschwerde von Free Press beinhalten Grundsatzfragen des offenen Internet und einer entsprechenden Politik."

Netzneutralität als Stärkungsmittel für Wahlfreiheit der Kunden und Innovation

Die Tethering-Anwendungen stellen laut van Schewick, seit Jahren eine der eloquentesten Befürworterinnen klarer, gesetzlicher Netzneutralitätsregeln und Gutachterin des US-Kongresses, „eine wichtige Innovation bei der Weiterentwicklung des mobilen Internet dar. Denn sie erlauben Nutzern, viele Geräte über eine Breitbandverbindung anzuschließen."

Nicht nur erschwere Verizon seinen Nutzern, Geräte ihrer Wahl anzuschließen. Der Provider maße sich auch an, *Gewinner und Verlierer* im Wettbewerb zu bestimmen. Genau dagegen wurden Netzneutralitätsregeln immer als Korrektiv gesehen. Van Schewick gehört auch zu denen, die wiederholt gewarnt hatten, sich bei der Entscheidung für oder wider eine gesetzliche Absicherung der Netzneutralität darauf zu konzentrieren, wie häufig gegen das klassische, ungeschriebene Neutralitätsprinzip verstoßen wurde.

Barbara van Schewick, Juristin und Informatikerin an der Universität Stanford, erforscht seit fast einem Jahrzehnt das Thema Netzneutralität und ist in den USA eine gefragte Gutachterin im Kongress.
Foto Susanne Kern, Pressefoto Kraufmann & Kraufmann GmbH, mit freundlicher Genehmigung der Alcatel-Lucent-Stiftung

Tatsächlich meldeten verschiedene Nutzer Widerspruch an, nachdem das konservative Enquête-Kommissionsmitglied Peter Tauber (CDU) gebloggt hatte, die „Netzneutralität ist in Deutschland derzeit nicht in akuter Gefahr. Es gibt keine erkennbare Zahl an Verstößen." Tauber sagte, auch die Befürworter einer gesetzlichen Absicherung hätten diesbezüglich „außer Unkenrufen und düsteren Zukunftsprognosen keine belastbaren Fakten vorbringen können."

Dem widersprachen auf Taubers Blog gleich mehrere Nutzer und wiesen unter anderem darauf hin, dass auch in Deutschland das Tethering unterbunden werde. So habe man zwar bei einem Mobilfunkvertrag 1 GB Datenvolumen, dürfe dies aber nur mit einem bestimmten Mobiltelefon nutzen, „nicht jedoch die SIM-Karte mal schnell ins Notebook stecken oder sein iPad mit dem Handy tethern." Der Provider schreibe einfach vor, mit welchem Gerät das bezahlte Datenvolumen genutzt werden könne.

Weitere Berichte betrafen die offensichtliche Verlangsamung von Skype-Zugriffen über einen T-Connect L-Anschluss, die sich nur mittels VPN-Verbindung umgehen ließ, sowie Verzerrungen beim Zugriff auf Webangebote, die durch Beeinträchtigungen der Nutzung von JavaScripts durch einen Zwangsproxy von T-Mobile entstanden. „So sieht Netzneutralität aus, wenn sie der Markt regelt – welcher Nichttechniker kann denn analysieren, woran die Fehler liegen und hat Alternativen", fragte einer der Nutzer bei Tauber nach.

Ein Sonderkündigungsrecht entstehe durch die Datenbeeinflussung von Seiten der T-Mobile übrigens nicht, da das Netzwerkmanagement ja zum Wohl der Kunden sei. Auch Verizon hatte die Blockade des Tethering nicht damit begründet, dass man eigene Angebote verkaufen möchte, sondern damit dass „ein solcher Nutzen nicht vereinbar wäre mit den bekannten technischen Standards, die nach gesundem Ermessen notwendig sind für das Management und den Schutz des Netzes des Lizenznehmers."

Die Enquête-Kommission müsse sich fragen lassen, ob sie die Probleme ausreichend recherchiert habe, schrieb Journalist Falk Lüke. Eine, wenn auch allgemeine Liste von Vorfällen notierte das Gremium der EU-Telekommunikationsregulierungsbehörden *BEREC* in der Tat bereits im vergangenen Jahr, und es spricht von dokumentierten Verstößen (insbesondere Blockaden von Voice-over-IP-Diensten) in Österreich, Kroatien, Deutschland, Italien, den Niederlanden, Portugal, Rumänien und der Schweiz. Blockaden oder Behinderungen von p2p-Diensten listete BEREC für Frankreich, Griechenland, Ungarn, Litauen, Polen und das Vereinigte Königreich. Teilweise würden die blockierten Dienste gegen Aufpreise angeboten.

Die Regulierer gaben sich trotz dieser Befunde allerdings zögerlich in Bezug auf eine gesetzliche Regulierung, genauso wie die EU-Kommission, die sich nach einer Konsultation zu den Transparenz- und optionalen Mindeststandards laut neuer TK-Rahmenrichtlinie erst einmal auf den Beobachterposten zurückgezogen hat.

Malte Spitz vom Bundesvorstand der Grünen moniert:

> *„Nur weil aktuell nicht jeden Tag Fälle bekannt werden, wo die Netzneutralität verletzt wird, herrscht alles andere als selige Ruhe. Sprich: Wir müssen jetzt dafür kämpfen, dass die Netzneutralität gesetzlich verankert wird, ansonsten besteht die Gefahr, dass wir dem Internet von heute in 10 Jahren nachweinen."*

Er habe übrigens noch kein Argument gehört, wieso es falsch sei, Netzneutralität rechtlich abzusichern, sagte Spitz und beklagte den Dissens zwischen Konservativen und Opposition in der Enquête-Kommission. Es sei mehr als bedauerlich, dass die Enquête-Kommission keine Empfehlung für eine entsprechende Änderung im Telekommunikationsgesetz beschlossen habe,

> *„zumal uns andere Länder gerade vormachen, wie die Neutralität der Netze gesetzlich geschützt werden kann und auch die EU in ihrer 'digitalen Agenda' die Bedeutung der Netzneutralität explizit betont."*

Die Initiative ProNetzneutralität, zu deren Gründern auch Malte Spitz gehört, hat rund 10.000 Unterschriften für eine gesetztliche Absicherung gesammelt. http://pro-netzneutralitaet.de/

Niederlande als Vorreiter

Die Vorreiterrolle bei der Regulierung der Netzneutralität hat gerade Nachbar Niederlande übernommen. In einer knappen Regelung, dem neuen Artikel 7.4a des niederländischen Telekommunikationsgesetzes, wird festgehalten, dass Anbieter öffentlicher elektronischer Netzwerke, die Zugang zum Internet bieten, sowie Provider von Internetzugangsdiensten Anwendungen und Dienste im Netz nicht behindern oder verlangsamen dürfen, es sei denn, dies sei unabdingbar wegen Datenstaus im Netz oder der Netzsicherheit. Vom Nutzer selbst georderte Blockaden bestimmter Datenverkehre (Spam, Kinderschutzfilter) werden ausgenommen, und natürlich müssen die Provider etwaigen Gerichtsurteilen oder richterlichen Verfügungen nachkommen.

Diese Regelung geht noch über die Open-Internet-Verordnung der FCC hinaus, da sie alle Arten von Diensten, also auch die mehr und mehr ins Zentrum rückenden Mobilfunkdienste einschließt. Eigens klargestellt wird auch, dass der Internetzugang nicht verteuert werden darf, wenn die Nutzerin Zugang zu bestimmen Anwendungen oder Diensten möchte. Überdies werden Minimalanforderungen für die Qualität des Netzzugangs in Aussicht gestellt, zumindest für Unternehmen, die öffentliche Kommunikationsnetzdienste anbieten. Was Provider über dedizierte, nicht für den Internetzugang vorgesehene Netzwerke machen, können sie selbst entscheiden.

Ein Hochgeschwindigkeitsnetz, das klassische Internetzugangsdienste anbietet, dürfte darunter aber wohl nicht fallen. Internet und Internetzugang seien breit zu definieren, um Versuchen von Providern entgegenzuwirken, die Neutralitätsverpflichtung zu umschiffen. Während andere europäische Länder offenbar Erfahrungen auch mit der Umsetzung der neuen EU-Vorgaben zu Transparenz und Mindestqualitätsoption abwarten, entschied man sich in den Niederlanden, wie übrigens zuvor bereits in Chile, den Schritt zur Absicherung der Netzneutralität in der nationalen Gesetzgebung zu machen.

Netzneutralität und Netzmerkmanagement

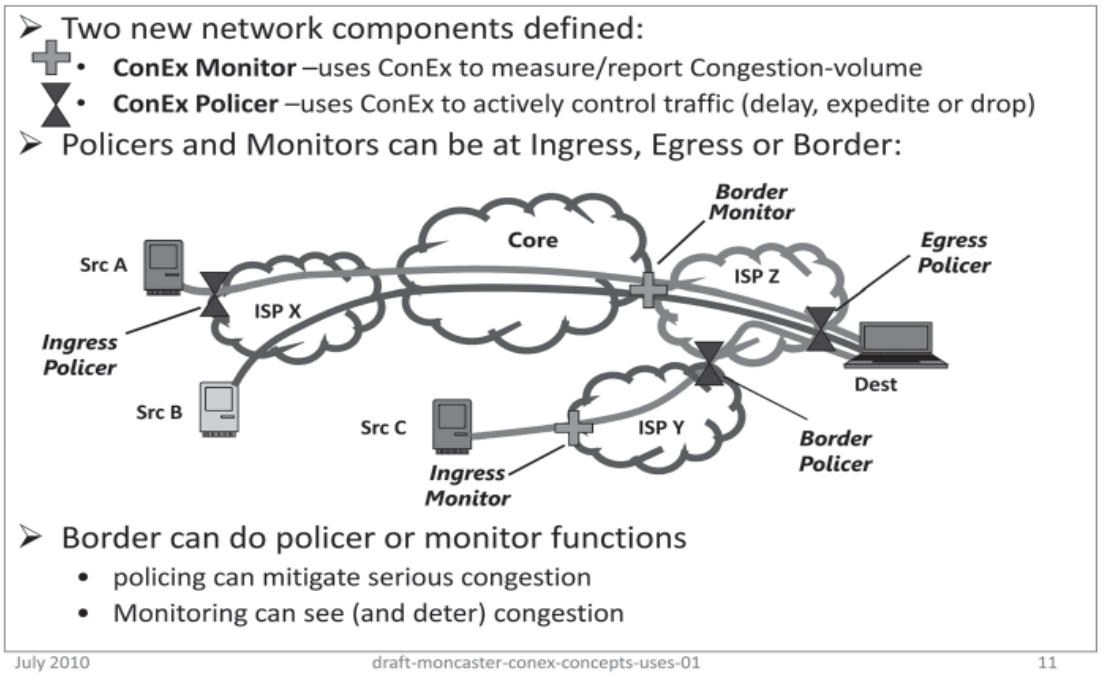
Auch nach einer Verankerung von Netzneutralität als gesetzliche Norm darf ein Netzbetreiber Datenverkehre managen – auch in der niederländischen Regelung ist ein *Staumanagement* durchaus zulässig. Über die Frage, inwieweit sich Netzneutralität einerseits und Netzwerkmanagement andererseits behindern, was man auch als Dilemma zwischen einem *best-effort*-Ansatz und dem viel beschworenen *Quality-of-Service*-Versprechen sehen könnte, darüber sind sich selbst Entwickler und Administratoren noch nicht einig, auch nicht darüber, ob beides vielleicht doch vereinbar wäre.

Das Problem ist, dass es zu Kapazitätsengpässen, die das Staumanagement notwendig machen würden, ganz offenbar noch weniger Daten gibt als zu Verstößen gegen die Netzneutralität. Eine Umfrage der deutschen Enquête-Kommission jedenfalls erbrachte keine Belege für auffällige Kapazitätsengpässe, schreibt ein Enquête-Kommissionsmitglied in der Debatte um Taubers Blogbeitrag.

Genau hier will eine Arbeitsgruppe der für die Entwicklung des IP-Protokolls maßgeblichen Standardisierungsorganisation,

Monika Ermert

Monika Ermert arbeitet seit 1993 als freie Journalistin für verschiedene Tages- und Wochenzeitungen, und ist regelmäßige Autorin für Fachzeitschriften wie die c't (insbesondere heise online) und Intellectual Property Watch. Mit dem Thema Netzneutralität beschäftigt sie sich seit 2006. Damals hielten europäische Politiker Netzneutralität noch allein für ein Problem des US-Markts. Monika Ermert lebt mit ihrem Lebensgefährten und zweieinhalb Kindern in München.



ConEx Concepts and Uses draft 01.
Wir danken Bob Briscoe (British Telecom) für die Druckgenehmigung.

der *Internet Engineering Task Force (IETF),* ansetzen. Die Arbeitgruppe *ConEx* (congestion exposure, in etwa: Staumeldungen) entwickelt seit mehreren Jahren ein Set von Protokollen, das zunächst einmal erlauben soll, Lastprobleme vom Endsystem zurück ans Netzwerk zu melden.

Wie mit den genaueren Informationen über den Preis für die Nutzer umgegangen werden soll, sei dann wieder eine andere Frage, sagt Bob Briscoe, Chefwissenschaftler bei *British Telecom.* Trotzdem hält er es für den besseren Weg, erst einmal Transparenz herzustellen, statt unterschiedslos Volumengrenzen einzuziehen oder aber den Verkehr mit *Deep Packet Inspection (DPI)* zu überwachen und zu filtern. In genau diese Richtung – hin zu mehr und mehr Totalkontrolle der Pakete per DPI – geht aktuell aber die Entwicklung laut den Technikern.

Briscoe befürchtet überdies eine Art Wettrüsten zwischen Applikations- und Netzseite in dem verzweifelten Versuch, die Kontrolle über das Netz zu behalten. Der ConEx-Ansatz sei besser, nicht nur weil er Transparenz schaffe durch Mitteilung der Sender darüber, welchen Bandbreiteneintrag sie bringen, sondern auch, weil er völlig Anwendungsneutral sei und lediglich auf den Bedarf an Bandbreite abstelle.

Allerdings gibt es innerhalb der IETF erhebliche Widerstände gegen die Entwicklung. Viele Ingenieure befürworten nach wie vor den Ausbau von Bandbreiten anstatt des Versuchs, einen befürchteten Mangel zu verwalten. Sie argwöhnen, dass ein aufwändiges Netzwerkmanagement ein Mehr an Komplexität und damit neue Fehlerquellen für den Betrieb bringt – die Netzneutralitäts-Befürworter warnen eher vor den damit erweiterten Kontrollmöglichkeiten. Die Debatte um Effekte eines *optimierten Netzwerkmanagements* beziehungsweise eines erneuten Anlaufs, Quality of Service schmerzloser zu erreichen, hat die Politik erst noch zu führen. Das könnte dauern!

Quellen:

Unvollendeter Bericht der Arbeitsgruppe Netzneutralität:
http://www.bundestag.de/internetenquete/dokumentation/2010/Sitzungen/20110627/11-06-27_Enquete-Kommission_PG_Netzneutralitaet_Gesamttext.pdf
Klage von Free Press gegen Tethering-Blockaden nach Verhandlungen zwischen Google und Verizon:
http://www.freepress.net/files/FreePress_CBlock_Complaint.pdf
http://petertauber.wordpress.com/2011/07/05/internet-enquete-vom-konsens-taktischen-spielchen-und-falschen-annahmen/
Wissenschaftliche Artikel, Stellungnahmen von Barbara van Schewick:
http://www.law.stanford.edu/directory/profile/313/#publications_cases
Mitteilung der Europäischen Kommission zu Netzneutralität:
http://ec.europa.eu/information_society/policy/ecomm/doc/library/communications_reports/netneutrality/comm-19042011.pdf
Berec-Stellungnahme:
http://www.erg.eu.int/doc/berec/bor_10_42.pdf
Ergebnisse der EU-Konsultation 2010:
http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/report.pdf
Rohübersetzung des Niederländischen Gesetzes (veröffentlicht von Bits of Freedom):https://www.bof.nl/2011/06/15/net-neutrality-in-the-netherlands-state-of-play/
Entwurf im niederländischen Original:
https://zoek.officielebekendmakingen.nl/dossier/32549/kst-32549-17

Sebastian Jekutsch (Einleitung), Miloš Bárta, Eva Pechová, Sarah Bormann, Leonhard Plank

Sie trafen sich bei Foxconn

Wanderarbeit in osteuropäischer IT-Industrie

1. Teil: Einleitung

Der taiwanesische Hersteller Hon-Hai Precision Industy Co. Ltd., besser bekannt als Foxconn, fertigt elektronische Komponenten und Geräte für Markenfirmen wie Dell, Nokia, Sony oder Apple. Diese Firmen vergeben die Herstellung komplett an so genannte Kontraktfertiger und sind selbst nur noch Entwicklungs- und Marketingunternehmen. Foxconn, bekannt für die Herstellung des iPhone und iPad, ist der derzeit größte Kontraktfertiger, mit etwa 1 Million Arbeitnehmern allein in China, aber auch mit Produktionsstätten in Europa.

Berichte über sich häufende Selbstmorde von Arbeitern im Werk Shenzhen und anderen haben Foxconn in die Schlagzeilen gebracht. Auch in diesem Jahr ist schon ein Opfer zu beklagen[1]. Foxconn ist bekannt für seine militärisch organisierte Struktur[2], nichtsdestotrotz gehören die dortigen Arbeits- und Lebensbedingungen zu den besseren in China[3]. Weit verbreitet ist die Wanderarbeit: Foxconn beschäftigt zumeist junge Frauen aus dem mittleren und ärmeren China.

Man muss aber nicht nach Fernost reisen, um unfaire Arbeitsbedingungen und Wanderarbeit in der IT-Industrie zu entdecken. Während der Großteil der elektronischen Bauteile, Leiterplatinen und ganzer Geräte tatsächlich in China hergestellt wird, finden in Osteuropa häufig noch kundenspezifische Anpassungen, Softwareeinspielungen, Tests und Verpackung statt. Beispiel Tschechien: 40 % der von uns in Westeuropa gekauften Computer werden dort endkonfektioniert. Neben Tschechien spielen das etablierte Ungarn und das aufstrebende Rumänien eine Rolle[4]. Die meisten von uns werden sich noch an die Verlegung des Bochumer Nokia-Werks in eine kleine rumänische Grenzstadt erinnern[5].

Wir dokumentieren in diesem Artikel die Arbeitsbedingungen von Migranten bei Foxconn in Tschechien, vollwertiges EU-Mitglied seit Mai 2004. Die Arbeiter sind nicht direkt dort angestellt, sondern über Agenturen, die die Akquise, Vermittlung, und den Transfer aus dem Herkunftsland organisieren. Die Arbeiter bezahlen dafür und enden auf diese Weise in einer Schuldenspirale, die ihnen keine Freiheit mehr lässt. Sie können sich kein Rückflugticket leisten, auch weil sie weniger Lohn bekommen als die angestellten Arbeiter und dies bei 12-Stunden-Schichten in 6-Tage-Wochen[8]. Ihr Lebensumfeld ist entsprechend rar. Eine Dusche, eine Toilette, eine Küche für 30 Arbeiter erwartet sie nach Schichtende.

Der Bericht „Sie trafen sich nahe Kolín" von Eva Pechová[6] aus dem Jahr 2008 beschreibt dies, der dazu passende Comic von Miloš Bárta[7] bebildert es. Beides entstammt dem Projekt „Czech made?" des multikulturellen Zentrums in Prag, dem wir genauso wie den Autoren für die Abdruckrechte danken. Ergänzt haben wir die Übersetzung eines Interviews mit einem tschechischen Foxconn-Mitarbeiter aus dem empfehlenswerten Reader „Under pressure: working conditions and economic development in ICT production in Central and Eastern Europe" der Organisation WEED, Berlin 2010[4]. Er redet offen über die Unterschiede zwischen Festanstellung und Leiharbeit.

Anmerkungen

1 *golem.de: Suizidserie bei Foxconn geht weiter. http://www.golem.de/1101/80731.html (14.1.2011)*

2 Students & Scholars Against Corporate Misbehaviour (SACOM): Workers as Machines – Military Management in Foxconn. http://sacom.hk/archives/740 (12.10.2010)

3 Joel Johnson: 1 Million Workers. 90 Million iPhones. 17 Suicides. Who's to Blame?. Wired Magazine, March 2011. http://www.wired.com/magazine/2011/02/ff_joelinchina/all/1 (28.2.2011)

4 Sarah Bormann, Leonhard Plank: Under pressure: working conditions and economic development in ICT production in Central and Eastern Europe. WEED (World Economy, Ecology and Development), Berlin, September 2010. http://www.pcglobal.org/files/under-pressure_final_version.pdf (19.11.2010)

5 Der Tagesspiegel: Nokia macht Bochumer Werk dicht. http://www.tagesspiegel.de/wirtschaft/unternehmen/nokia-macht-bochumer-werk-dicht/1142242.html (15.1.2008)

6 Eva Pechová: Potkali se u Kolína (Sie trafen sich nahe Kolín), a2 kulturní týdeník 45/2008, Bericht innerhalb des Projekts „Czech made?" des Multikulturellen Zentrums in Prag. Die Übersetzung basiert auf der Dokumentation der EMF migration conference 2009 (http://www.emf-fem.org/Areas-of-work/Migration/EMF-migration-conference-2009)

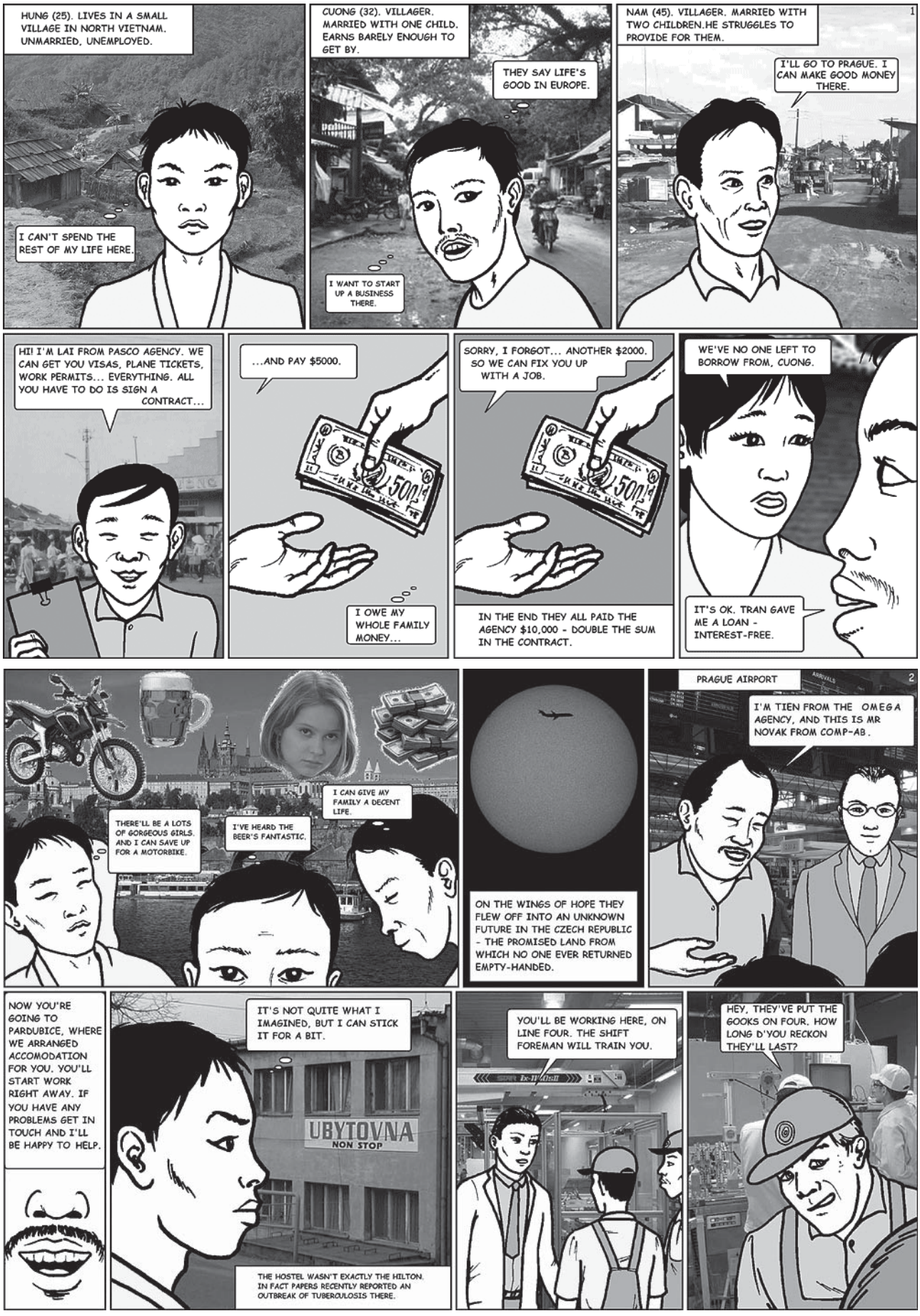
7 Miloš Bárta: Czech made? An exhibition of comics on migrant labour. (http://www.europeancity.cz/czechmade/index.php?option=com_content&task=view&id=41&Itemid=13&lang=english)

8 Michal Krebs, Eva Pechová: Vietnamese Workers in Czech Factories – Research Report – Excerpt. La Strada Czech Republic 2009

Videostill aus dem Dokumentarfilm „Behind the Screen" (http://www.behindthescreen.at), der während der FIfF-Jahrestagung 2011 in München gezeigt wird.

Miloš Bárta

2. Teil: Vietnamesische Gastarbeiter



alle Comics von Miloš Bárta *http://www.europeancity.cz/czechmade/images/stories/barta/*

Eva Pechová

3. Teil: Sie trafen sich nahe Kolín

Cuong, Hung und Nam, drei Arbeiter aus verschiedenen Teilen Vietnams, sind nach Tschechien gekommen, um zu arbeiten. Sie trafen sich das erste Mal in einem Schulungszentrum, in dem vietnamesische Arbeiter auf ihre Reise in die Tschechische Republik und die Arbeit in der Foxconn-Fabrik in Pardubice vorbereitet werden. Jeder der drei bezahlte mehr als 9.000 US-Dollar.

„Ungefähr die Hälfte der Summe bezahlten wir für den Vertrag mit der vietnamesischen Agentur Nosco. 1.500 US-Dollar gingen an die Agentur in Tschechien; wir wissen nicht, was mit dem restlichen Geld geschehen ist, da wir keine Belege oder irgendetwas bekommen haben. Es ging wahrscheinlich an irgendwelche andere Mittelsmänner."

Eine Mitarbeiterin in einer der Agenturen berichtet anonym: „Die Agentur in Vietnam behält für gewöhnlich die Hälfte des Geldes. Die andere Hälfte geht an den tschechischen Partner. Beide Agenturen haben neben den offiziellen Ausgaben wie Schulungen, Flugticket, Versicherungen, Tschechischkurs und so weiter auch hohe Bestechungskosten. Empfänger sind Mitarbeiter der tschechischen und die vietnamesischen Botschaft, Behörden in Vietnam und Arbeitgeber in Tschchien."

Bevor sie Vietnam verließen dachten Cuong, Hung und Nam, dass sie ihre Schulden innerhalb eines Jahres zurückzahlen können. Die beiden verbleibenden Jahre waren dann fürs Geldverdienen eingeplant. Recht bald wurde ihnen klar, dass sie die Schulden erst am Ende der drei Jahre abgezahlt haben werden. Das war natürlich keine günstige Verhandlungsposition gegenüber den Arbeitgebern.

Das größte Problem, das sich für die drei während ihrer Reise durch die tschechischen Fabriken ergab, war die Tatsache, dass sie keinerlei Kenntnisse des Rechtssystems und der Sprache besaßen. Nach drei Monaten bei Foxconn trat ein Dolmetscher an sie heran und forderte sie auf, einen neuen Vertrag zu unterzeichnen.

„Der Text war nicht auf Vietnamesisch, deshalb wussten wir nicht, ob es um das Ende der Probezeit oder einen Jobwechsel ging. Uns wurde erzählt, dass die Fabrik verlagert wird und dass wir unterschreiben sollten, also haben wir unterschrieben." Tatsächlich aber unterschrieben sie einen Vertrag zur Beendigung ihres Jobs in Pardubice und einen neuen Vertrag für die Foxconn-Fabrik in Kutna Hora – mit einer weiteren Probezeit. „Nirgends in der Welt dauert die Probezeit 6 Monate, nicht einmal in Vietnam", beklagte Nam.

Für ausländische Arbeiter mit einem Arbeitsvisum ist die Probezeit ein besonders sensibles Thema; verlieren sie in dieser Zeit unerwartet ihren Job, verlieren sie auch ihre Aufenthaltserlaubnis – mit einem festen Job wird diese verlängert. Cuong, Nam und Hung begannen im Juni 2008 in der neuen Fabrik in Kutná Hora zu arbeiten. Mitte August erhielten sie einen Brief der Agentur Favigroup (diese hatte die Agentur Nosco, die die Arbeiter zunächst beschäftigt, übernommen) mit der Information, dass Foxconn Arbeitnehmer aufgrund „wirtschaftlicher Probleme" entlassen würde und dass Arbeitnehmer an den Fertigungsstraßen 4 und 5 – diejenigen an denen die drei Männer arbeiteten – betroffen seien. Das Schreiben enthielt auch das Angebot für kostenlose Beschäftigungsberatung bei TPCA in

Kolín (Toyota Peugeot Citroen-Autofabrik in Kolín, ca. 15 km von Kutna Hora, der zweitgrößte Autoproduzent im Land nach Skoda) und den Hinweis, dass sie sich so schnell wie möglich bei der Agentur melden sollten.

„Wir waren total erschrocken. Wir hatten Angst, dass es den Job in Kolín bald nicht länger geben würde. Diese Angst brachte uns dazu, Foxconn zu verlassen und uns bei der Agentur zu registrieren. Zunächst wollte der Dolmetscher, dass wir knapp 300 € [umgerechnet nach aktuellem Kurs, die Red.] für die Beratung zahlten, aber wir haben protestiert und er klein beigegeben. Wir haben allerdings 60 € für eine medizinische Überprüfung bezahlt", sagte Hung.

Die drei Arbeiter bereuten später ihre Entscheidung, Kutná Hora zu verlassen. „Die Arbeit bei TPCA ist sehr fordernd. Tschechen wollen dort nicht arbeiten, also haben sie uns eingestellt. Und schlussendlich wurden in Kutná Hora keine Beschäftigten entlassen. Wir waren die Einzigen, die während der Probezeit gegangen sind, aus Angst, entlassen zu werden", fügte Hung hinzu.

Nun haben Nam, Cuong und Hung eine zusätzliche Sorge: „Unsere Arbeitserlaubnis ist nur bis Ende des Jahres gültig. Wir wissen nicht, was danach passiert. Wenn sie unsere Erlaubnis bei TPCA nicht verlängern, laufen unsere Visa aus. Wir wissen nicht, wie wir schnell einen anderen Job finden sollen. Der Bedarf an Arbeitskräften ist im Augenblick nicht besonders groß."

Wenn die Krise beginnt und sie ihren Job als Leiharbeiter verlieren, droht ihnen sofortiger Entzug der Arbeitserlaubnis und damit der Aufenthaltserlaubnis. Ihre Schulden sind dann nicht abbezahlt, sie verlieren ihre Krankenversicherung und verstecken sich als Illegale vor der Polizei und der Ausländerbehörde. Ihre Lage wäre besser, hätte Foxconn sie direkt aus Vietnam geholt und angestellt. Sie könnten in diesem Fall bei fehlender Arbeit oder gesundheitlichen Problemen leichter zurück nach Hause.

Alles was Cuong, Hung und Nam passierte, geschah im rechtlichen Rahmen. Nichtsdestotrotz haben sie das Gefühl, dass sie in der Falle sitzen und ihr Schicksal in Tschechien außerhalb ihrer Kontrolle liegt. Jemand hat sie ausgesucht, Geld mit ihnen gemacht, aber sie sind diejenigen, die das ganze Risiko tragen. Hin und wieder haben sie das Gefühl, in diesem Land nicht willkommen zu sein.

„Ich würde den Medien gern sagen, dass die Tschechen fairer zu den Arbeitern aus Vietnam sein sollten. Wir haben nichts Falsches gemacht. Wir sind nur hierher gekommen, um Geld zu verdienen; wenn die Arbeit erledigt ist, gehen wir zurück nach Vietnam – wir werden nicht für immer hier bleiben", sagt Nam, der diese Botschaft gern an seine Kollegen in der Fabrik weitergeben möchte.

Sarah Bormann und Leonhard Plank

4. Teil: Interview mit einem tschechischen Foxconn-Mitarbeiter

Warum möchten Sie anonym bleiben?
Man könnte mich sonst feuern. Es ist nicht erlaubt, Geheimnisse über die Firma zu verbreiten. So steht es im Arbeitsvertrag.

Wie sieht Ihr Arbeitsplatz im Betrieb aus?
Er ist in einer großen Halle mit mehreren Produktionsstraßen. Die Arbeiter führen in der Regel immer die gleichen monotonen Arbeitsschritte durch. Die Fabrik steht am Rande der Stadt. Wir produzieren Computer, Monitore, Set-Top-Boxen und auch Handys. In der Regel bauen wir Komponenten zusammen, die hauptsächlich aus China kommen. Es wird nur wenig fürs Inland produziert, das meiste landet auf dem europäischen Markt.

Wie sieht eine typische Arbeitswoche aus?
In den meisten Abteilungen arbeiten wir in drei Schichten, in den verbleibenden in zwei Schichten. In der Regel haben wir also 8-Stunden-Schichten, die regelmäßig wechseln. Wenn die Auftragslage steigt arbeiten wir jedoch mehr, andersherum aber auch weniger. In manchen Zeiten gehen wir Samstags oder sogar Sonntags zur Arbeit. Es passiert schon mal, dass wir drei Monate lang 12-Stunden-Schichten fahren, wenn viel zu tun ist. Das ist erlaubt, weil laut Arbeitsvertrag die Arbeitszeiten flexibel gestaltet werden können. Einen vorläufigen Schichtplan bekommen wir am Anfang einer solchen Phase, die genauen Arbeitszeiten werden aber erst eine Woche vorher festgelegt. Das Privatleben und die persönlichen Umstände spielen dabei keine Rolle. Entweder arbeitest Du oder verlässt die Firma. Manche Kollegen stressen die Überstunden sehr.

Wird im Akkord gearbeitet?
Der Schichtleiter läuft durch die Reihen und ermahnt uns, die vorgegebenen Normen zu erfüllen. Wenn nicht, dann kontrolliert er die Produktionslinie genauer. Man darf nicht so viele Fehler machen. Fehler müssen korrigiert werden, womit ein Teil des Bonusses weg ist. Jemand der häufig Fehler macht wird entlassen.

Wie hoch ist der Durchschnittslohn eines Arbeiters?
Den Durchschnittslohn kenne ich nicht. Meiner ist 585 € [umgerechnet gemäß Kurs 2009, die Red.]. Er hängt von den Nachtschichten, Überstunden und Boni ab. Mein Bonus ist 78 €. Der Arbeitgeber kann ihn verringern, z. B. wegen eines unordentlichen Arbeitsplatzes, dreckigen Mülleimern und ähnlichem. Das gilt dann gleich für die ganze Produktionsstraße. Wenn also ein Kollege schlechte Arbeit macht, sind alle betroffen. Boni bekommt man für die Erfüllung von Produktionszielen oder dem Erfüllen der vorgegebenen Überstunden. Wenn jemand mehr als vier Stunden fehlt, fällt ein Teil des Bonus für den ganzen Monat weg. Wer krank wird, verliert den Bonus ganz.

Haben Ihre Kollegen arbeitsbedingte Krankheiten?
Manche haben Probleme, ich weiß aber nicht ob es wegen der Arbeit ist. Einige haben Probleme mit den Augen, andere mit der Atmung, sie haben Asthma. Foxconn hat ergonomische Verbesserungen eingeführt, die allerdings auch die Produktivität erhöhten. Es gibt nun bessere Arbeitsplatzeinteilungen, die Teile liegen näher beieinander, um die Transportwege zu verkürzen. Neue Werkzeuge vereinfachen zudem die Abläufe.

Welche Art von Verträgen haben die Arbeiter?
Diejenigen die schon länger da sind haben unbefristete Verträge, die meisten aber, die im letzten oder in diesem Jahr begannen, haben Befristungen, meist für ein Jahr, manchmal sogar nur für ein halbes. […]

Wie viele Migranten arbeiten derzeit in der Firma?
Die Anzahl der Ausländer hängt von dem aktuellen Produktionsvolumen ab. Manchmal sind es 30 %, manchmal annähernd 50 %, in manchen Abteilungen können es sogar 70 % werden. Die Fremdarbeiter kommen und gehen. Derzeit sind die meisten Vietnamesen, gefolgt von Mongolen, Bulgaren, Rumänen und Slowaken. Die Kollegen aus der Mongolei sind inzwischen weniger geworden weil während der Krise Arbeiter entlassen wurden. Sie wurden als Gruppe angeheuert, ihre Visa liefen ab und damit ihre Arbeitsverträge. Sie konnte man am einfachsten loswerden.

Wie viele der Migranten kommen mittels Agenturen und wie lange bleiben sie?
Knapp die Hälfte wird geworben, schätze ich. Es gibt viele von den Agenturen, am bekanntesten ist mir Xawax, eine slowakische Agentur. Manche der Fremdarbeiter, z. B. die Vietnamesen, haben hier ununterbrochen drei Jahre gearbeitet. Ich nehme an, dass sie gleich für ganze Zeit angeheuert wurden, denn man kann sie ja nicht so einfach nach Hause schicken, weil es so weit weg ist. Bei den Bulgaren zum Beispiel passiert es hingegen, dass sie für einen Monat zurückgeschickt werden, wenn es zu wenig Arbeit gibt. Danach kommen sie wieder. Oder auch nicht, hängt davon ab, wer es ist.

Gibt es Unterschiede zwischen den Arbeitsbedingungen von Angestellten und Leiharbeitern?
Die Leiharbeiter arbeiten in der Regel 12-Stunden-Schichten, fünf oder sechs Mal pro Woche. Auch die Angestellten arbeiten manchmal sehr viel. Die ausländischen Leiharbeiter kommen meist hier hin, um Geld zu verdienen, daher arbeiten sie immer so viel wie der Arbeitgeber es möchte. Ich habe gehört, dass bei den Agenturarbeitern mit dem Unterschreiben des Arbeitsvertrags immer auch ein Auflösungsvertrag unterschrieben wird, ohne Datum und ohne dass eine Kopie ausgehändigt wird. Sie können also nicht verhindern, dass ihnen gekündigt wird. Aber das habe ich nur gehört, ich habe es nicht gesehen. Die Arbeitszeiten sind flexibel, gerade deshalb beschäftigt Foxconn bevorzugt Leiharbeiter.

Gibt es typische Arbeiten die für Leiharbeiter reserviert sind?
Manche Kunden haben gleich bleibende Auftragsvolumen. Dort werden meistens die Festangestellten eingesetzt. Für schwankende Produktionsnachfrage werden Leiharbeiter eingesetzt, denn wenn keine Arbeit mehr da ist, müssen sie auch nicht beschäftigt werden.

Würden Sie sagen, dass Foxconn die Lage der migrantischen Arbeiter ausnutzt, weil diese ständig Angst haben, entlassen zu werden und nach Hause zu müssen?
Ja, das glaube ich. Sie akzeptieren alles was von ihnen verlangt wird. Ich habe gehört, dass ihnen angedroht wurde, ihre Visa nicht zu verlängern, wenn sie nicht Überstunden machen. Ich bezweifle, dass die Arbeiter ihre Situation verbessern können. […]

Sylvia Johnigk, Kai Nothdurft

Diskurs zum EU Forschungsprojekt INDECT

Das FIfF im Streitgespräch mit Projektbeteiligten

Möglicherweise zeitigt die anhaltende Kritik in der Öffentlichkeit bei den INDECT-Projektbeteiligten endlich Wirkung. Die Mitglieder der Ethikkommission und einige wichtige Projektergebnisse wurden inzwischen veröffentlicht. Das ist vielleicht zum Teil auch ein Erfolg der FIfF-Kampagne gegen das Projekt.

Am 29. Dezember 2010 hielt Sylvia Johnigk auf dem 27c3, dem letzten Jahrestreffen des Chaos Computer Clubs den Vortrag „The INDECT–Project or … how the EU cultivates surveillance techniques".[1] Der Vortrag kritisierte das Projekt, das sich mit der Entwicklung von Überwachungstechnologien beschäftigt. Im Anschluss meldete sich aus dem Auditorium Herr Derkacz zu Wort, der sich als Projektbeteiligter zu erkennen gab und behauptete, dass viele der im Vortrag gemachten Aussagen unrichtig seien. Es entwickelte sich eine lebhafte Diskussion zwischen ihm und dem übrigen Publikum. Im Anschluss fand noch ein Gespräch im kleineren Kreis statt, bei dem nochmals die unterschiedlichen Sichten ausgetauscht wurden. Wir vereinbarten mit Herr Derkacz, die Diskussion fortzusetzen. Wir erhielten von ihm später einen ausführlichen Brief, den er als Richtigstellung von uns veröffentlicht haben wollte.

Wir drucken die Rückmeldung im Folgenden ab, wollen den Brief aber im Sinne eines Diskurses auch beantworten.[2]

Betreff: Misleading information about INDECT
Datum: Thu, 17 Feb 2011 17:33:39 +0100
Von: derkacz <derkacz@kt.agh.edu.pl>
An: sylvia@fiff.de
CC: fiff@fiff.de

Good afternoon,

Please find attached a document with comments and clarifications to information you give about INDECT.

We refer only to selected statements that pass to the public misleading information about the project.

27c3 was not the only case when you have given misleading information about INDECT. We would be obliged if the clarifications we send could be available at websites containing your presentations and other statements about the project.

That would be honest with respect to persons who are recipients of your information and persons who are involved in the project.

We were even more surprised to find out that broadcasting of the misleading information did not stop after the event in Berlin where clarifications to your presentation were given.

Similar set of false and uncorrect statements could be found in leaflets distributed at "Computers, Privacy & Data Protection CPDP 2011" event in Brussels.

In your presentation you mentioned a few times the question of ethics and lawfulness of what is done within the project.

Do you think that concious broadcasting of untrue information is ethical and lawful?

As I said to you in Berlin we are open to answer questions relevant to INDECT.

A good opportunity to become informed about work and outcomes of the project will be an international conference organised by INDECT in June this year: MCSS 2011. The scope of the conference includes ethical issues and law aspects in video surveillance, Internet monitoring, security research. Document with Call for Papers is attached to the mail - please feel free to distribute the document.

Regards,

Jan Derkacz

PS One of the charges against INDECT was that it performs video recordings of citizents without their consent (which by the way is not true). I was video-recorded at the event in Berlin and, what is more, the recording was made public in Internet, both without my consent. It would be interesting to have your opinion on it.

Misleading information about INDECT

Here is a list of misleading information about INDECT with clarifications:

Main documents are not published. A project that is funded by EU taxpayers is subject to secrecy and censorship.

This is definitively NOT true! No new information policy has been applied to the INDECT project. All relevant information of the INDECT project has been, is and will continue to be made publicly available on the project's website (http://www.indect-project.eu/). The project makes more than average effort in making the information available. The project is definitively interested in exposing research of the project to a broad public debate.

There are numerous ways of dissemination. For example, project results are presented at conferences, in scientific journals and in standardization activities. Furthermore, in May last year INDECT organized a two days' international conference where project results were presented in details: http://mcss2010.indect-project.eu/.

In June this year, INDECT will organize another international conference where current project results will be presented in details: http://mcss2011.indect-project.eu/.

The INDECT Project Consortium certainly agrees that transparency is a prerequisite for avoiding misunderstandings. It is for exactly this reason that all relevant documents of the INDECT project are publicly available on the project's website (http://www.indect-project.eu/). In order to make project information more user friendly and more complete, INDECT has just revamped and updated its website.

INDECT is funded under the Seventh Framework Program (FP7); grant agreement 218086, as a "Collaborative Project". INDECT research area is defined by the FP7 call "Increasing the Security of citizens" (SEC-1). INDECT is one out of 60 EU projects related to security call in the framework of FP7. For all funded under FP7 projects, and their reports, there are dissemination levels that are indicated by one of the following codes:

- PU = Public.
- PP = Restricted to other program participants (including the Commission Services).
- RE = Restricted to a group specified by the consortium (including the Commission Services).
- CO = Confidential, only for members of the consortium (including the Commission Services).

The vast majority of FP7 reports (including INDECT deliverables) are "PU" (public). Exemptions to public disclosure consider cases which contain financial statements or could impact negatively on law enforcement capabilities or business competitiveness. FP7 Security Programme projects do not contain classified information, but publishing police operational documents means making the

police weaker what would be against the idea of increasing security.

Partners are developing an infrastructure for linking existing surveillance technologies to form one mighty instrument for controlling the people.

This is definitively NOT true! INDECT is a research project. The list of objectives DOES NOT include ANY kind of global monitoring of ANY society.

The INDECT methodology imposes:

- First, detecting specific crimes (like: Internet child pornography, promotion of totalitarian symbols, trafficking in human organs, spread of botnets, viruses, malware as well as terrorism, hooliganism and thievery), and, only then,
- Second, detecting specific criminals standing behind the detected crimes.

The INDECT project is to be tested on the visitors to the 2012 European Football Championship in Ukraine and Poland.

This is definitively NOT true! The INDECT project is working on tools for a monitoring system to detect threats such as throwing objects in stadiums, in particular hazardous items (knives, fire crackers). The main purpose of this research is to develop new technology for automatic threat detection and privacy protection. Anyway, there are no plans to carry out tests during the 2012 championship at stadiums in Poland and Ukraine. At this stage the project builds the experimental setups inside the university campuses and in direct surroundings of some universities. It should be underlined that only individuals that have given written consent will participate in the research. By doing this, predefined procedures are followed, comprising letters for permissions to administer and collect consent from the people involved in the experiments. The examinations are conducted exclusively within the universities and immediately adjacent lands, in the wake of obtaining all the possible approvals and permits, from people whose image and voice is recorded and stored.

Tests during 2012 European Football Championship are overinterpretation as in the INDECT Work Plan, the INDECT Consortium has only stated that "scenarios for proceeding in the event of terrorist threats during European Football Championships 2012 (Euro 2012) in Poland and Ukraine will be prepared as a part of INDECT realization".

INDECT has known plans of test of technologies during the Olympic Games in 2012 London, rebellions, civil wars and flash mobs. Data are collected without the data subject's knowledge. Mass surveillance is carried out of people who are no danger. Data are collected without designation of purpose. Data economy or the subject's right to access or erasure are ignored. Preventive without cause collection and processing of information is possible without tangible suspicion.

This is definitively NOT true! The INDECT project will never involve processing of any personal data without the prior written consent of individuals. Should any personal data of individuals be used during the project, this will be done on the basis of "informed consent" of individuals participating in the tests. INDECT will not make any personal data processed in connection with the project available to third parties. The project will not give any personal data available processed in connection with the project to third parties.

The INDECT Project Coordinator has designated an Ethics Board. The Ethics Board supervises the ethical aspects of the project's activities. The Ethics Board ensures strict fulfillment of the EU ethical rules on privacy, data protection, prevention of dual use, etc. The Ethics Board ensures strict fulfillment of the ethical rules set to deal with privacy, data protection, prevent dual use and guarantee informed consent of users in the project.

For more details, you may want to consult the project's website: http://www.indect-project.eu/, for example tests, please refer to: http://www.indect-project.eu/events/wp1/car-plate-recognition-tests.

The Ethics Board reports to the Commission on potential improper use of research results. This requires inter alia that Article 8 of the EU Charter of Fundamental Rights be complied with, which gives everyone the right to the protection of their own personal data. It should be noted that personal data processing is limited by human rights, and voluntary acts are guaranteed on informed consent forms signed by persons whose data is being processed.

For more details, you may wish to consult the ethics section of the project's website: http://www.indectproject.eu/approach-to-ethical-issues.

There is no independent control over INDECT research.

This is definitively NOT true! First of all, the independent Ethics Review panel of the European Commission made a check of the ethical issues raised by the project. All the steps of the evaluation procedure including expert opinions, hearing procedure, have been passed successfully. Only then the project was selected for financial support.

Furthermore, the Ethics Board is an independent body. The Board does not view its role as ensuring compliance as a minimalist task, solely designed to ensure legal compliance. Rather, it sees its function as broader, including overseeing scientific and societal issues related to the research activities conducted within the project. The Ethics Board performs reviews of project Deliverables. The reviews consider such aspects as: indication and assessment of ethics related content of project reports, indication of legal framework relevant to the Deliverables, providing recommendations and proposals for possible implementation of tools elaborated in INDECT.

Finally, the INDECT Project was a subject to scrutiny carried out by Polish General Inspector of Personal Data Protection (pol. Główny Inspektor Ochrony Danych Osobowych – GIODO). Following the scrutiny a letter was issued by the Office of GIODO signed by The Director of Inspection Department. The letter sta-

tes that the scrutiny that was performed at AGH University of Science and Technology had for the scope compliance with regulations concerning protection of personal data (law from 29th August 1997 on Protection of Personal Data) and regulation of the Minister of Interior Affairs and Administration, dated to 29th April 2004 with respect to processing of personal data and technical and organizational conditions that equipment and information systems used to process personal data should be conformant to. During control, no negative comments were received.

As all projects realized in the scope of EU 7th Framework Program INDECT is a subject to periodic reviews. This year the project will undergo a mid-term review. Independent experts will evaluate the work progress of INDECT, compliance of the research performed with objectives defined before the project was accepted for financing.

INDECT technology gather information from, and fills up central/government data bases such as passports, Schengen Information System (SIS), border control system, dangerous people databases, movement databases (flight information records, toll, rail tickets), social security data, telephone tapping, cell phone tracking (e.g. via GSM/GPS), customer databases, financial transactions, RFID sensors, satellite cameras, banking information, DNA-related information, and VISA Information System (VIS). INDECT technically and organizationally supports the EU border protection agency FRONTEX.

This is just ridiculous and an obvious example of incompetence when speaking about the project's application. INDECT has absolutely nothing to do with this type of data. INDECT will NOT use highly sensitive material, such as telephone intercept, VoIP, images in passports, etc. Researchers from the INDECT consortium do not have access to nonpublic personal information stored in databases, such as the Schengen Information System (SIS), a system of border control.

INDECT researches EU Trojan Horses which record users' private computer activity.

INDECT does not involve the creation of any technology, which uses software tools remotely installed on users' computer systems. This is misinterpretation of INACT Content-Based Search System (INDECT Advanced Image Catalogue Tool) that is researched by INDECT in order to target child pornography. INACT consists of two units:

INACT Indexer and INACT Searcher. Using INACT Indexer, police officers are able to convert child pornography evidence files into a hash/descriptor database. Using INACT Searcher and the previously generated database, suspect file systems of individual, arrested computers, can be searched for similar/identical images (proofs).

„Arrested" – which means put into custody according to the country regulations. For example in Poland the Police in order to do a search of a suspect's computer has to obtain a legal warrant, which is issued only in cases when a justified suspicion of commitment of crime exists. Currently, the first version of INACT is tested by Polish Police. In the next steps the INACT search engine will be developed with respect for more efficient searching. Consequently, the statement about EU Trojan Horses is, again, absolutely not true!

Until Sep. 2010 neither civil rights activists nor privacy officers are members of the Ethics Board.

This is definitively NOT true! At the very beginning of the project (Jan. 2009), the INDECT Project Coordinator designated an Ethics Board which was accepted by Project Board. The initial composition of the Ethics Board has already included, among others, a human rights lawyer, a professor of law and a professor of human computer interaction. In Dec. 2009, the project has decided to add a new member, a professor of ethics, as an additional external expert to the project's Ethics Board. Because of the strong emphasis on the ethical issues, on Jan./Feb. 2011 yet another new external member joins the Ethics Board (a professor of ethics and philosophy).

Herr Derkacz kritisiert in seiner Email, dass wir uns einerseits gegen Videoüberwachungen aussprechen, er aber auf dem Kongress auch ohne seine Einwilligung gefilmt wurde, und er bittet uns, das zu kommentieren.

Wir können bis zu einem gewissen Grad das unangenehme Gefühl verstehen, das Sie, Herr Derkacz beschleicht, wenn Sie gefilmt werden. Der Unterschied zu einer Überwachungskamera ist aber aus unserer Sicht der Zweck der Aufnahme und die Intention des Aufgenommenen. Die Filmaufnahmen beim Kongress dienen der Dokumentation einer in und für die Öffentlichkeit geführten Diskussion der ebenso öffentlich gehaltenen Vorträge. Wenn man sich in dieser Situation als Diskussionsteilnehmer zu Wort meldet, muss man in Kauf nehmen, gefilmt zu werden. Die Filmaufnahmen und das Live-Streaming erfolgen seit mehreren Jahren und sollten insofern bekannt sein, weshalb die aktive Teilnahme an der Diskussion eine bewusste Entscheidung darstellt. Wir gehen davon aus, dass es Ihnen, Herr Derkacz auch darum ging, Ihre Kritik öffentlich zu machen. Es wäre dabei immer noch möglich gewesen, dies unter Pseudonym oder anonym zu tun, etwa durch Aufsetzen einer Sonnenbrille (Maskierung).

Wenn man die Problematik auf das Filmen bei einer Demonstration überträgt, bewirkt das Filmen eines Teilnehmers durch die Polizei eine Einschüchterung bei der freien Äußerung seiner politischen Überzeugung und schränkt das Demonstrationsrecht dadurch ein. Wenn der gleiche Teilnehmer sich auf das Sprecherpodium bei der Kundgebung begibt und dort von einer Fernsehkamera gefilmt wird, die seine Rede in den Nachrichten überträgt, geschieht das auf seinen expliziten Wunsch hin.

Als normaler Teilnehmer am Kongress informiert man sich frei und anonym (in der Regel wird man dann nicht gefilmt). Erst durch das aktive Einschalten in die Diskussion nach dem Vortrag entstand die Filmaufnahme und Veröffentlichung des Diskussionsbeitrags.

Sie werfen uns vor, unethisch zu handeln, indem wir die Unwahrheit sagen.

Sie erwähnten in ihrem Brief eine Wiederholung der „falschen" Aussagen bei einer Veranstaltung in Brüssel. Ihre „richtig stellende" Antwort erreichte uns im Februar. Dort nahmen Sie auch auf die Veranstaltung in Brüssel Bezug. Bis dahin waren Ihre korrigierenden Aussagen auf dem Kongress für uns zunächst reine Gegenbehauptungen, die nicht durch Argumente oder Belege untermauert waren. Zudem wurden die Aussagen in Brüssel nicht von uns getroffen. Wir vermuten, dass die von uns unter *Creative Commons* veröffentlichten Folien und Flyer dort von Dritten weiter verwendet wurden.

Unabhängig davon halten wir die meisten unserer Aussagen nach wie vor für richtig unter den folgenden Zugeständnissen:

Im mündlichen Vortrag hätten wir klarer abgrenzen können, wann INDECT als Projekt gemeint war und wann wir von den Folgen von Technologien sprechen, die im Rahmen von INDECT entwickelt werden. Als FIfF halten wir die Grenze zwischen beiden Aspekten für fließend und für eine eher theoretische Spitzfindigkeit, weil wir der Meinung sind, dass jeder Wissenschaftler auch für die Ergebnisse seiner Forschung verantwortlich ist. Wir wollen beide Aspekte explizit zusammen betrachten. Dennoch kann man das, was jeweils gemeint ist, sicher klarer voneinander abgrenzen, und wir werden dies in zukünftigen Beiträgen auch so halten – so bereits geschehen bei einem weiteren Vortrag.

Sie erläutern, dass unsere Aussagen zum EU-Trojaner auf einem Missverständnis beruhen.

Ihre Ausführungen dazu halten wir für glaubwürdig und Ihre Kritik an unserer Aussage daher für berechtigt. Wir werden dies zukünftig nicht mehr behaupten. Auf bereits veröffentlichte Informationen haben wir aber nur noch einen geringen Einfluss. Wir werden, wie von Ihnen gewünscht, eine Richtigstellung dieses Punktes auf unserer Webseite vornehmen.

Auf einer Veranstaltung im März 2011 haben wir in den bereits im Mai 2010 gedruckten Flyern den Passus geschwärzt und dort den EU-Trojaner auch nicht mehr im Vortrag erwähnt.

Sie behaupten, dass die wesentlichen Dokumente entgegen unserer Aussage veröffentlicht wurden.

Zu dieser Aussage haben Sie sich in Ihrem Diskussionsbeitrag auf dem Kongress bereits selbst widersprochen. Sie gaben dort indirekt zu, dass nicht alle Dokumente veröffentlicht werden, sondern nur die, „die auch veröffentlicht werden sollen".

Wir bleiben bei unserer Aussage: Einige Dokumente wurden gar nicht veröffentlicht. Bei einigen Dokumente fehlen Textseiten. Veröffentlichungen wurden wieder zurückgezogen (z. B. die Ethik-Richtlinie) und anschließend wieder veröffentlicht, das INDECT-Werbevideo[3] wurde gelöscht.

Inzwischen ist ein (aus unserer Sicht wesentliches) Dokument zur Modellierung abnormen Verhaltens und Erkennung kriminellen Verhaltens veröffentlicht worden.[4] Dies geschah aber erst nach unserer Kritik auf dem Kongress im Dezember 2010. Das Dokument stammt vom 23.7.2010, hätte also bereits beim Kongress verfügbar sein sollen.

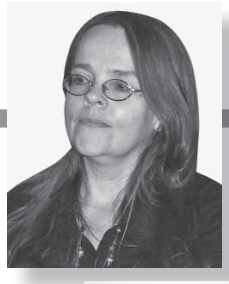
Die bis dahin veröffentlichten Beispiele von „abnormal behaviour" passten aus unserer Sicht nicht zu den offiziellen Projektzielen. Wir haben daraus geschlossen, dass wesentliche Dokumente dazu bis zum damaligen Zeitpunkt nicht veröffentlicht waren, was sich, wie gerade belegt, auch bestätigt hat.

Sie sagen in Ihrem Antwortbrief:

> *„Exemptions to public disclosure consider cases which contain financial statements or could impact negatively on law enforcement capabilities or business competitiveness. FP7 Security Programme projects do not contain classified information, but publishing police operational documents means making the police weaker what would be against the idea of increasing security."*

Dies besagt also, dass Inhalte, die Finanzen und Geschäftsgeheimnisse enthalten oder solche, die die Strafverfolgung schwächen würden, nicht veröffentlicht werden. Dies sehen wir bereits als kritische und kritikwürdige Intransparenz an.

- Finanzinformationen: Um Transparenz und Zweckbindung der Verwendung von Steuergeldern/Projektmitteln sicherzustellen, sollten auch die Finanzdaten veröffentlicht wer-



Sylvia Johnigk und Kai Nothdurft

Sylvia Johnigk studierte Informatik an der TU-Berlin und befasste sich schon im Studium mit Themen wie Datenschutz und Informationssicherheit, arbeitete fünf Jahre in der Forschung am Thema Informationssicherheit und acht Jahre bei einem Finanzdienstleister als IT-Security Consultant in Frankfurt am Main. Seit Mitte des Jahres 2009 ist sie selbständig und leitet ein kleines Unternehmen in München, das sich auf Beratung von Unternehmen zum Thema Informationssicherheitsmanagement mit dem Schwerpunkt Mitarbeitersensiblisierung spezialisiert hat.

Kai Nothdurft studierte Informatik an der Uni Bremen und beschäftigte sich schwerpunktmäßig mit Datenschutz und IT-Sicherheit. Nach dem Studium arbeitete er fünf Jahre als Freiberufler im Schulungs- und Consultingbereich. Seit 1999 arbeitet er als IT-Sicherheitsbeauftragter für ein großes deutsches Versicherungsunternehmen.

den. Diese sollten nur insofern eingeschränkt preisgegeben werden, als darin keine vertraulichen Daten wie Bankverbindungen enthalten sind. Es ist dagegen wünschenswert darzustellen, wofür Steuergelder eingesetzt werden und welche Projektpartner welche Gelder erhalten.

- Geschäftsgeheimnisse: Warum werden Geschäftsinteressen einzelner Firmen mit Steuermitteln gefördert? Warum dürfen die Firmen Projektergebnisse kommerziell für sich verwerten, obwohl die Allgemeinheit sie bezahlt?

- Gefährdung operativer Polizeiarbeit: Auch bezüglich der operativen Polizeiarbeit wären nur personenbezogene Daten von konkret Verdächtigten oder Ermittlern zu entfernen. Informationen aus laufenden, nicht abgeschlossenen Verfahren dürften dem Forschungsprojekt ohnehin nicht zur Verfügung stehen. Außerdem sehen wir folgenden Widerspruch: Wie kann die jetzige Polizeiarbeit geschwächt werden, wenn die Technik nur Forschung ist, ausschließlich ein Prototyp entwickelt wird und der mögliche spätere Einsatz, wie von Ihnen in der Diskussion behauptet, gar nicht Thema von INDECT ist? Anderenfalls ist INDECT eben kein reines Forschungsvorhaben sondern ein Entwicklungsprojekt, und die erwarteten Ergebnisse müssen sich erst recht der von uns geforderten unabhängigen Technikfolgenabschätzung und dem politischen Diskurs stellen.

Sie bekräftigen die Unabhängigkeit der Ethik-Kommission, die von uns bezweifelt wird. Sie haben ferner (in der Diskussion in Berlin) behauptet, dass die Zusammensetzung der Ethik-Kommission entgegen unserer Aussage keineswegs geheim sei.

Zu dem damaligen Zeitpunkt war die Zusammensetzung geheim, und nur einige Mitglieder waren öffentlich bekannt. Inzwischen wurden die Namen allerdings veröffentlicht (siehe unten).

Die Geheimniskrämerei des Projekts nährte Spekulationen, die Sie sich damit selber zuzuschreiben haben. Die uns damals bekannten veröffentlichten Informationen zeigten, dass der Vorsitzende der Ethik-Kommission von seiner eigenen Assistentin kontrolliert werden sollte.

Außerdem stellten wir uns folgende Fragen: Was ist die Motivation, die Namen geheim zu halten, wenn man solche Verdächtigungen vermeiden will? Gibt es da noch andere *Leichen im Keller*, die man verbergen möchte? Angeblich hat, wer nichts zu verbergen hat, doch nichts zu befürchten!

Bei den in Ihrem Antwortbrief erwähnten (nicht durch konkrete Namen überprüfbaren) weiteren Personen handelt es sich bisher immer noch nicht um Datenschützer oder Bürgerrechtler.

Der von Ihnen erwähnte polnische Datenschutz-Beauftragte gehörte eben nicht der Kommission an. Er hat das Projekt nur zu Beginn geprüft, und eine Kontrolle während der Laufzeit ist allein damit keinesfalls gewährleistet. Warum wurde dem EU-Parlament die Auskunft verweigert, wer Mitglied der Kommission ist? Wie wird eine vom Projekt unabhängige Kontrolle der Ergebnisse gewährleistet? Selbst wenn aus den oben genannten Argumenten für Geheimhaltung nicht die Öffentlichkeit die Kontrolle ausüben sollte, müsste es eine von der Öffentlichkeit als vertrauenswürdig eingestufte, zur Vertraulichkeit verpflichtete Kontrollinstanz geben. Wir haben sehr deutlich gemacht, warum die derzeitige Ethik-Kommission diese Rolle nicht erfüllt.

Dass die Zusammensetzung der Kommission nicht veröffentlicht wurde, machte die Rolle die Ethik-Kommission unglaubwürdig. Aus unserer Sicht entsprach die Information über die Zusammensetzung der Ethikkommission nicht den Geheimhaltungsinteressen, die in Ihrem Schreiben genannt wurden.

Inzwischen wurden immerhin die Mitglieder der Ethik-Kommission veröffentlicht – was vielleicht auch ein Erfolg der öffentlichen Kritik (des FIfF und anderer) ist:[5]

- Drew Harris, PSNI Assistant Chief, Police
- Dobrosław Kot, External Doctor of Philosophy
- Emil Pływaczewski, External Academia, Professor of Law
- Andreas Pongratz X-Art Industry, Head of the company
- Tom Sorell, External Professor of Ethics
- Ralph Roche, PSNI Human Rights Lawyer
- Zulema Rosborough PSNI Police Officer 8 Mariusz Ziółko AGH Researcher in the domain of security-related technologies

Until Sep. 2010 neither civil rights activists nor privacy officers are members of the Ethics Board.

This is definitively NOT true!

Auch nach der Veröffentlichung der Mitglieder stellen wir fest: Es sind immer noch kein NRO-Vertreter und kein Datenschützer in der Kommission, weshalb wir die Kommission nicht für geeignet halten, die Auswirkungen der Forschungsergebnisse kritisch zu überprüfen. Schlimmer noch, es ist nur ein einziges unabhängiges Mitglied vertreten, das (soweit wir das erkennen können) nicht selbst Projektbeteiligter ist (Prof. Sorell). Die Kommission hat – ein weiterer Kritikpunkt – auch gar nicht die Aufgabe, die Projektergebnisse auf Verträglichkeit mit ethischen Grundsätzen zu prüfen, sondern sie beschränkt sich auf die rechtskonforme Durchführung des Projekts während der Laufzeit, was eigentlich eine Selbstverständlichkeit sein sollte.

Sie kritisieren unsere Bewertung, dass mit INDECT ein mächtiges Überwachungsinstrument geschaffen wird:

„Partners are developing an infrastructure for linking existing surveillance technologies to form one mighty instrument for controlling the people. *This is definitively not true ...“*

Dazu fragen wir: Was genau stimmt hier nicht, vielleicht die Wertung „mighty“? Oder ist eine Überwachungskamera keine Überwachungsinfrastruktur? Forschen Sie nur an unnützen Sachen, die keine praktische Wirkung haben? Oder meinen Sie, dass Überwachungsinstrumente keine Wirkung erzielen, durch die Menschen beeinflusst (*controlled*) werden?

Weshalb Sie hier versuchen, dagegen zu argumentieren, liegt unseres Erachtens erneut am unterschiedlichen Bezug. Wir beziehen uns hier eben nicht auf INDECT als isoliert betrachtetes Projekt, sondern auf den Einsatz der in INDECT erforschten oder vielmehr entwickelten Technologien in der Praxis. Es handelt sich

hier um eine Bewertung der zu erwartenden Projektergebnisse. Das können wir zukünftig gerne deutlicher hervorheben, falls es missverständlich war.

Sie sagen, dass entgegen unserer Behauptung kein Einsatz von INDECT in Stadien erfolgt.

Unsere Aussage beruhte auf folgenden Informationen:

Es wurde vom INDECT Projekt eine Genehmigung eingeholt, in einem Stadion arbeiten zu können.[6] Wozu dient dieser Aufwand, wenn man nicht zumindest in Erwägung gezogen hat, solche Tests durchzuführen?
Es gab eine öffentliche Ankündigung vor Journalisten von Andrzej Czyzewski[7] und diverse Presseberichte[8]. Selbst auf der INDECT-Projektseite wurde erwähnt, dass ein entsprechender Antrag gestellt wurde. Missverständnisse (sofern es wirklich welche sind) sind hier ggf. der desaströsen PR des Projekts geschuldet.

Können Sie bestätigen, dass auf den Einsatz in Stadien (wo auch immer) während der gesamten Projektlaufzeit verzichtet wird? Wie sieht es mit dem späteren Einsatz der Technologie nach Projektabschluss aus, den wir sogar noch problematischer finden, als einen Einsatz im Projekt selbst?

Was genau sind die Szenarien (Erkennung von Gewalt in Stadien), die nach Ihrer Aussage durchaus im Projekt betrachtet werden und die wir angeblich überinterpretieren? Auch Ihre Antworten auf die Fragen des EU-Parlaments lassen reichlich Raum für Spekulationen.[9]

Sie sagen zum Einsatzszenario bei den Olympischen Spielen in London, dass kein Test in ‚real life' ohne Zustimmung der Betroffenen erfolgt.

Wir haben unsere Information aus dem Bericht in Spiegel-Online vom 24.1.2010: „Britische Polizei will Bürger mit Drohnen überwachen",[10] Sie sollten, falls das falsch ist, zu einer Richtigstellung auffordern, die wir ggf. auch publizieren.

Unsere Kritik an der rechtlichen Zulässigkeit bezieht sich wiederum auf Probleme des späteren Einsatzes der in INDECT entwickelten Technik, nicht auf die Durchführung des Projekts selbst.

Sie bezeichnen unsere Aussage, dass INDECT-Daten auch mit Daten aus anderen Kontexten verknüpft werden oder diese anreichern, als lächerlich und als inkompetent.

Aus den Folien wird aus unserer Sicht sehr deutlich, dass sich unsere Aussage nicht auf die Projektdurchführung bezieht, sondern es sich dabei um einen Ausblick in die Zukunft handelt. Wir stellen die Forschungsergebnisse von INDECT in einen gesamtpolitischen Kontext zur Europäischen Sicherheitspolitik, die unter anderen auch das INDECT-Projekt finanziert. Man kann leider nicht ausschließen, dass Überwachungsdaten aus Technologien, die innerhalb des INDECT-Projekts entwickelt werden, mit anderen existierenden Datenbanken von Sicherheitsbehörden verknüpft werden. Eine derartige Naivität fänden wiederum wir lächerlich.

Das Projekt besitzt einen politischen Kontext. Es muss auch in diesem Kontext in seinen gesamtgesellschaftlichen Auswirkungen bewertet werden!

Anmerkungen

1 *Link zum 27C3 Vortrag: http://www.youtube.com/watch?v=9jerN8iSXCc*
2 *Wir werden diesen Diskurs auch ins Englische übersetzt auf der FIfF Projektseite: panopticum-europe.eu publizieren*
3 *http://upload.wikimedia.org/wikinews/en/3/39/INDECT-400px.ogv*
4 *Del 4.3. machine learning methods for behavioural profiling http://www.indect-project.eu/files/deliverables/public/D4.3.pdf/view*
5 *http://www.indect-project.eu/ethics-board-members*
6 *http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-6912&language=EN*
7 *U.a. erwähnt in einer parlamentarischen Anfrage von MdB Andrej Hunko: http://www.andrej-hunko.de/start/downloads/doc_download/40-open-letter-indect, S.3 Frage 11. Is it true that INDECT is to be used or tested during the 2012 UEFA cup in Poland, as announced by the INDECT project leader Andrzej Czyzewski in 2008 to German journalists?*
8 *http://derstandard.at/1282273529132/Projekt-Indect-EU-erforscht-perfekte-Schnueffelei*
9 *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2010-6912+0+DOC+XML+V0//EN*
10 *http://www.spiegel.de/panorama/gesellschaft/0,1518,673671,00.html*

Sylvia Johnigk

Bewertung der Sicherheitsmaßnahmen im Forschungs-Rahmenprogramm

Das Europäische Parlament hat eine Studie in Auftrag gegeben, die das Forschungsprogramm FP7 der EU zu Sicherheitsthemen bewertet. Im Folgenden werden die Ergebnisse dieser Studie zusammengefasst. Die Studie trägt den Titel: „Review of security measures in the Research Framework Programme". Autoren sind Mr. Julien Jeandesboz, Mr. Francesco Ragazzi. Verantwortlicher: Mr. Alessandro Davoli. Die Studie entstand im Auftrag des „European Parliament's Committee on Civil Liberties, Justice and Home Affairs". Die ausführlichen Ergebnisse können unter http://www.europarl.europa.eu/studies nachgelesen werden (dort den Titel in die Suchmaske eingeben).

Die Studie liefert eine Bewertung des EU *public-private dialogue*[1] in der Sicherheitsforschung und der Projekte, die zur Zeit im Rahmen des 7. Forschungs-Rahmenprogramms (FP7) finanziert werden. Untersucht wurde dabei ihr Beitrag zur Entwicklung von Freiheit, Sicherheit und Gerechtigkeit.

In der Studie wurden zwei Fragen gestellt, die aus den allgemeinen Zielsetzungen abgeleitet wurden, die das *Stockholmer-Programm*[2] definiert:

- In welchem Ausmaß wird von der EU finanzierte Sicherheitsforschung zum Nutzen der Bürger eingesetzt?
- In welchem Ausmaß tragen die Projekte zur Stärkung der Grundrechte und Freiheiten bei?

Ziele der Studie waren:

- einen Überblick über den public-private dialogue zu liefern, der von der Europäischen Kommission befürwortet wird,
- die qualitative und quantitative Analyse der Forschung im Rahmen des FP7,
- die Untersuchung der zukünftigen Entwicklung der EU-Sicherheitsforschung und -entwicklungstätigkeiten[3].

Wesentliche Ergebnisse

Bewertung des public-private dialogue

EU-Sicherheitsforschungs- und Entwicklungsaktivitäten waren primär dadurch geprägt, dass zwischen Repräsentanten der Verteidigungsministerien und Innenministerien der EU-Staaten und Vertretern der Verteidigungs- und Sicherheitsindustrien der EU und assoziierten Staaten enge Kontakte hergestellt wurden. Aus diesem Prozess wurden Vertreter der Zivilgesellschaft, des Parlaments, Bürgerrechtler und Datenschutzbeauftragte größtenteils ausgeschlossen.

Das Ergebnis dieses Prozesses ist ein Dialog, der entsprechend eingeschränkt ist. Er richtet Sicherheitsforschung an den Interessen von Sicherheitsdiensten, -services und Sicherheitsindustrien aus, ohne die Bedürfnisse einer freiheitlichen EU zu berücksichtigen.

Analyse der Sicherheitsforschung, die im Rahmen des FP7 unternommen wird

Es zeigt sich im Rahmen der geförderten Forschungsprojekte eine ungleichmäßige Verteilung der Förderung, die sich auf eine kleine Anzahl von Staaten und eine kleine Anzahl von Organisationen konzentriert, die meistens aus großen Verteidigungs- und Sicherheitsunternehmen und angewandten Forschungsinstitutionen stammen. Zusätzlich arbeitet ein großer Anteil dieser Projekte an der Entwicklung von Überwachungstechnologien und vernachlässigt die breite Reflexion der Auswirkungen solcher Technologien auf die Bürger und Personen, die von der europäischen Sicherheitspolitik betroffen sind.

Zukünftige Entwicklungen im Feld der Sicherheitsforschung in der EU

Pläne für die zukünftige Entwicklung der Sicherheitsforschung auf europäischer Ebene zeigen, dass die oben erwähnten Tendenzen nicht grundlegend in Frage gestellt werden. Obwohl die Planungen ein wachsendes Bewusstsein für Grundfreiheiten und Rechte zeigen, bleiben sie zu sehr begrenzt durch die Interessen der Rüstungs- und Sicherheitsindustrie und der nationalen und europäischen Sicherheitsbüros und Dienststellen.

Empfehlungen

Die wichtigste Empfehlung zur kurzfristigen Umsetzung ist, eine gründliche Untersuchung der durch die EU geförderten Sicherheitsforschung einzuleiten, die vier Aspekte umfassen soll:

- Analyse von Konten und Etats durch die Revisoren des Europäischen Gerichtshofs,
- Evaluation des Datenschutzes und der Vertraulichkeit durch den Europäischen Datenschutzbeauftragten EDPS und/oder die Arbeitsgruppe Art. 29,
- Bewertung zu Grundrechten und Freiheit, geleitet durch die Grundrechteagentur der EU und schließlich
- vollständige Auswertung durch eine STOA[4] des Europäischen Parlaments.

Die wichtigste mittelfristig zur Umsetzung empfohlene Maßnahme ist, dass das EU Parlament darauf bestehen soll, dass

- die Kontrolle der Sicherheitsmaßnahmen im Forschungsrahmenprogramm in die Zuständigkeit der Forschungsabteilung anstelle der Abteilung für Industrie gegeben wird,
- eine Zweckbindung für einen festgelegten Anteil (10-15 %) der zukünftigen Mittel der Sicherheitsforschung für den Bereich Freiheit und Grundrechte vorgeschrieben wird,
- im Kontext der EU Innen- und Außensicherheitspolitik ein spezifischer Forschungsbereich zu Freiheiten und Grundrechten entsteht.

Anmerkungen

1 *Dabei handelt es sich um eine Kooperation zwischen öffentlichem und privatwirtschaftlichem Sektor.*
2 *http://de.wikipedia.org/wiki/Stockholmer_Programm*
3 *so wie vorgesehen im Abschlussbericht des Europäischen Forums für Sicherheitsforschung und Innovation (ESRIF) und der Kommission „Europäische Agenda für Sicherheitsforschung und Innovation" vom Dezember 2009*
4 *STOA = Science and Technology Options Assessment*

Joerg Zeltner

Der Bologna-Prozess und seine Auswirkungen auf die studentische Gesellschaft

Bericht aus dem KIF-Arbeitskreis 2011

Im Rahmen der **K***onferenz der* **I***nformatik-***F***achschaften (KIF), die zweimal pro Jahr durch Studentinnen und Studenten von Universitäten und Fachhochschulen organisiert wird und im Juni dieses Jahres zu Gast in Hamburg war, finden Diskussionsrunden und Arbeitskreise zu einer Vielzahl von Themenbereichen statt. Einige davon behandeln technische Fragestellungen, andere beschäftigen sich mit Organisation und Planung und wieder andere drehen sich auch um politische Themen wie die Wechselwirkungen zwischen Informatik und Gesellschaft. Auf der aktuellen* 39,0-ten KIF *wurde im Rahmen eines Arbeitskreises über den hochschulpolitischen* Bologna-Prozess *und seine Auswirkungen diskutiert.*

Der Begriff *Bologna-Prozess* bezeichnet ein politisches Vorhaben, mit dem bis zum Jahr 2010 ein einheitlicher Europäischer Hochschulraum geschaffen werden sollte. Der Name beruht auf einer im Jahr 1999 von 29 europäischen Bildungsministerinnen und Bildungsministern in der italienischen Stadt Bologna unterzeichneten gleichnamigen Erklärung. Diese stellt an sich lediglich eine politische Absichtserklärung dar und ist nach wie vor nicht rechtlich bindend. Das erklärte Ziel der Bologna-Erklärung war, ein dreigliedriges Studiensystem und ein unter möglichst vielen Hochschulen vergleichbares Kreditpunkte-System einzuführen.

Neben den hehren Absichten der europäischen Bildungsministerinnen und Bildungsminister wurden viele kritische Stimmen laut:

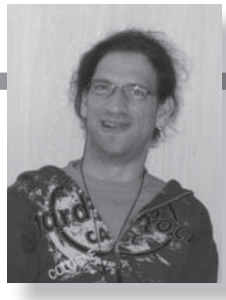
So stellt sich unter anderem die Frage nach der Legitimation des Prozesses, da Studentinnen und Studenten sowie Studierendenverbände erst sehr spät, lange nachdem der Prozess in Angriff genommen worden war, hinzugezogen wurden. Eine spezifische Abstimmung über den Prozess an sich wurde nie abgehalten – sicherlich auch deshalb, weil über lange Zeit keinerlei öffentliche Debatte geführt wurde.

Abseits der *grauen Theorie* beobachten Studierende im Bereich der Informatik, Technikwissenschaften und weiterer Studienrichtungen, dass sich im Rahmen des Bologna-Prozesses die Tendenz zu Anwesenheitspflicht in Vorlesungen, Seminaren und Übungen erhöht hat und häufig höhere Ansprüche innerhalb einer kürzeren Gesamtstudienzeit gestellt werden.

In einem Arbeitskreis auf der KIF wurde diskutiert, ob obligatorische Einschränkungen wie zum Beispiel Anwesenheitspflicht für die Studierenden eine im Allgemeinen nützliche oder aber eine hinderliche Regelung sind. Obwohl beide argumentativen Seiten vertreten waren, ergab die Diskussion den Konsens, dass die mit dem Bologna-Prozess begründeten Regelungen (welche – so ein Ergebnis der Debatte – oft genug überhaupt nicht durch den Beschluss erzwungen werden) häufig auf Kosten der Studierenden gehen, sei es durch Einschränkung in der Modulbelegung wegen unumgänglicher Anwesenheit oder durch Beschneidung von Unternehmungen außerhalb des Curriculums.

Weitere Fehlentwicklungen offenbaren sich, wenn manche Universitäten durch stetige und anhaltende Senkung der staatlichen Zuschüsse quasi gezwungen werden, sich dem Paradigma der Rentabilität zu unterwerfen und beispielsweise zur Kostendeckung in absurder Weise Studierende anwerben, obwohl für diese keine Kapazitäten mehr vorhanden sind, nur um mit den zusätzlichen Studiengebühren die laufenden Kosten zu decken.

Da Studierende aus verschiedenen Standorten Deutschlands und Österreichs auf der KIF anwesend waren, konnte ein Erfahrungsaustausch über diverse Umsetzungen des Bologna-Prozesses stattfinden. Dabei wurde unter anderem deutlich, dass das Ziel der besseren Vergleichbarkeit und Anrechnung von Modulen über Hochschulgrenzen hinweg nicht erreicht wurde. Viele Universitäten erkennen an anderen Hochschulen belegte Kurse und Module nur unzureichend oder gar nicht an. Individuellere Auslegungen der Studieninhalte außerhalb der eigenen Hochschule, so zum Beispiel Auslandsfachsemester, werden ebenfalls nicht oder nur zu einem geringen Anteil als tatsächliche Leistungen anerkannt. Das führt zu dem strukturellen Problem, im Rahmen eines standardisierten Verfahrens erlangtes Wissen zu messen. Dies wurde im Arbeitskreis kritisch diskutiert, denn jede Messung hängt von willkürlich gewählten Parametern ab und kann somit den individuellen Studierenden nicht gerecht werden.



Joerg Zeltner

Joerg Zeltner studierte Informatik und Philosophie an der Universität Bonn und der RWTH Aachen, arbeitet als freier Autor und Dramaturg für diverse Theater-, Film- und Fernsehproduktionen. Er war 2007-2011 im FIfF-Vorstand und fungierte als Kontaktperson zwischen KIF und FIfF.

Im Arbeitskreis stellte sich heraus, dass an verschiedenen Hochschulen sehr unterschiedliche Vorgaben zur freien Wahl und Anrechnung von Fächern auf das Studium bestehen. Einige Hochschulen haben sehr enge Studienpläne, von denen eine Abweichung kaum möglich oder zumindest nicht vorgesehen ist. Andere haben großzügigere Wahlpflicht-Pools oder umfassen individuelle Ergänzungen im Modulplan. Das widerspricht dem erklärten Ziel der deutlicheren Vergleichbarkeit von Studiengängen unterschiedlicher Hochschulen.

Zu guter Letzt wurden die Auswirkungen des Bologna-Prozesses auf die Struktur der Gesellschaft *außerhalb der Hörsäle* besprochen. Die geringe Wahlbeteiligung an Hochschulwahlen (zum Teil weniger als 10 %) wurde als ein Indiz dafür gesehen, wie sehr sowohl Politik als auch Gesellschaft aus dem Fokus der Hochschulausbildung herausgerückt sind.

Unter den Studierenden herrschte die übereinstimmende Meinung, dass auf *höherer Ebene* wahrscheinlich keine Planung dieser Effekte stattgefunden hat, aber die eingetretenen Effekte einer Änderung der aktuellen Verhältnisse selbst entgegen wirken: Wer sich nicht für Politik interessiert, wird auch nicht politisch aktiv.

Im Gesamtkonsens des Arbeitskreises wurde zum Ende der Diskussion hin deutlich: Wer in der heutigen Welt nicht bereits in den ersten Jahren des Erwachsenwerdens eine „political literacy", d. h. ein Grundwissen über politische Prozesse, Abläufe und Zusammenhänge erworben hat, wird insgesamt unkritischer und verliert seinen Blick auf die Funktionsweise des Ganzen. Ein hoch spezialisiertes Bachelor-Master-System, welches einzelne Studiengänge weiter und weiter verengt, riskiert eine Welle von *Fachidioten* als Absolvierende. Das wird erhebliche negative Auswirkungen auf die gesamte Gesellschaft haben, da eine gesunde Gesellschaft darauf aufbaut, dass kritische Geister mit breiter Bildung den Status quo hinterfragen, Missstände aufzeigen und sich für ihre Beseitigung einsetzen.

Ganz persönlich möchte ich hier ergänzen: Eine Gesellschaft, die nicht die persönliche Freiheit und die Allgemeinbildung über das Angebot eines breiten Spektrums an Bildungsthemen fördert oder dieses sogar durch politische Entscheidungen strukturell erschwert, bringt sich selbst in Gefahr.

Sebastian Jekutsch

Altcomputer aus Europa

Von Reuse, Recycling und illegalem Export

Desktop-Computer, Röhrenmonitore, Laptops, Handys und sicher auch bald LCD-Displays, Smartphones und Tablets: Die Menge an ausgedienter Hightech, mit der wir unser Geld verdient und unsere Freizeit verbracht haben, ist enorm und wächst zusehends. Doch wohin damit? Die Europäische Union (EU) hat bei der Beantwortung dieser Frage vor nunmehr fast 10 Jahren weltweit Trends gesetzt – mit unterschiedlichem Erfolg.

Computer, Handys und alles dazwischen und daran (kurz: IT) sind eine besondere Kategorie von Elektrogeräten, denn in ihnen sind ungewöhnlich viele Metalle, Chemikalien und Verbundstoffe verarbeitet und das in vergleichsweise hoher Qualität. Wenn sie entsorgt werden sollen, stößt es auf besonderes Interesse, denn sie sind genauso giftig wie wertvoll.

Es gibt zwei Arten von Regelungen für die Behandlung von Elektroaltgeräten: (a) Verwertungsgebot und (b) Exportverbot. Beides ist motiviert durch (c) eine nachhaltige Behandlung von für Mensch und Umwelt gefährlichen Stoffen in den Geräten. Das Agieren mit den Altgeräten ist zunehmend getrieben vom Wert der Rohstoffe, die in ihnen stecken. Seit einiger Zeit intensiviert sich auch die Diskussion über den Zugang zu wichtigen Rohstoffen; eine gesetzliche Regelung hierzu gibt es aber noch nicht.

Drei Richtlinien bestimmen unseren Umgang mit Altgeräten: Die EU-Elektroschrottrichtlinie WEEE (a), das Baseler Abkommen über deren Export (b) und die EU-Richtlinie RoHS zu deren gefährlichen Inhaltsstoffen (c). Alle drei wurden von den EU-Mitgliedsländern in nationales Recht übernommen (siehe auch [10]). Die EU ist weltweit Vorreiter auf diesem Gebiet.

RoHS – Restrictions of Hazardous Substances Directive 2002/95/EG

Der Grundgedanke der RoHS-Richtlinie ist, dass die Probleme mit dem Elektroschrott sich eher durch verbessertes Produktdesign *(upstream)* lösen lassen als durch seine verbesserte Entsorgung *(downstream)*. Die Richtlinie beschränkt sich darauf, gewisse Stoffe zu verbieten bzw. ihre Mengen deutlich zu reduzieren und auf Ersatzstoffe zu verweisen. Zu nennen wären hier Schwermetalle, Flammschutzmittel und Weichmacher. Wo es keinen Ersatz gibt, bleibt alles beim Alten. So bleibt Quecksilber in LCD-Bildschirmen erlaubt [8]. Eine inzwischen unbeliebte Alternative wären vielleicht Röhrenbildschirme, die enthalten jedoch zwingend Blei – das deshalb ebenfalls erlaubt bleibt. Es wurden zudem einige generelle Ausnahmen für medizinische und militärische Geräte zugelassen.

Blei wurde jedoch deutlich eingeschränkt in seiner Benutzung im Lot *(Lötzinn)* zur Bestückung der Platinen. Dort hilft es, die Schmelztemperatur zu senken und damit die Verarbeitungsdauer und benötigte Hitze. Blei ist aber nicht nur in der Entsorgung giftig, sondern in den Dämpfen beim Löten auch während der Herstellung und Reparatur. In Folge der RoHS-Richtlinie

wurde in China die Computer-Produktion auf weniger bleihaltige Lote umgestellt. Wegen der Marktmacht europäischer Markenhersteller wirkte sich das auch auf Produkte amerikanischer Auftraggeber aus, denn die Produktionsstraßen werden einheitlich gefahren.

Die EU-Richtlinie hat ihren Arbeitsplatz weniger gesundheitsschädlich gemacht. © SACOM, Pun Ngai

Folge der Ent-Blei-ung ist aber ein gestiegener Anteil von Zinn und Silber in den Computerplatinen. Da diese Stoffe derzeit noch nicht ausreichend als Recycling-Material zur Verfügung stehen (im Gegensatz zum Blei), stieg der Rohstoffabbau in Bergwerken. Zinn kommt zu einem erheblichen Teil aus dem Kongo oder Indonesien [13] und die dortigen Verhältnisse sind haarsträubend.

Es ist ein wesentlicher Schwachpunkt der RoHS-Richtlinie, dass sie lediglich auf die Inhaltsstoffe an sich achtet, nicht aber darauf, ob die Gewinnung oder Verarbeitung eines (Ersatz-)Stoffs umwelt- und menschenfreundlich ist. Auch wird ausschließlich betrachtet, was im Endprodukt ist, und damit später in unseren Landen entsorgt werden muss, nicht aber, welche Stoffe im Herstellungsprozess genutzt werden. So sind gefährliche Reinigungsmittel nicht durch die EU verboten [14]. Dass also die Arbeiterinnen in Übersee, die Platinen löten, es nun bleifreier tun können, ist eher Zufall und nicht explizit beabsichtigt.

Dennoch war die RoHS-Richtlinie ein großer Fortschritt. Auch Kalifornien hat inzwischen ein ähnliches Gesetz, genauso wie die Türkei, Kanada, Australien, Südkorea, Japan und sogar China [1]. Die EU arbeitet weiter daran; gerade in diesen Tagen wurde in der Kommission eine Ausweitung der Regelungen beschlossen.

WEEE – Waste from Electrical and Electronic Equipment Directive 2002/96/EG

WEEE ist die englische Abkürzung für Elektro(nik)schrott, bezeichnet aber auch die EU-Richtlinie, die den *Downstream* regelt, also die Frage, was mit einem Gerät geschieht, wenn der Besitzer es nicht mehr haben möchte. In Deutschland wurde sie mit der RoHS-Richtlinie durch das Elektro- und Elektronikgerätegesetz in nationales Recht umgesetzt. Das ElektroG ist seit 2005 in Kraft.

Grundprinzip der WEEE-Richtlinie ist die *erweiterte Herstellerverantwortung:* Der Hersteller ist nicht nur für die Produktion und die Gewährleistung während der Nutzung, sondern auch für die Entsorgung seines Produkts verantwortlich. Rein formal könnten wir beim Hersteller unser Altgerät also einfach zurückgeben, beim Kauf haben wir die Entsorgungskosten nämlich meist schon bezahlt. In Deutschland läuft die Entsorgung von Elektroaltgeräten seit dem ElektroG in aller Regel aber anders ab (siehe auch [6]):

1. Verbraucher bringen Altgeräte zu einer kommunalen Sammelstelle. In den Hausmüll dürfen sie die Geräte nicht werfen, und sei es nur eine Computermaus. Manche Hersteller bieten selbst organisierte Rücknahmen an, das ist aber die Ausnahme.

2. Auf dem Sammelhof wird das Gerät in einen von fünf Containern gelegt, je nach Geräteart. Die gesamte IT gehört zusammen mit der Unterhaltungselektronik in eine solche Gruppe. Manche Kommunen sortieren hier schon funktionsfähige Geräte aus und verkaufen sie, meist Haushaltsgeräte.

3. Wenn ein Container voll ist, wird das einer staatlichen Zentrale (EAP) gemeldet, welche gemäß einem Berechnungsmodell einen Hersteller anweist, den Container abzuholen. Das Modell basiert im wesentlichen auf dem Anteil der aktuell verkauften Geräte und zwar nach Anzahl und Gewicht [5].

4. Der ausgewählte Hersteller beauftragt daraufhin ein Transportunternehmen, den Container abzuholen und einen leeren aufzustellen.

5. Die Geräte werden zu einem vom Hersteller ausgesuchten Recyclingunternehmen transportiert.

6. Dort erst wird nach wiederverwendbaren Geräten und Teilen gesucht. Der verbleibende Schrott wird manuell zerlegt, einige Teile getrennt und der Rest geschreddert, schließlich mechanisch-elektrolytisch-thermisch die Rohstoffe getrennt, die das Recyclingunternehmen dann verkauft.

Bevor wir auf die Wirksamkeit dieses Vorgehens eingehen: Es ist allgemeiner Konsens, dass die Wiederverwendung *(Reuse)* der Geräte nachhaltiger ist als ihre stoffliche Verwertung *(Recycling),* während Recycling wiederum der finalen Entsorgung (Müllhalde und Verbrennung) vorzuziehen ist. Das sieht die Bundesregierung [6] genauso wie die EU [3]. Daran muss sich das Gesetz messen lassen.

Sammlung, Transport und Verwertung sind auf verschiedene Akteure verteilt. Jeder fühlt sich folglich nur für einen Teil des Wegs zuständig und macht es dem Nachfolger gelegentlich schwerer als nötig. So ist es für das Recycling wichtig, dass Röhrenbildschirme nicht zerspringen, weil Vorder- und Rückglas getrennt recycelt werden müssen. Eine Eignung als Secondhand-Ware kann so schon während des Transports oder sogar beim Abholen eines Containers enden, da hier die Behälter oft sorglos umgefüllt werden. Am Recycling verdient der Spediteur ja schließlich nicht.

ElektroG, Anhang II, nach §7: „Das Symbol für die getrennte Sammlung von Elektro- und Elektronikgeräten stellt eine durchgestrichene Abfalltonne auf Rädern dar."

Problematisch ist also, dass nicht schon an der Sammelstelle konsequent auf Wiederverwendung geachtet wird. Am Ende der Kette ist es oft zu spät. So ist zwar die Recycling-Quote mit Einführung des ElektroG deutlich gestiegen, die *Reuse*-Quote aber sogar gesunken [4].

Die WEEE-Richtlinie und damit das ElektroG fordern lediglich eine *Sammel*quote, nämlich 4 kg Altgeräte pro Einwohner pro Jahr, ein Wert, der für jedes Land leicht erreichbar war. Dennoch wird nach Schätzung der EU-Kommission nur ein Drittel aller Geräte ordentlich entsorgt, da europaweit vermutlich durchschnittlich 15 kg anfallen [8].

Auch die viel gelobte Herstellerverantwortung zeigt in der Umsetzung mal wieder, dass Eigennutz nicht Gemeinnutz ist:

- Da jeder Hersteller auch die Geräte der anderen entsorgen muss (der Handyhersteller beispielsweise auch Drucker), sinkt die Motivation, die eigenen Geräte Recycling-freundlicher zu machen. Eine Rückkopplung auf die Gerätegestaltung „findet daher nach Aussage der Hersteller nicht statt" [3].

- Die Hersteller haben wenig Interesse an Wiederverwendung und Secondhand-Nutzung. Im Gesetz wird zwar gefordert, eine Wiederverwendung solle ermöglicht werden, eine Quote wird aber nicht gefordert. „Der Gesetzgeber hat die Verantwortung abgegeben." [3]

- Durch den Wettbewerbsdruck, den die Hersteller bei der Ausschreibung ausüben, gewinnt das billigste Transport- und Recyclingunternehmen. Die Bundesregierung kann sich zwar rühmen, dass mit dem ElektroG die Kosten deutlich gesunken seien [6]. Das führt aber zu Schrotttransporten quer durchs Land. Und in der Vergangenheit wurde mancher Preis vermutlich nur durch illegalen Export gehalten: ein Fall für *Basel*.

Basel Convention on the Control of Transboundary Movement of Hazardous Wastes and their Disposal

Das *Baseler Übereinkommen* legt fest, welche Abfälle (nicht nur WEEE) als gefährlich einzustufen sind, und verbietet deren Export in Länder, die nicht ausreichend damit umgehen können. Aus dem Übereinkommen und seiner gesetzlichen Umsetzung [10] folgt ganz klar: Elektroschrott (wie er heutzutage zusammengesetzt ist) darf die EU nicht verlassen. Nicht so eindeutig ist leider, wie Schrott definiert ist: Neugeräte gehören natürlich nicht dazu, auch funktionsfähige Secondhand-Ware darf als *Entwicklungshilfe* exportiert werden, allerdings auch ein *reparaturfähiges Produkt* – eine schwammige Formulierung, die viele Probleme bereitet. Die zollamtliche Kontrolle, ob in einem Schiffscontainer voll mit Computern und Monitoren alles benutzbar oder reparierbar ist, ist extrem aufwändig. Wenn man bedenkt, dass allein in Hamburg jährlich vermutlich 155 000 Tonnen Elektroschrott das Land und die EU-Grenzen verlassen [10], können nur stichprobenartige Prüfungen erwartet werden. Es kommt erschwerend hinzu, dass in den Containern die guten Geräte trickreich nach vorne gestellt werden, dass viele zweifelhafte Geräte wegen abgeschnittener (aber reparierbarer) Kabel nicht leicht testbar sind, und dass viele Kleingeräte in Secondhand-Exportautos versteckt werden [12]. Folge des Überwachungsproblems: Die Hälfte [7] oder sogar 75 % [9] aller Elektroexporte der EU sind vermutlich illegal. Der Export ist lukrativ. *Ökopol* schreibt in [10]:

> *„In den Empfängerstaaten werden funktionsfähige Geräte und Komponenten zu höheren Preisen gehandelt als dies in Deutschland der Fall wäre. Der Transport selber ist relativ preiswert."*

Konkreter wird die *Deutsche Umwelthilfe (DUH)* [12]:

> *„Nach DUH-Informationen kursieren in der Abfallszene Angebote der Exporteure, die beispielsweise für ausrangierte Computerbildschirme 50 ct bis 1 Euro bezahlen. Das ist für die angesprochenen Unternehmen lukrativ, denn für eine seriöse Entsorgung müssen die Unternehmen den Entsorgern normalerweise rund 4 Euro bezahlen – die Differenz für Hersteller und Entsorger beträgt also 4,50 bis 5,00 Euro pro Gerät."*

Zur Deklaration der Ware als Entwicklungshilfe resümiert das *Basel Action Network,* eine Nichtregierungsorganisation zur Beobachtung der Umsetzung des Baseler Übereinkommens:

> *„This new trade is not driven by altruism, but rather by the immense profits that can be made through it"* [9].

Die Reste der Resteverwertung inmitten der Ghanaischen Hauptstadt Accra. Im Volksmund heißt das Gebiet „Sodom und Gomorra". © 2009 Basel Action Network (BAN)

Der Export ist aber auch gefährlich. Auslöser für das Baseler Übereinkommen war 1988 das Auftauchen giftigen italienischen Mülls in Nigeria, der allmählich die dortige Deltagegend zerstörte. Italien hat den Müll wieder zurückgenommen [9]. Was heute jedoch mit Elektromüll geschieht, ist nicht weniger schlimm. Viele kleine Recycling-Unternehmen in Hinterhöfen der Entwicklungsländer schlachten importierten Elektroschrott aus, mit primitiven Mitteln und kaum vorhandenem Schutz vor giftigen Substanzen. Die Reste werden wild deponiert.

Blick in eine chinesische Recyclinghütte, in der Computerteile verbrannt werden, um die wertvollen Metallteile vom Rest zu trennen. © 2008 Basel Action Network (BAN)

Exportländer und Elektroaltgeräte-Abnehmer finden sich über die Welt verstreut. Indien war ein Schwerpunkt, hat aber inzwischen ausreichend eigenen Schrott. Europa führt vor allem nach Afrika aus; nach Nigeria steht nun Ghana im Fokus: Viele Fernseh- und Zeitungsberichte haben in jüngster Zeit die dortigen Zustände dokumentiert. Aus den U.S.A. kommen die Geräte vor allem nach China und benachbarten asiatischen Ländern. Anders als in der EU ist solcher Export in den U.S.A. legal, denn sie sind das einzige Industrieland, das das Abkommen nicht ratifiziert hat (neben Afghanistan und Haiti).

Fazit: Basel funktioniert nicht wirklich, denn die U.S.A. weigern sich und die EU kontrolliert nicht.

Was tun?

Die hier vorgestellten gesetzlichen Regelungen sind teilweise erfolgreich. Sie können verbessert werden, aber auch danach werden sie wohl weiterhin umgangen werden. Wir als Konsumenten sollten daher darauf achten, dass unsere Altgeräte den richtigen Weg nehmen.

Wie ich meinen alten Computer entsorge

Eine Aufrüstung geht nicht? Bekannte und Verwandte haben schon bessere Geräte? Eine Reparatur lohnt sich nicht mehr? Das Teil auf den Dachboden zu stellen, ist auf jeden Fall keine nachhaltige Lösung.

Trotz aller berichteten Probleme ist der einzig saubere Weg, den Computer zur kommunalen Sammelstelle zu bringen. Die Wahrscheinlichkeit einer ordentlichen Entsorgung ist hier am größten. Wenn Sie das Gerät verkaufen wollen, tun Sie es nur zu einem guten Preis. Bitte niemals als Schrott für ein paar Euro verkaufen oder gar an Unbekannte verschenken. Ein illegaler Export ist dann nahezu sicher. Fallen Sie daher nicht auf Schrotthändler rein, die oft direkt vor den Sammelstellen stehen. Stellen Sie Ihr Gerät auch nicht auf den Sperrmüll. Sie würden sich wundern, wie schnell es eingesammelt wird.

Wenn Sie erwägen, Geräte für einen guten Zweck zu spenden, lassen Sie sich nicht entmutigen: Das Angebot ist inzwischen riesig. Helfen kann hier vielleicht der Verein *ReUse Computer*, siehe http://www.reuse-computer.de/. Es gibt auch einige lokale Initiativen, in Hamburg beispielsweise *Mook Wat PC*, siehe http://www.pc.mookwat.de/. Als legale Entwicklungshilfe ist die Spende durchaus zweifelhaft. Sicherlich werden in Entwicklungsländern Computer benötigt, bedenken Sie aber, dass die danach anstehende Entsorgung ganz sicher nicht mehr sauber geschehen wird.

Vergessen Sie nicht, vorher Ihre Festplatte mit den persönlichen Daten auszubauen.

Wie ich mein altes Handy entsorge

Die meisten ungenutzten Handys dürften in unseren Schubladen liegen. Zum einen werden Handys meistens ausgemustert, obwohl sie noch funktionieren und einen Nutzwert haben. Zum anderen sind Handys so klein, dass das Recycling besonders schwierig und die Neigung besonders hoch ist, es einfach in den Müll zu werfen.

In den U.S.A., wo es kein national geregeltes Rücknahmesystem gibt und WEEE-Richtlinie, RoHS oder Basel keine Rolle spielen, entstehen private, stationäre Rücknahmesysteme: Das Handy wird in die Klappe gelegt, das Gerät scannt das Modell automatisch, behält es ein und druckt einen Gutschein aus oder spendet für einen guten Zweck. © 2011 ecoATM (www.ecoatm.com)

Sie können das Gerät natürlich versuchen zu verkaufen. Das macht oft Mühe für die paar Euro. Die wenigsten wissen aber, dass es Servicestellen dafür gibt:

- Unter http://www.deutschepost.de/electroreturn finden Sie eine kostenfreie Versandmarke, die Sie einfach auf einen Umschlag kleben, in den Sie das Handy stecken, und der dann in den Briefkasten kann. Kostet nichts und sichert eine sorgfältige Behandlung. Geld gibt es dafür nicht.

- Sie können das Handy auch einfach bei Ihrem Netzanbieter zurückgeben. In der Regel fragt der nicht weiter nach, ob man überhaupt Kunde sei, sondern nimmt das Gerät an sich. Geld fließt auch hier nicht.

- Über http://www.handysfuerdieumwelt.de/ bekommen Sie vielleicht sogar noch etwas zurück – der Versand funktioniert dann ähnlich. Auch http://www.zonzoo.de/ bietet ein ähnliches System. http://www.wirkaufens.de/index.php/verkaufen/1/Handys.html hilft Ihnen bei Ermittlung des Preises.

Vergessen Sie nicht, vorher Ihre SIM-Karte zu entfernen.

Was die Politik tun könnte

- Warum nicht ein Elektromüll-Pfand einführen? Warum nicht eine Altgeräte-Rücknahmepflicht beim Kauf eines neuen Geräts? Die derzeit diskutierte Novelle der WEEE-Richtlinie möchte aber lediglich die Sammelquote auf 65 % des produzierten Gesamtgewichts erhöhen [11]. Soweit in den Pressemitteilungen zu sehen, gibt es allerdings erste Überlegungen, eine Wiederverwendungs-Quote einzuführen.

- Die Verteilung der Verantwortung auf viele Akteure im deutschen ElektroG erzeugt zwar Wettbewerb, aber auch die beschriebenen Probleme. Die Sammel- und Recycling-Quoten beispielsweise in Schweden [3] zeigen, dass eine zentrale Koordination nachhaltiger wirkt.

- Bezüglich des illegalen Exports gibt es Vorschläge, mit den Entwicklungsländern zu kooperieren. Der Gedanke des *Best of two worlds*-Ansatzes: Die in den Industrieländern gesammelten Altgeräte werden in die Entwicklungsländer transportiert, wo die Arbeitskosten für das Ausschlachten der Geräte am geringsten und der Nutzen der aussortierten Secondhand-Geräte am größten ist. Der Rest-Elektromüll geht dann wieder zurück zu uns, in die spezialisierten Recyclingfabriken [15].

Und vielleicht sollten wir Informatiker uns fragen: Warum brauchen wir ständig neue, leistungsfähigere Computer? Warum verlangt unsere Software immer mehr von der Hardware? Warum gelingt uns kein überzeugendes Hardware-Design, so dass die Anwender immer gleich das ganze Gerät austauschen wollen, um mit der Entwicklung mitzuhalten?

Literatur

[1] Solving the E-Waste Problem Initiative: "StEP Annual Report 2010". April 2011

[2] United Nations University: "2008 Review of Directive 2002/96 on WEEE. Final Report". August 2007

[3] Eva Leonhardt: „Geregelte Verantwortungslosigkeit? Erfahrungen mit der Produktverantwortung bei Eletro(nik)-Geräten aus Sicht eines Umwelt- und Verbraucherschutzverbandes". Deutsche Umwelthilfe Juni 2007

[4] Moritz Schröder: „Was einmal im Container landet, ist nicht mehr brauchbar". tageszeitung vom 24.3.2010

[5] Knut Sander u.a.: "The Producer Responsibility Principle of the WEEE Directive. Final Report". Ökopol / iiiee / RPA August 2007

[6] Antwort der Bundesregierung auf die kleine Anfrage 16/3276 „Defizite der Elektroaltgeräteverordnung". Deutscher Bundestag, 16. Wahlperiode, Drucksache 16/3552

[7] Soenke Zehle, Lotte Arndt, Sarah Bormann: „Unsichtbare Kosten. Ungleiche Verteilung ökologischer Risiken in der globalen Computerindustrie". Weltwirtschaft Ökologie & Entwicklung e.V. (WEED e.V.), Bonn August 2007

[8] Sara Nordbrand: "Out of Control: E-waste trade flows from the EU to developing countries". SwedWatch April 2009

[9] Jim Puckett u.a.: "The Digital Dump. Exporting Re-use and Abuse to Africa". The Basel Action Network, Seattle Oktober 2005

[10] Knut Sander, Stephanie Schilling: „Optimierung der Steuerung und Kontrolle grenzüberschreitender Stoffströme bei Elektroaltgeräten / Elektroschrott". Umweltbundesamt Texte 11/2010

[11] Aktuelle Informationen zum Stand der WEEE-Novelle finden Sie unter: http://ec.europa.eu/environment/waste/weee/index_en.htm (geprüft am 28.7.2011)

[12] Deutsche Umwelthilfe: „Deutschland ist Exportweltmeister – auch dank Elektroschrott!" Pressemitteilung 20.6.2007

[13] Cornelia Heidenreich: „IT-Industrie muss mehr tun als lediglich Strom sparen". FIfF-Kommunikation 3/2009, S.43f.

[14] Sebastian Jekutsch: „Bad Apple". FIfF-Kommunikation 2/2011, S.29f.

[15] Christian Wölbert: „Neue Wege für E-Schrott. Kooperationen mit Entwicklungsländern sollen das Entsorgungsproblem lösen." c't 26/2010, S.75f.

Sebastian Jekutsch

Sebastian Jekutsch lebt in Hamburg, arbeitet in der Softwarequalitätssicherung, ist Mitautor der neuen FIfF-Broschüre zur elektronischen Gesundheitskarte und beschäftigt sich als FIfF-Mitglied vor allem mit dem Thema *Faire Computer*.
Kontakt: *sj@fiff.de*

Stefan Hügel

95/46/EG – die EU-Datenschutzrichtlinie

1994 fand in Bremen die Jahrestagung zum 10jährigen Bestehen des FIfF statt: „1984 plus 10 – Realität und Utopien der Informatik". Die *Zeit* schrieb damals: „Es gibt sie tatsächlich in Deutschland: kritische Informatiker, die sich gegen blinde Technikbegeisterung wehren und sich über die Auswirkung ihrer Arbeit Gedanken machen."[1]

„Im Mittelpunkt der Tagung stand die Frage: Welche Utopien und Visionen in den Bereichen Arbeit und Alltag, Staat und Umwelt haben in der Vergangenheit bei der Entwicklung der Informatik eine entscheidende Rolle gespielt, welche bestimmen Gegenwart und Zukunft? Schon vor zehn Jahren gehörten zu den brisanten Themen die innige Verflechtung der Informatik mit der Rüstung, die Automatisierung der Arbeit, der „gläserne" Mensch, die weltweite Vernetzung, die Fehleranfälligkeit informationsverarbeitender Systeme und die Verantwortung der Computerfachleute", so hieß es in der Pressemitteilung. Wichtiges Thema war dabei – damals wie heute – der Datenschutz.

Schon vor der Tagung hatte Thilo Weichert – damals Vorsitzender der DVD – eine kritische Bilanz aus 10 Jahren deutschem Datenschutzrecht gezogen: „10 Jahre Grundrecht auf Datenschutz – kein Grund zum Feiern".[2] Gleichzeitig stand 1994 die Verabschiedung der noch heute gültigen EU-Datenschutzrichtlinie 95/46/EG unmittelbar bevor.

Diese war dann auch Thema auf der Tagung. *Stefan Walz*, damals Datenschutzbeauftragter Bremens, stellte die geplante Richtlinie in seinem Beitrag dar. Er ging dabei auf die Geschichte des Datenschutzes in Europa, beginnend mit der Konvention des Europarats: dem *Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten*. Davon ausgehend beschrieb er die Regelungsziele der Richtlinie, insbesondere auch im Hinblick auf den grenzüberschreitenden, möglichst freien und ungehinderten Informationsverkehr und die Vermeidung eines datenschutzrechtlichen „Flickenteppichs". Dabei waren Unterschiede in den Datenschutzkonzeptionen der einzelnen Mitgliedsstaaten zu überwinden – insbesondere den Abweichungen des Richtlinienentwurfs vom deutschen Datenschutzmodell war ein Abschnitt gewidmet.

Wir drucken im Folgenden den damaligen Beitrag von Stefan Walz ab. Aktuell steht bekanntlich eine Überarbeitung der Richtlinie an – an der öffentlichen Konsultation Anfang des Jahres hatte sich auch das FIfF beteiligt.[3] Möge der Blick in die Vergangenheit wertvolle Hinweise für die Gestaltungsaufgaben der Zukunft geben.

Originalquelle

Stefan Walz (1995): Datenschutz in Europa. Die Datenschutzrichtlinie der Europäischen Union, in: Hans-Jörg Kreowski, Thomas Risse, Andreas Spillner, Ralf E. Streibl, Karin Vosseberg (Hg.): Realität und Utopien der Informatik, Münster: agenda Verlag, 120-127

Wir danken dem Autor herzlich für die Genehmigung zum Nachdruck.

Anmerkungen

1 *Dieter Brehde: 1984 und zehn Jahre. Die Zeit Nr. 43, 21.10.1994, http://www.zeit.de/1994/43/1984-und-zehn-jahre (Abruf 21.08.2011)*

2 *Thilo Weichert: 10 Jahre Grundrecht auf Datenschutz – kein Grund zum Feiern. FIfF-Kommunikation 3/1994, 31-34*

3 *FIfF e.V.: Novellierung der Datenschutzrichtlinie. Stellungnahme zur EU-Konsultation. FIfF-Kommunikation 1/2011, 5-10*

Stefan Walz

Retrospektive

Datenschutz in Europa

Die Datenschutzrichtlinie der Europäischen Union

1 Gemeinsamer Standpunkt verabschiedet: Durchbruch für die Harmonisierung

Für die Harmonisierung des Datenschutzrechts der Mitgliedstaaten in der Europäischen Union ist zu Anfang dieses Jahres der hoffentlich entscheidende Durchbruch erzielt worden. Viereinhalb Jahre sind seit der Vorlage des ersten Richtlinienentwurfs der EU-Kommission im September 1990 vergangen, bis im Februar 1995 der so genannte *„Gemeinsame Standpunkt" des EU-Ministerrats zum Geänderten Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* vom 15.10.1992 (ABl EG, Nr. C 311, S. 30 ff.) verabschiedet werden konnte.

2 Das erste europäische Konzept: Die Datenschutz-Konvention des Europarats

Die Diskussion konzentrierte sich in den letzten Jahren in erster Linie auf den *Richtlinienvorschlag der EG-Kommission* (s.o. 1). Doch muss, wer über Datenschutz auf europäischer Ebene spricht, mit der *Konvention des Europarates von 1981* beginnen. Das „Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten" versuchte erstmals, für den Bereich der Mitgliedstaaten des Europarates ein Mindestmaß an einheitlichem Datenschutz zu schaffen. Die Regelungsziele des Übereinkommens waren denen des heutigen EG-Richtlinienvorschlags durchaus vergleichbar: Die

Harmonisierung des Datenschutzstandards im Bereich des Europarates sollte zur Konsequenz haben, dass der grenzüberschreitende Verkehr personenbezogener Daten – von bestimmten Ausnahmen abgesehen – nicht mehr beschränkt werden können sollte. In den Erwägungsgründen der Richtlinie wird an mehreren Stellen auf die Bedeutung der Vorarbeiten des Europarates und die Parallelität der grundlegenden Zielsetzung hingewiesen, gleichzeitig aber deutlich gemacht, dass die EG im Hinblick auf den materiellen Datenschutzstandard deutlich über die Konvention von 1981 hinausgehen will.

Das Regelungswerk des Europarats ist im Laufe der vergangenen Dekade durch zahlreiche bereichsspezifische Empfehlungen verfeinert und präzisiert worden; sie betreffen u.a. medizinische Datenbanken, Personalinformationssysteme, die Direktwerbung und die Datenverarbeitung durch die Polizei. In den letzten drei Jahren, d.h. seit dem Systemwechsel in den osteuropäischen Staaten, hat die Europarats-Konvention dort eine vorher nicht erwartete neue Bedeutung erhalten. Der Anschluss an die westliche Wertegemeinschaft vollzieht sich in einer Reihe von Staaten des früheren „Ostblocks" über die Unterzeichnung bzw. Ratifikation von Vereinbarungen des Europarats. Dies gilt insbesondere für die Menschenrechts- und die Datenschutzkonvention, die beide aufgrund ihres Inhaltes besonders geeignet sind, die Abkehr vom früheren stalinistischen Regime zu symbolisieren.

3 Die Regelungsziele der Richtlinie: Gemeinschaftsweiter Schutz des Persönlichkeitsrechts und Freiheit des grenzüberschreitenden Datenverkehrs

Ausgangspunkt für die Initiative der Kommission war zunächst die Erkenntnis, dass der für 1993 angestrebte Binnenmarkt einen grenzüberschreitenden, möglichst freien und ungehinderten Informationsverkehr auch und gerade mit personenbezogenen Daten braucht. Einzelne Fälle des Verbots von Datenexporten aus Mitgliedstaaten der EG in Partnerländer ohne Datenschutzgesetzgebung (etwa der bekannte „Fiat-Fall" in Frankreich) hatten das Risiko eines „Flickenteppichs" unterschiedlicher nationaler Datenschutzgesetzgebungen – neben Staaten ohne jede eigene Regelung – deutlich gemacht.

Anders ausgedrückt: Die Konzeption des EG-Binnenmarktes als (auch) „informationeller Großraum" hat eine Harmonisierung der Regelungen über den Umgang mit personenbezogenen Daten im Zusammenhang mit dem Waren-, Dienstleistungs- und Kapitalverkehr zur zwingenden Voraussetzung. Es ist vor allem den vielfältigen Bemühungen der Datenschutzbeauftragten und -kommissionen in den EG-Ländern zu verdanken, dass dieser auf die kommerziellen Aspekte der EG-Integration konzentrierten Sichtweise die Dimension der Grundrechtssicherung hinzugefügt wurde. Die EG-Kommission erkannte die Notwendigkeit des europaweiten Schutzes des Persönlichkeitsrechts und der Privatsphäre vor den Risiken der immer umfassender betriebenen Datenverarbeitung, nicht zuletzt auch dafür, die soziale Akzeptanz ihrer Vorschläge zu erhöhen.

Wenn, schlagwortartig formuliert, dem informationellen Großraum ein „Grundrechts-Großraum" entsprechen soll, darf sich der gleichwertige Schutz der personenbezogenen Daten auch nicht auf ein Mindestlevel beschränken, vielmehr muss er zwingend auf einem hohen Niveau hergestellt werden. Die Gleichwertigkeit des Schutzniveaus wiederum verhindert, dass „Datenoasen" entstehen oder bestehen bleiben, die zu Wettbewerbsverzerrungen führen könnten. Noch einmal: Freier Informationsverkehr und harmonisierter Schutz personenbezogener Daten auf hohem Niveau bilden die beiden Grundintentionen des Richtlinienvorschlages.

Harmonisierung heißt dabei, dass vorhandene Rechtssysteme angeglichen werden und Mitgliedstaaten ohne Datenschutz-Legislation verpflichtet werden, ein der Richtlinie entsprechendes nationales Gesetz zu erlassen. Die Richtlinie hat dabei, vergleichbar dem deutschen Bundesdatenschutzgesetz (BDSG), die Funktion eines Rahmens, der durch bereichsspezifische Verordnungen und Richtlinien ausgefüllt werden kann. Für die ISDN-Problematik hat ja die Kommission – zusammen mit dem Vorschlag zur Harmonisierung – einen speziellen Richtlinien-Entwurf vorgelegt.

4 Vom 1. Entwurf zum Geänderten Vorschlag

Die Beratung der Richtlinie in den verschiedenen EG-Gremien benötigte im ersten Durchgang zwei Jahre und verlief mühevoll und kontrovers. Entscheidende Bedeutung für die Änderungen im zweiten Kommissionsvorschlag gegenüber dem ersten, im September 1990 vorgelegten Text waren in erster Linie die Debatten und Beschlüsse des Europäischen Parlaments. Beigetragen haben aber auch die Stellungnahmen der Konferenz der Datenschutzbeauftragten und -kommissionen in der EG. Einflussreiche Lobbygruppen haben sich intensiv um Korrekturen in ihrem Sinne bemüht und damit teilweise auch Erfolg gehabt.

5 Systemdivergenz als Hauptproblem

Hauptproblem für eine schnelle Verständigung auf EG-Ebene waren die prinzipiellen Divergenzen der in den Mitgliedstaaten vorhandenen Datenschutzkonzeptionen. Diese Unterschiede machen die Schwierigkeit der Aufgabe deutlich, die die Kommission zu bewältigen hatte und hat, um eine inhaltliche Angleichung zu erzielen. Nur wenn man diese Systemdifferenzen kennt und akzeptiert, dass ein Rechtsinstrument der EG Bestandteile verschiedener Rechtsordnungen integrieren muss, um in den Mitgliedstaaten akzeptiert zu werden, ist eine faire und gleichzeitig realistische Beurteilung des neuen Textvorschlages möglich.

Da gibt es den Unterschied zwischen Lizensierungsmodellen, also Rechtsordnungen, die die Einrichtung und Nutzung von Datenverarbeitung von der Genehmigung durch eine Kontrollinstitution abhängig machen (z.B. Frankreich, Großbritannien), und dem deutschen Konzept der genehmigungsfreien Verarbeitungserlaubnis, wenn die Zulässigkeitsvoraussetzungen des Datenschutzrechts eingehalten sind. Stärker legalistisch orientierten Systemen, die nur staatlichem Recht effiziente Schutzqualität zubilligen, stehen Staaten gegenüber, die die Regelung des Umgangs mit personenbezogenen Daten mehr der Selbstregulierung durch die betroffenen Verbände und Interessengruppen

überlassen wollen (z. B. die Niederlande). Die Datenschutzinstitutionen sind in mehreren Mitgliedstaaten strikt auf Funktionen hoheitlicher Genehmigungen und Kontrolle beschränkt, während im deutschen Modell das Element der Hilfestellung und Beratung der datenverarbeitenden Stellen im Vordergrund steht. Während mancherorts, z. B. in Frankreich, sensitive Datenkategorien benannt werden, die einem Sonderschutz unterstehen, folgt die Datenschutzdoktrin in Deutschland spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts der These, dass die Schutzwürdigkeit personenbezogener Angaben ausschließlich vom Verwendungskontext abhängt. Während das Datenschutzrecht hierzulande das höhere Eingriffsrisiko eher dem öffentlichen Bereich zubilligt, also im Verhältnis zwischen Staat und Bürger sieht, sind es anderswo in erster Linie die privaten Datenverarbeiter, denen die Verarbeitungsrestriktionen gelten.

6 Abweichungen vom deutschen Datenschutzmodell

Der Richtlinienvorschlag weist nach wie vor, d. h. auch in der Fassung des Gemeinsamen Standpunkts (s.o. 1), in mehreren Bereichen Abweichungen vom BDSG bzw. generell vom deutschen Datenschutzkonzept auf, d. h. Regelungen, in denen – aus deutscher Sicht – systematische „Fremdkörper" auftauchen bzw. interpretationsbedürftige Anleihen bei ausländischen Rechtsordnungen gemacht wurden. Dazu nur wenige Beispiele:

Konstruktiv abweichend aus deutscher Sicht ist Art. 7, der die Voraussetzungen für die *Zulässigkeit der Datenverarbeitung* für den öffentlichen und den nicht-öffentlichen Bereich gemeinsam regelt. Dies entspricht dem Wunsch des Europäischen Parlaments und auch der Mehrheit der EG-Datenschutzkonferenz. Die nach den Bereichen Verwaltung und Wirtschaft differenzierenden Zulässigkeitskataloge des ursprünglichen Richtlinienvorschlags wurden zu sehr allgemein formulierten Generalklauseln zusammengeschmolzen. Würde man den Text dieses Artikels wörtlich ins BDSG übernehmen – was aber nicht zwingend geboten ist –, würde der Verarbeitungsrahmen zumindest für öffentliche Stellen erheblich ausgeweitet. Anders als im ursprünglichen Text finden sich im geänderten Vorschlag auch keine speziellen Bestimmungen mehr über erlaubte Zweckänderungen und die Zulässigkeitsbedingungen für Übermittlungen. Anders ausgedrückt: Im Vergleich mit dem Urtext hat sich die neue Richtlinien-Version noch stärker von der Systematik des deutschen Datenschutzrechts entfernt.

Für *sensitive Daten* – Art. 8 zählt dazu Angaben über die rassische und ethnische Herkunft, die politische Meinung, die religiöse, philosophische oder moralische Überzeugung, die Gewerkschaftszugehörigkeit oder die Gesundheit – stellt die Richtlinie ein grundsätzliches Verarbeitungsverbot auf, das allerdings unter einer Reihe von Voraussetzungen aufgehoben werden kann. Im deutschen Regelungskontext wären möglicherweise als Konsequenz dieser für unser Recht neuen Regel-Ausnahme-Systematik eine Reihe spezieller gesetzlicher Erlaubnisse zu schaffen.

Weniger dramatisch als vorher befürchtet wird sich nach dem Text des Gemeinsamen Standpunkts die grundsätzlich statuierte *Meldepflicht* für alle automatisierten Dateien, also auch für die der privaten datenverarbeitenden Stellen, zu einem von der Datenschutz-Kontrollbehörde zu führenden Register darstellen (Art. 18). Mit dem Prinzip einer umfassenden Registrierung folgte die Kommission dem Beispiel einer ganzen Reihe nationaler Rechte: Die vorherige Anmeldung und Überprüfung bzw. sogar Genehmigung von Dateien bildet den Eckpfeiler des Datenschutzsystems u.a. in Frankreich, Großbritannien und in den Niederlanden. Allerdings wird der zunächst erwartete Zuwachs an Bürokratisierung für die deutschen Unternehmen dadurch stark abgemildert, dass anstelle der Registermeldepflicht die Bestellung eines internen Datenschutzbeauftragten treten kann, der ein ebenfalls internes Dateiverzeichnis führt. Insoweit wurde auch dem Wunsch der deutschen Aufsichtsbehörden entsprochen, in der Richtlinie alternativ das BDSG-Modell (§§ 36, 37 BDSG) vorzusehen, um jedenfalls im deutschen Rechtsraum den Aufbau einer neuen Registerbürokratie, die keine entsprechende Effektivierung der Kontrolle erwarten lässt, zu vermeiden.

In den Beratungen der EG-Gremien und in den Interventionen verschiedener Lobbygruppen – nicht zuletzt aus den USA – wurde die Regelung der Zulässigkeitsvoraussetzungen für die *Weitergabe personenbezogener Daten in Drittstaaten* (Art. 25, 26) besonders intensiv diskutiert und kritisiert. Für Zielländer, die nicht Mitglied der EG sind und die kein angemessenes Schutzniveau, also insbesondere keine Datenschutzgesetzgebung aufweisen, geht die Richtlinie von einem grundsätzlichen Verbot des Datenexports aus. Diesem Prinzip steht ein abschließender Katalog von Ausnahmen gegenüber, wozu insbesondere der Fall gehört, dass die Übermittlung von Daten in einen Drittstaat ohne Datenschutzrecht zur Erfüllung eines Vertrages (z. B. eines Reisevertrages) notwendig ist. Als Ausnahme lässt die Richtlinie auch die viel diskutierte „Vertragslösung" zu, also die Absicherung der Einhaltung des Datenschutzrechts des Exportstaates durch einen Vertrag zwischen der übermittelnden Stelle und dem ausländischen Empfänger. § 17 BDSG, der die Datenübermittlung durch Bundesbehörden an Stellen außerhalb des Geltungsbereichs des BDSG normiert, müsste bei Inkrafttreten der Richtlinie entsprechend neu gefasst bzw. präzisiert werden; für die grenzüberschreitende Weitergabe durch nicht-öffentliche Stellen müsste eine entsprechende Bestimmung neu geschaffen werden.

7 Akzeptanz der Rechtsangleichung

Der an ausgewählten Divergenzbeispielen gezogene Vergleich von Konzeption und Regelungsinhalten des Richtlinien-Vorschlags einerseits und des deutschen Datenschutzrechts andererseits darf nicht missverstanden werden. Es wäre ein verfehlter Ansatz, aus der einzelstaatlichen Perspektive die Vorstellungen der Gemeinschaft ängstlich daraufhin abzuprüfen, inwieweit sie vom eigenen Recht abweichen, und dann alle Bemühungen daran zu setzen, im weiteren Beratungsverfahren noch so viel wie möglich von dem in Deutschland bestehenden Regelungsmodell „zu retten". Eine *integrationsfreundliche Sichtweise* muss die von unseren EG-Partnern entwickelten Lösungsmodelle zur Kenntnis nehmen, sich um deren Verständnis bemühen und sich auf den Versuch einlassen, gemeinsame Grundstrukturen herauszudestillieren und bewährte Elemente von unseren Nachbarstaaten zu übernehmen. Dies gilt auch dann, wenn das soeben reformierte BDSG oder die jüngeren Landesdatenschutzgesetze erneut novelliert werden müssten. Diese Konsequenz ergibt sich

keineswegs nur im Bereich des Datenschutzes; die parallele Problematik stellt sich bei vielen anderen auf Harmonisierung angelegten Initiativen der Kommission, zuletzt vor allem im Bereich des Umweltschutzes.

Die Akzeptanz der Richtlinie im deutschen Rechtsraum ist dadurch ganz entscheidend erhöht worden, dass im Laufe der Beratungen wichtige Kernforderungen der deutschen Delegation durch Ausnahmeregelungen im Text des Gemeinsamen Standpunkts oder Klarstellungen bzw. Interpretationen in den teilweise neu formulierten Erwägungsgründen erfüllt worden sind. So wird der *betriebliche Datenschutzbeauftragte* weder abgeschafft noch bleibt er auch nur unerwähnt, was vielfach fälschlich gleichgesetzt wurde. Vielmehr wird er in Art. 18 Abs. 2 ausdrücklich anerkannt. Explizit richtlinienkonform ist aufgrund Art. 28 Abs. 1 auch das deutsche *duale Kontrollmodell* mit separaten Überwachungsbehörden für die öffentliche Verwaltung (Datenschutzbeauftragte des Bundes und der Länder) und die Wirtschaft (Aufsichtsbehörden für den nicht-öffentlichen Bereich). Die Existenz eines Spielraums für bereichsspezifische Regelungen, also für die Weiterentwicklung des Datenschutzes über den Stand des Inkrafttretens der Richtlinie hinaus, wird jetzt ausdrücklich im Erwägungsgrund Nr. 9 erwähnt.

8 Konsequenzen und weiteres Verfahren

Mit Inkrafttreten der Richtlinie wird es in allen EU-Ländern die Gebote der rechtmäßigen Datenerhebung und der Zweckbindung der Datenverarbeitung, den Sonderschutz für besonders sensible Daten, die Rechte des Bürgers auf Auskunft, Berichtigung und Löschung sowie externe unabhängige Kontrollinstanzen geben, alles Kernpunkte auch der deutschen Datenschutzgesetzgebung in Bund und Ländern. Doch steht diese Erfolgsmeldung unter Vorbehalt: Um überhaupt den Konsens der Mehrzahl der Regierungen zu erreichen, findet sich im „Gemeinsamen Standpunkt" eine Reihe vage formulierter Generalklauseln; außerdem mussten zahlreiche Sonderwünsche einzelner EU-Staaten mit Ausnahmebestimmungen erfüllt werden. Dazu nur zwei Beispiele: Die Richtlinie beschränkt ihren Anwendungsbereich und damit die Harmonisierungswirkung auf die Datenverarbeitung in und aus „Dateien" (Art. 3 Abs. 1). Damit bezieht sie im wesentlichen nur den automatisierten, nicht den manuellen Umgang mit persönlichen Angaben ein, eine Regelungssituation, die in Deutschland nur noch für die Privatwirtschaft, jedoch nicht mehr für die öffentliche Verwaltung gilt. Nicht durchsetzen ließ sich auch die in Deutschland inzwischen selbstverständliche völlige Kostenfreiheit der Auskunft an den Betroffenen (vgl. stattdessen Art. 12 Nr. 1: „ohne ... übermäßige Kosten").

Der Richtlinienentwurf geht jetzt zur 2. Lesung ins Europäische Parlament, die bis Juni 1995 abgeschlossen sein könnte, sodann ein weiteres Mal in den Ministerrat. Mit dem Inkrafttreten, dessen genauer Zeitpunkt noch nicht prognostiziert werden kann, beginnt eine dreijährige Übergangsfrist, innerhalb derer die Mitgliedstaaten die Richtlinie in ihr nationales Recht umsetzen müssen.

Für die bereichsspezifische Gesetzgebung in Deutschland kommt es maßgeblich auf die zur Wirkung der Richtlinie lange diskutierte Alternative zwischen Sperrwirkung oder Mindeststandard an. Es geht dabei um die Frage, ob die Richtlinie über ihr Schutzniveau hinausgehende Bestimmungen verhindert oder auch nach ihrem Inkrafttreten die Befugnis der Mitgliedstaaten bestehen bleibt, für Teilbereiche von Verwaltung und Wirtschaft – also z. B. im Arbeits- und Sozialrecht – im Vergleich zum allgemeinen Datenschutzrecht strengere Normen zu erlassen. Der neu formulierte Erwägungsgrund Nr. 9 des Entwurfs spricht insoweit von einem „Spielraum" für Verbesserungen, der allerdings nur „im Rahmen der Durchführung der Richtlinie" ausgefüllt werden kann.

Die Datenschutzgesetze von Bund und Ländern werden aufgrund der Richtlinie voraussichtlich nur in wenigen Punkten geändert werden müssen, etwa bei den Meldepflichten für Dateien. Eine detaillierte Analyse des Änderungsbedarfs für das deutsche Recht kann sinnvollerweise und verbindlich erst dann vorgenommen werden, wenn der Text nach dem Gesetzgebungsverfahren durch die Organe der Europäischen Union (s.o.) feststeht. Die dafür notwendigen Vorarbeiten erfolgen im Rahmen der EU-Datenschutzkonferenz sowie der deutschen Datenschutzkonferenz und ihres EU-Arbeitskreises.

9 Zusammenarbeit der Datenschutzinstitutionen in der Europäischen Union

Vor allem die europaweite Diskussion über den Richtlinienentwurf und seine mühselige Beratung in den EG-Organen haben den inzwischen bis auf zwei in allen Mitgliedstaaten eingerichteten unabhängigen Datenschutz-Kontrollinstitutionen deutlich gemacht, wie wichtig verstärkte Kooperation und intensivierter Meinungsaustausch sind. Seit 1993 haben mehrere Konferenzen und Arbeitsgruppensitzungen auf EG-Ebene stattgefunden. Dass hier Erfolge möglich sind, zeigt die Forderung nach Lockerung der ausschließlichen Anknüpfung des anwendbaren Rechts an den Sitz der speichernden Stelle, die auch im Geänderten Vorschlag der Kommission von 1992 noch unberücksichtigt geblieben war. Im Gemeinsamen Standpunkt wurde dieser Kritik, die auch von mehreren nationalen Delegationen in der

Stefan Walz

Dr. **Stefan Walz** war zum Zeitpunkt der Veröffentlichung dieses Artikels Datenschutzbeauftragter der Freien Hansestadt Bremen. Er ist heute Leiter des Referats III B 4 (Patent- und Erfinderrecht) im Bundesministerium der Justiz.

EU-Ministerratsarbeitsgruppe vorgetragen worden war, Rechnung getragen: Maßgebliches Kriterium ist nicht mehr der Ort, an dem die speichernde Stelle, d. h. z. B. die Unternehmenszentrale, „ansässig" ist, was tendenziell zur grenzüberschreitend einheitlichen Anwendung eines einzigen nationalen Rechts, d. h. auch auf die Filialen in anderen Staaten der Union, geführt hätte. Vielmehr gilt nach dem neuen Art. 4 Abs. 1a) für jede Niederlassung eines Unternehmens das jeweils im „Gastland" anzuwendende einzelstaatliche Recht.

Zum Themenkreis Datenschutz in der EU-Telekommunikationspolitik und -legislation haben die europäischen Datenschützer einen ständigen Arbeitskreis eingesetzt, der unter der Leitung des Berliner Datenschutzbeauftragten steht. Dieses Gremium hat inzwischen auftragsgemäß Ende 1994 eine gemeinsame Stellungnahme zu dem Geänderten Vorschlag für die ISDN-Richtlinie erarbeitet und der Kommission zugeleitet. In einer Entschließung hat die Konferenz in Madrid im Mai 1994 ihre Sorge darüber geäußert, dass die EU mit Nachdruck die Einrichtung gemeinschaftsweiter Telekommunikationsnetze und –dienste betreibt, ohne dass vorher die allgemeine Datenschutz- und/oder die ISDN-Richtlinie in Kraft getreten wären. Die Konferenz forderte daher die zuständigen EG-Gremien auf, unaufschiebbare Rechtsinstrumente in diesem Bereich dann jedenfalls mit speziellen Datenschutznormen auszustatten. Weitere Tagesordnungspunkte der Zusammenkünfte auf EU-Ebene waren und sind u.a. der Ausbaustand und die erfolgten bzw. zukünftig notwendigen Kontrollaktivitäten bei den innergemeinschaftlichen Datensystemen (u.a. EUROPOL, Zollinformationssystem) sowie beim Schengener Informationssystem.

Diese vergleichsweise lockere Kooperation der Datenschutzbehörden in der EU wird sich nach Inkrafttreten der Richtlinie zu einer Institution verfestigen. Nach Art. 29 und 30 der Richtlinie ist eine unabhängige „Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten" einzusetzen, die sowohl die bei der Umsetzung des Gemeinschaftsrechts in einzelstaatliche Vorschriften auftauchenden Fragen prüft als auch die Kommission bei allen geplanten Rechtsakten oder Maßnahmen im Datenschutzbereich berät.

Viola Bräuer

Behind the Screen

Filmpremiere in Salzburg,12. August 2011

Ein tanzender Junge auf dem Elektronikschrottplatz in Ghana – Endstation für Computer, Drucker, Monitore, Kabel, die hier verbrannt werden.

Der Film „Behind the Screen – Das Leben meines Computers" von Stefan Baumgartner, Sandra Heberling und Simon Fraissler, StudentInnen des Masterstudienganges MultiMediaArt der FH Salzburg, dokumentiert den Lebensweg von Elektronik – von der Rohstoffgewinnung bis zur Verschrottung.

Gold ist einer der für die Fertigung von Hardware benötigten Rohstoffe. Goldminen in Ghana vergiften das Trinkwasser und missbrauchen einstige Ackerflächen als Abraumhalden. Versprochene Ausgleichzahlungen an die lokale Bevölkerung bleiben leere Versprechungen oder sind zu gering, um Ausgleich zu sein. Ghanaer, die selbst Gold fördern, tun dies illegal.

Die Herstellung von Hardware ist monotone Fliessbandarbeit. Sie erfolgt in Billiglohnländern, zu denen auch Tschechien zählt. Via Leiharbeitsfirmen kommen noch billigere Arbeitskräfte aus Rumänien und der Mongolei nach. Je schwieriger es ist, auf dem heimischen Arbeitsmarkt einen Job zu finden, desto weniger Rechte erwarten die Menschen. Der Zug immer billigerer Arbeitskräfte erschwert eine starke Gewerkschaft und damit geregelte Arbeitszeiten und -löhne.

Der Film zeigt auch Hardware, die im Namen der Anbindung der dritten Welt an den technischen Fortschritt nach Ghana verschifft wird. Die meisten Geräte sind kaputt und einige Computer sind mit Aufklebern versehen, die diese als Eigentum bestimmter Regierungen mit vertraulichen Daten ausweisen. Hier haben Datenschutz, Schutz von vertraulichen Daten und Umweltschutz im Team versagt.

Den FilmemacherInnen aus Österreich ist es gelungen, sachlich zu dokumentieren. Die Interviews mit Wirtschaftswissenschaftlern, Vertretern der Gewerkschaften und Umweltaktivisten sind durchweg aufklärend und beschreibend. Kameraführung und Schnitt pragmatisch, ohne Effekthascherei oder Sentimentalitäten. Es ist die Stärke des Films, dass er nur berichtet. Er hinterlässt Fragen zum Selber-Denken.

Dabei ist mir aufgefallen, dass fast nur Männer interviewt wurden. Aus meiner eigenen Erfahrung in Ghana und den europäischen Ostblockstaaten weiß ich, dass es von wesentlicher Bedeutung ist, Frauen zu interviewen, gerade wenn es um wirtschaftliche Themen geht. Das ist einer der kulturellen Unterschiede.

Die Absicht des Regisseurs Stefan Baumgartner – das eigene Konsumverhalten kritisch zu hinterfragen – wird erreicht, obwohl die eigentliche Computernutzung im Film sehr einseitig

dargestellt wird. Es ist eben nicht nur der Lifestyle einer Generation, es ist vor allem die Abhängigkeit einer technisch hochentwickelten *ersten* Welt von Energie, Rohstoffen, Technik. Mensch stelle sich spaßeshalber eine mittlere deutsche Großstadt drei Tage ohne Strom, Benzin und Kaffee vor.

Es ist das komplexe System, das es zu verstehen gilt, und da gibt es wenig Unterschied zwischen dem Goldgräber, der in einem Doppelbett allein schläft und aus lauter Fürsorge für seinen kleinen Bruder diesem eine Isomatte vermacht, und den auf Gewinn orientierten Konzernen.

Der eigentliche Unterschied besteht zwischen dem Ärger am PC und dem tanzenden Jungen auf der Müllkippe.

Der Film wurde u.a. gefördert durch das FIfF.

Michael Prinzinger

Internetzugang für Flüchtlinge

Das Passauer Bündnis für die Rechte der Flüchtlinge braucht Ihre/Deine Hilfe, um Flüchtlingen in und um Passau zu einem Internet-Zugang zu verhelfen

Informationen und Kommunikation waren schon immer überlebenswichtig. Das ist es, was uns Menschen ausmacht. „Informationen und Ideen mit allen Verständigungsmitteln ohne Rücksicht auf Grenzen zu beschaffen, empfangen und zu verbreiten"[1] ist ein menschliches Grundbedürfnis und daher ein Menschenrecht.

Mit geliebten Menschen im Ausland kommunizieren und neue Sprachen lernen, Zug- und Buspläne herausfinden, sich über seine grundlegenden Rechte informieren: Das Internet macht heutzutage all dies einfacher. Ob wir es wollen oder nicht, es wird immer schwerer, diese Grundbedürfnisse ohne das Internet zu erfüllen.

Über zweihundert Flüchtlinge in Passau und Umgebung sind durch Gesetze, die ihre Bewegungsfreiheit einschränken, Gefangene in den überfüllten Flüchtlingslagern, in denen sie gezwungen sind zu leben. Der Zugang zu Arbeit und Sprachkursen, und damit auch zur Gesellschaft, wird ihnen grundsätzlich verweigert.

Nach einer Reise von Tausenden von Kilometern, auf der Suche nach Sicherheit und Zuflucht, finden sie sich in einem System wieder, dass darauf ausgerichtet ist, sie dazu zu bringen, das Land wieder zu verlassen. Das Bayerische Gesetz hat seine Zielsetzung deutlich festgeschrieben: „die Bereitschaft [von Flüchtlingen] zur Rückkehr in das Heimatland fördern" [2].

Wenn sie nicht abgeschoben werden, müssen Familien mit Kindern zwei bis drei Jahre warten, bis sie aus dem Lager ausziehen dürfen. Die Wartezeit für Alleinstehende beträgt meist sechs bis sieben Jahre. Internetzugang kann ein Fenster zur Außenwelt öffnen und Flüchtlingen helfen, in dieser Zeit des Wartens ihre eigenen Grundrechte zu erfahren und zu sichern. Der Zugang zu Information kann Flüchtlingen dazu verhelfen, während der Zeit der Gefangenschaft ein selbstbestimmteres und unabhängigeres Leben zu führen.

Bitte unterstützen Sie/unterstütze das Passauer Bündnis darin, Internetzugang für Flüchtlinge zur Verfügung zu stellen! Helfen Sie/hilf den lokalen Flüchtlingen, Zugang zu Unabhängigkeit und Grundrechten zu bekommen! Unsere Arbeit für Flüchtlinge ist unbezahlt und Internet kostet immer noch Geld [3]. Daher bitten wir Dich/Sie um finanzielle Unterstützung für dieses Projekt. Konto-Inhaber: Z.A.K.K. e.V., Sparkasse Passau, Konto-Nr.: 240 298 596, BLZ: 740 500 00

Bitte unbedingt als Betreff: **„Internet ins Lager"** angeben.

Vielen Dank.

[1] Allgemeine Erklärung der Menschenrechte (Artikel 19)
[2] Bayerische Asyldurchführungsverordnung (DV Asyl) vom 04.06.2002
[3] Flüchtlingsarbeit ist nicht umsonst und (genauso wie eine Internetverbindung auch!) schon gar nicht kostenlos. Deshalb freuen wir uns über Spenden.

Michael Prinzinger hat letztes Jahr den zweiten Platz des FIfF-Studienpreises für seine Diplomarbeit über das Phantomprotokoll bekommen. Wegen seines Aufenthalts in Neuseeland konnte er leider nicht zur Preisverleihung kommen, ist aber nun wieder in Deutschland und hilft bei einer Passauer Flüchtlingshilfegruppe.

Sie hatte die tolle Idee, Internet in die fünf Flüchtlingslager in und um Passau zu bringen. Die Flüchtlinge dort leben ziemlich abgeschottet und isoliert, so dass ein Internetzugang ihr Leben sehr bereichern würde. Sie haben bereits die Erlaubnis der bayrischen Regierung und von der TU München gespendete Computer erhalten. Ein Verein in München würde rechtlich für die Internetnutzung haften. Was noch fehlt sind *Internetpaten*, die die Kosten für eine Internet-Flat für ein Lager und Jahr übernehmen würden. Eine typische monatliche Internet-Flat kostet ca. 30 Euro, der Jahresbetrag wäre also 360 Euro. Einen Sponsor haben sie schon gewonnen und suchen noch vier.

Michael Prinzinger fragt, ob das FIfF einmalig Pate eines der Lager werden könnte, und – wenn unsere finanzielle Situation das momentan nicht zulässt –, ob unsere Mitglieder das Projekt fördern wollen. Es können sich natürlich auch mehrere Menschen eine Patenschaft teilen. Spendenbescheinigungen kann die Initiative ausstellen.

FIfF e.V.

Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

Das FIfF-Büro

Geschäftsstelle FIfF e.V.
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail:fiff@fiff.de

Die aktuellen Bürozeiten entnehmen Sie bitte unseren Webseiten.

Bankverbindung:
Sparda Bank Hannover eG
Spendenkonto: 800 927 929
BLZ 250 905 00
IBAN: DE66 2509 0500 0800 9279 29
BIC: GENODEF1S09

FIfF im Netz

Das ganze FIfF:
www.fiff.de

FIfF-Mailingliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/fiff-L
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-Mitgliederliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/mitglieder
Beiträge an: *mitglieder@lists.fiff.de*

Mailingliste Videoüberwachung:
An- und Abmeldung unter
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

Beirat

Michael Ahlmann (Bremen); **Peter Bittner** (Köln); **Dagmar Boedicker** (München)**; Prof. Dr. Wolfgang Coy** (Berlin); **Prof. Dr. Wolfgang Däubler** (Bremen); **Prof. Dr. Leonie Dreschler-Fischer** (Hamburg), **Prof. Dr. Christiane Floyd** (Hamburg); **Prof. Dr. Klaus Fuchs-Kittowski** (Berlin); **Prof. Dr. Michael Grütz** (Konstanz); **Prof. Dr. Thomas Herrmann** (Dortmund); **Prof. Dr. Wolfgang Hesse** (Marburg); **Dr. Eva Hornecker** (Glasgow/UK); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Klaus Köhler** (München); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Klaus-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppburg); **Prof. Dr. Frieder Nake** (Bremen); **Prof. Dr. Rolf Oberliesen** (Bremen); **Prof. Dr. Arno Rolf** (Hamburg); **Prof. Dr. Alexander Rossnagel** (Kassel); **Prof. Dr. Gerhard Sagerer** (Bielefeld); **Prof. Dr. Gabriele Schade** (Erfurt); **Prof. Dr. Dirk Siefkes** (Berlin); **Prof. Dr. Marie-Theres Tinnefeld** (München); **Dr. Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

- **Stefan Hügel (Vorsitzender)** – Frankfurt am Main
- **Jens Rinne (stellv. Vorsitzender)** – Mannheim
- **Carsten Büttemeier** – Bremen
- **Sylvia Johnigk** – München
- **Prof. Dr. Hans-Jörg Kreowski** – Bremen
- **Prof. Dr. Dietrich Meyer-Ebrecht** – Aachen
- **Kai Nothdurft** – München
- **Raffael Rittmeier** – Bremen
- **Prof. Dr. Britta Schinzel** – Freiburg
- **Julia Stoll** – Grenzach-Wyhlen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	**1.200 Stück**
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Carsten Büttemeier, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Jens-Holger Streck,
Schwerpunktredaktion	Stefan Hügel, Sylvia Johnigk
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert@mtsf.de.* Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	The Espace Léopold photo by Lydia González Dios
Druck	Meiners Druck, Bremen

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

FIfF-Jahrestagung 2011

„Dialektik der Informationssicherheit – Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit"
11. – 13.11.2011 in München

FIfF-Vorstandssitzung

13. November 2011 in München (im Rahmen der Jahrestagung)

FIfF-Kommunikation

4/2011 »Killerroboter&Co«
Hans-Jörg Kreowski u.a.
(Redaktionsschluss: 27.10.2011)

1/2012 »Dialektik der Informationssicherheit«
Sylvia Johnigk, Kai Nothdurft u.a.
(Redaktionsschluss: 03.02.2012)

2/2012 »Verfassungsbeschwerden«
Jens Rinne, Raffael Rittmeier u.a.
(Redaktionsschluss: 04.05.2012)

3/2012 »Visualisierung«
Britta Schinzel u.a.

4/2012 »Enquête-Kommission „Internet und digitale Gesellschaft«
Stefan Hügel u.a.

W&F – Wissenschaft & Frieden:

3/11 – Soldaten im Einsatz

4/11 – Demokratie im Arabischen Raum

DANA – Datenschutz-Nachrichten:

2/11 – Datenschutzprobleme moderner Technik

3/11 – Online-Spiele

4/11 – Datenschutz im Bildungswesen

Das FIfF-Büro

Geschäftsstelle FIfF e.V.
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de

Wichtiger Hinweis: Postvertriebsstücke wie die FIfF-Kommunikation werden von der Post auch auf Antrag nicht nachgesandt; daher bitten wir alle Mitglieder und Abonnenten, dem FIfF-Büro jede Adressänderung rechtzeitig bekannt zu geben!

Schluss FIfF

„It's just a hype …" – html wurde 20!

„Das Internet ist eine Spielerei für Computerfreaks, wir sehen darin keine Zukunft", verkündete Ron Sommer, damals Telekom-Chef, vollmundig 1990. In der Tat war das Internet zu jener Zeit lediglich ein Netz von Datenleitungen zwischen Rechenzentren – allerdings bereits weltweit: Zwischen den Großrechnern und in den lokalen Rechner-Netzwerken konnte man Dateien transferieren, auf die Terminalebene entfernter Rechner zugreifen oder E-Mails und Newsgroup-Postings im Zeileneditor verfassen. Mit den Protokollen ftp, telnet und mailto war die notwendige Standardisierung geschaffen worden. Mit anlogen Telefonmodems – über so genannte Akustikkoppler, wo rigide Vorschriften der Telefongesellschaften noch jede elektrische Veränderung am Telefonanschluss untersagten – gab es erste zaghafte Ansätze einer flächendeckenden Ausbreitung des Internets.

Den Startschuss für eine neue Dimension der Internet-Nutzung setzte der Physiker Tim Berners-Lee, damals Wissenschaftler am CERN, vor nun genau 20 Jahren: Am 6. August 1991 enthüllte er in einem Posting an die Newsgroup alt.hypertext seine Epoche machende Entwicklungen, die *hypertext mark-up language* (html) für die Codierung von Internetseiten und das *hypertext transport protocol* (http) für ihre Übertragung im Internet. Er eröffnete damit dem Internet eine neue Ära, die Ära des *world wide web*, des weltweiten ‚Verwebens' von Dokumenten. Trefflicher als mit den ersten beiden Sätzen auf seiner erste html-Seite (siehe Screenshot) kann man die Möglichkeiten, die Berners-Lee mit html und http geschaffen hat, nicht formulieren.

Auf der erste Website http://info.cern.ch, auf der Berners-Lee diese Seite 1991 ins Netz stellte, finden wir diese primitiv anmutende Seite heute nicht mehr. Auch ist der Begriff world wide web etwas aus der Mode gekommen, wiewohl das Acronym www noch vielfach Prefix der Internetadressen von html-Servern ist. Das world wide web ist das ‚Web' geworden. Oder einfach ‚das' Internet – in einer deutlich anderen Bedeutung als vor 20 Jahren: Mit seiner enormen Schubkraft auf die Hardware- und Softwareentwicklung. Mit seinen nützlichen und angenehmen Seiten für die Wissenschaft, für die Wirtschaft und für den privaten Nutzer. Und mit seinem Missbrauchspotential.

„It's just a hype", beschied Bill Gates noch 1995. Und hätte Berners-Lee nicht umsichtig und vorausschauend auf alle Urheberrechte verzichtet und sich für einen offenen Standard eingesetzt, hätte er vermutlich recht behalten, und wir hätten heute konkurrierende, inkompatible Standards von Microsoft, Apple und Google. Und – ob es dann Google und andere Suchmachinen überhaupt schon gäbe? *Who knows …* Ob unter den „ungefähr 12.600" Treffern, die Google unter meinem Namen ausspuckt, nicht so einige sind, die ich nicht so gerne gefunden haben wollte – darüber brauchte ich mir dann wenigstens keine Sorgen zu machen ;-) dme

Zitate aus Frankfurter Rundschau, 06./07.08.2011, S. 30; Links der Screeshots ebd.

```
From: timbl@info .cern.ch (Tim Berners-Lee)
Newsgroups: alt.hypertext
Subject: WorldWideWeb: Summary
Keywords: heterogeneous hypertext, web, source, protocol, index, information retrieval
Message-ID: <6487@cernvax.cern.ch>
Date: 6 Aug 91 16:00:12 GMT
References: <6484@cernvax.cern.ch>
Sender: n...@cernvax.cern.ch
Lines: 84

In article <6...@cernvax.cern.ch> I promised to post a short summary  of the
WorldWideWeb project.  Mail me with any queries.

                WorldWideWeb - Executive Summary


The WWW project merges the techniques of information retrieval and hypertext to
make an easy but powerful global information system.

The project started with the philosophy that much academic information should
be freely available to anyone. It aims to allow information sharing within
internationally dispersed teams, and the dissemination of information by
support groups.
```

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.