H 7625

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

28. Jahrgang 2011 Einzelpreis: 7 EUR

1/2011 – März 2011

ISSN 0938-3476

• Datenschutz und Anonymität • Rüstungskontrolle • Rechtsstaat und Demokratie •

FIfF Kommunikation

Titelbild: Eine Wordle-Verarbeitung von »213.251.145.96/About.html« / Ralf E. Streibl

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Inhalt

Ausgabe 1/2011

inhalt

Schwerpunkt »WikiLeaks«

Aktuelles

FIfF e.V.

Studienpreis

Retrospektive

Rubriken

Editorial

Zwei Themen, mit denen sich auch die FIfF-Kommunikation bereits beschäftigt hatte, haben in den letzten Wochen viel Aufsehen erregt. Gerade musste ~~*Bundesverteidigungsminister Dr. Karl-Theodor zu Guttenberg*~~ zurücktreten – wegen eines mutmaßlichen Verstoßes gegen Immaterialgüterrechte. Und zuvor wurde eine Internet-Plattform weltweit heiß diskutiert: *Wikileaks*, das sich spätestens mit dem Video *Collateral Murder* und der Veröffentlichung der US-Botschaftsdepeschen nachdrücklich in das Bewusstsein der Öffentlichkeit gebracht hat. Beide Ereignisse und ihre Folgen sind natürlich auch bei uns ein Thema.

Die Debatte um zu Guttenberg wurde zu großen Teilen im Netz geführt. Mit Hilfe der Wiki-Plattform *GuttenPlag* wurde seine Dissertation akribisch untersucht – und eine Reihe von Passagen entdeckt, bei denen offenbar abgeschrieben wurde, angefangen bei der Einleitung. Dabei hat die Diskussion viele Facetten – die schon genannten Immaterialgüterrechte, die Frage nach wissenschaftlicher Redlichkeit, die Frage nach der Glaubwürdigkeit von Politikern und die Frage nach konservativen Werten. *Ralf E. Streibl* setzt sich in seinem Beitrag mit Aspekten der Affäre Guttenberg auseinander.

Zu Wikileaks gab es heftige Diskussionen. Neben der Debatte um die Rechtmäßigkeit der Veröffentlichungen – bis hin zum Vorwurf des Verrats – mussten die beteiligten Medien mit rund 250.000 einzelnen Meldungen angemessen umgehen. *Christiane Schulzki-Haddouti* berichtet in zwei Beiträgen vom Datenjournalismus – der journalistischen Aufarbeitung der US-Botschaftsdepeschen: *(Alp-)Traum Wikileaks* und *Datenberge und Nachhaltigkeit*. In einem weiteren Beitrag – *Anonyme Depots* – befasst sie sich mit Alternativen zu Wikileaks.

Forderungen vor allem konservativer Politiker, Wikileaks und seine Betreiber mit aller Härte zu verfolgen, und die – möglicherweise auf politischen Druck erfolgte – Sperrung von Konten und Serverkapazitäten lassen Zweifel an der demokratischen Einstellung so mancher Verantwortlicher aufkommen. Eine Reihe von Publikationen, Organisationen und Einzelpersonen haben auf Initiative der *taz* gegen die Kriminalisierung von Wikileaks Stellung bezogen und einen Appell formuliert – gegen die Angriffe auf Wikileaks, für Publikationsfreiheit und Kontrolle des Staats. Auch das FIfF hat den Appell unterzeichnet; wir dokumentieren ihn in diesem Heft.

Gleichzeitig sind mehrere Bücher zu Wikileaks erschienen – von der journalistischen Aufarbeitung über einen Insiderbericht zur Betrachtung der Folgen. *Stefan Hügel* hat sich die Bücher angesehen – und kommentiert zusätzlich einleitend die Reaktionen der Öffentlichkeit.

Eine Grundfrage hinter Wikileaks ist die Frage, wie wir mit Informationen umgehen und damit unsere Demokratie gestalten. Doch auch andere Artikel in diesem Heft betreffen direkt die Gestaltung unseres demokratischen Gemeinwesens: *Rolf Gössner* wurde fast 40 Jahre vom Verfassungsschutz beobachtet – bis das Verwaltungsgericht in Köln feststellte, dass die Überwachung durchgängig rechtswidrig war. Er selbst berichtet in seinem Beitrag *Rechtsstaatswidrige Dauerüberwachung* davon. Die Planung und Durchsetzung öffentlicher Großprojekte – und den Umgang mit Bürgerprotesten – beleuchtet unser Beiratsmitglied *Wolfgang Hesse* anhand der Ereignisse um *Stuttgart 21* und des diesbezüglichen Schlichtungsverfahren – wir meinen: „Oben bleiben!“

Das originäre Thema des FIfF ist der Frieden – auch in diesem Heft: *Jürgen Altmann* fordert eine Rüstungskontrolle für Roboter, und in der Retrospektive blicken wir auf einen Beitrag zurück, den *Manfred Domke* bereits vor 20 Jahren veröffentlicht hat: *Dual Use – Berücksichtigung militärischer Anforderungen bei der zivilen Entwicklung neuer Technologien*. Ein Thema, das nichts an Aktualität verloren hat.

Die *Volkszählung 2011* haben wir bereits im letzten Heft behandelt – ein Thema, das in der Öffentlichkeit noch viel zu wenig Beachtung findet. Über die letzten Entwicklungen berichtet die Anwältin *Eva Dworschak*. Und wer schon immer wissen wollte, wie große Organisationen mit Social-Media-Plattformen wie *Twitter* umgehen, wird vielleicht in dem lesenswerten Beitrag von *Gregor Koall* eine Antwort finden.

Ein Höhepunkt des FIfF-Jahres ist die Jahrestagung. Doch müssen wir die Leserinnen und Leser vertrösten, die in dieser Ausgabe die angekündigten Beiträge von der Jahrestagung 2010 in Köln erwartet haben. Aus Aktualitäts- und redaktionellen Gründen müssen wir die Beiträge leider verschieben. Sie erscheinen in der nächsten Ausgabe. Versprochen!

Dafür sind zwei Ergebnisse einer besonders erfreulichen Episode der Jahrestagung 2010 in diesem Heft enthalten: Nachdem schon in der letzten FIfF Kommunikation zwei Beiträge von Preisträgern des FIfF-Studienpreises veröffentlicht wurden, folgen nun die anderen beiden: *Phillip W. Brunst*, der mit dem ersten Preis ausgezeichnet wurde, und *Jens Jacobi*, der einen zweiten Preis erhalten hat, fassen die Inhalte ihrer Arbeiten für unsere Leserinnen und Leser zusammen. Wir nutzen die Gelegenheit, zur Einreichung von Beiträgen für den diesjährigen FIfF-Studienpreis aufzurufen.

Nicht zuletzt plant die EU-Kommission eine Novelle der Datenschutz-Richtlinie 95/46/EG zum Datenschutz. Wir haben uns an der öffentlichen Konsultation beteiligt – unsere Stellungnahme findet sich ebenfalls in dieser Ausgabe.

In Summe enthält das Heft eine bunte Mischung von Beiträgen – viele davon mit stark aktuellem Bezug. Wir wünschen auch dieses Mal eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Stefan Hügel und Ralf E. Streibl
für die Redaktion

Brief an das FIfF

Von konservativen Werten

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

„Ich möchte in den nächsten Jahren von der CDU/CSU kein Wort mehr über Werte hören." *Michael Spreng*, der das in seinem (empfehlenswerten) Blog *Sprengsatz* schreibt, ist nicht irgendwer. Unter anderem war er 2002 der Wahlkampfmanager des damaligen Kanzlerkandidaten Edmund Stoiber. Was veranlasst ihn zu einem solchen Statement?

~~Dr.~~ zu Guttenberg, natürlich. Auffallend schnell wurde ihm sein Doktortitel von der Universität Bayreuth entzogen – weil wissenschaftliche Standards nicht eingehalten worden seien. „Fehlende Fußnoten" – früher hieß so etwas mal „abschreiben". Zuvor hatte er bereits selbst vorsorglich seinen Verzicht erklärt. Interessant wäre jetzt noch zu wissen, wie es passieren konnte, dass eine Promotion, bei der nach so kurzer Prüfung offenbar bereits solche Mängel festgestellt wurden, zunächst mit *summa cum laude* bewertet wurde.

Zu Guttenbergs Beliebtheit tat das erst einmal keinen Abbruch. Nicht zuletzt dank einer massiven Kampagne in der Boulevardpresse schien seine Zustimmung in der Bevölkerung ungebrochen. Auch seine Parteifreunde standen mit deutlich überwiegender Mehrheit zu ihm. Law-and-Order-Politiker, die sonst schnell nach Bestrafung und Verschärfung der Gesetze rufen, haben ihn verteidigt – auch mit dem Hinweis, dass es ja schließlich Wichtigeres gäbe, als ein paar fehlende Fußnoten in einer Doktorarbeit. Nebenbei wird dazu auch noch der tragische Tod dreier Soldaten in Afghanistan instrumentalisiert. Wird sich ein kleiner Ladendieb künftig darauf berufen können: Alles nicht so schlimm; schließlich werden an anderer Stelle Menschen umgebracht?

Letztlich musste zu Guttenberg dennoch zurücktreten. Doch eins hat die Debatte wieder überdeutlich gezeigt: die „konservativen Werte"(TM) gelten meist nur für die anderen.

Erinnert sich noch jemand daran, wie gefährlich das Weihnachten war, das wir letztes Jahr erlebt haben? Im November trat Innenminister de Maizière mit sorgenumwölkter Miene vor die Kameras und gab eine Terrorwarnung heraus: Besonders große Menschenansammlungen – wie bei Weihnachtsmärkten – seien gefährdet.

Nun kann es sicher nie ausgeschlossen werden, dass ein Terroranschlag, auch in Deutschland, stattfindet. Das Manöver wirkte aber sehr durchsichtig: Die Terrorwarnung wurde wenige Tage vor der Innenministerkonferenz herausgegeben, und der Ruf der bekannten innenpolitischen Hardliner nach der Vorratsdatenspeicherung und weiteren Verschärfungen ließ dann auch nicht lange auf sich warten.

Die Bevölkerung reagierte dennoch besonnen auf die Panikmache aus Berlin. Es gab keine menschenleeren Weihnachtsmärkte. Und was die demonstrativ zur Schau getragene Polizeipräsenz gegen einen tatsächlichen Anschlag hätte ausrichten können, sei einmal dahingestellt. Wie zuverlässig der damalige Informant war, ist wohl inzwischen auch nicht mehr ganz klar.

Dennoch scheint die Debatte um die Vorratsdatenspeicherung langsam zu kippen. Nachdem zunächst der Bundesdatenschutzbeauftrage *Peter Schaar* sich für eine „*Vorratsdatenspeicherung light*" (aka „*Quick freeze plus*") ausgesprochen hat, scheint nun auch Justizministerin *Sabine Leutheusser-Schnarrenberger* die Seiten zu wechseln. Offensichtlich zeitigen die gebetsmühlenartig vorgetragenen Forderungen der Protagonisten Wirkung. Inzwischen gibt es sogar Befürworter an Stellen, an denen man sie überhaupt nicht erwartet hätte. Nochmal zum Mitschreiben: Die Datenspeicherung an sich ist das Problem, nicht ihre Dauer! Schön, dass eine Veröffentlichung von *Malte Spitz* nochmals deutlich vor Augen geführt hat, welch erheblichen Einbruch in die Privatsphäre die Vorratsdatenspeicherung bedeutet.

Erfreulich dagegen, dass der Versuch von EU-Innenkommissarin *Cecilia Malmström*, Netzsperren per Richtlinie europaweit durchzusetzen, zumindest vorläufig gescheitert ist. Die engagierte Arbeit von EDRi – *European Digital Rights* – hat sich gelohnt.

Der letzte Aufreger der vergangenen Wochen: Wikileaks. Einige Veröffentlichungen haben womöglich mehr enthüllt als beabsichtigt: So mancher Politiker – hauptsächlich in den USA – ließ die rechtsstaatliche Maske fallen und forderte die Todesstrafe für einzelne Beteiligte. Vor allem Konservative taten sich hier hervor, womit wir wieder bei den Werten angelangt wären. In die Diskussion mischen sich die Trennung mehrerer Aktiver von Wikileaks, die Vorwürfe gegen *Julian Assange* und die Äußerungen Beteiligter in der Presse, bei denen Außenstehende kaum mehr zwischen sachlich berechtigter Kritik und dem Austragen von Rivalitäten unterscheiden können. Der Boulevard kommt dabei zumindest auf seine Kosten. Wichtiger ist jedoch, was der frühere US-Botschafter *John C. Kornblum* auf den Punkt bringt: Wikileaks habe „der Öffentlichkeit dramatisch vor Augen geführt …, wie radikal und mit welchen Folgen sich unser Umgang mit Informationen zu Beginn des 21. Jahrhunderts verändert." Dieser Aspekt sollte trotz persönlicher Rivalitäten nicht untergehen.

Was passiert einstweilen im FIfF? Im Januar haben wir eine Stellungnahme zur geplanten Novelle der EU-Datenschutzrichtline abgegeben – nachzulesen in diesem Heft. Auf dem *Chaos Communication Congress* waren wir präsent: mit einem Stand und einem Vortrag zu INDECT, gehalten von *Sylvia Johnigk*.

Gleichzeitig laufen bereits wieder die Vorbereitungen auf die nächste Jahrestagung, die im November in München stattfinden wird. Auch unseren Studienpreis werden wir dabei wieder verleihen – wenn Ihr in den letzten zwei Jahren eine (Abschluss-)arbeit geschrieben habt, die Ihr einreichen wollt, seid Ihr bis 31. Mai 2011 herzlich dazu eingeladen. Beiträge von zwei Preisträgern des letzten Jahres sind in diesem Heft nachzulesen.

Mit fiffigen Grüßen

Stefan Hügel

FIfF e.V.

Novellierung der Datenschutz-Richtlinie

Stellungnahme zur EU-Konsultation

In ihrer Mitteilung COM(2010) 609 vom 4. November 2010 kündigt die europäische Kommission an, die aus dem Jahr 1995 stammende Datenschutz-Richtlinie 95/46/EG zu novellieren und lädt dazu ein, im Rahmen einer Konsultation Vorschläge dazu einzureichen. Dieser Text ist die leicht redaktionell überarbeitete Fassung unserer Stellungnahme.

Als Hauptziele nennt die Kommission:

1. *Stärkung der Rechte der einzelnen Bürgerinnen und Bürger,*
2. *Verbesserung des Binnenmarktes,*
3. *Revision der Datenschutzbestimmungen bei der Zusammenarbeit von Justiz und Polizei bei der Strafverfolgung,*
4. *Berücksichtigen der globalen Dimension des Datenschutzes,*
5. *Verstärken der Institutionen, um Datenschutz besser durchzusetzen.*

Wir begrüßen die Initiative zur Novellierung der Richtlinie. Zu einzelnen Aspekten des Datenschutzes nehmen wir im Folgenden Stellung und ersuchen die Kommission, die genannten Punkte bei der Novellierung zu berücksichtigen. Zusätzlich verweisen wir auf die Stellungnahme der DVD – Deutsche Vereinigung für Datenschutz e.V. –, die wir ebenfalls unterstützen.

Stärkung der Rechte der einzelnen Bürgerinnen und Bürger

Herstellung von Transparenz durch explizites Einverständnis zur Datenweitergabe – Opt-in statt Opt-out

Heutige Regelungen sehen in einer Reihe von Fällen vor, dass Einzelne der Weitergabe ihrer personenbezogenen Daten aktiv widersprechen müssen, wenn sie sie ablehnen (z.B. beim Listenprivileg). Liegt kein Widerspruch vor, ist die Datenweitergabe in solchen Fällen zulässig. Damit dürfen Daten auch ohne das Wissen der Betroffenen weitergegeben werden. Dies lehnen wir ab. Das FIfF fordert, grundsätzlich das explizite Einverständnis der Betroffenen zur Voraussetzung der Datenweitergabe zu machen. Das Listenprivileg ist abzuschaffen.

Damit die Datenweitergabe transparent wird, sind Dritte explizit zu benennen, Empfänger müssen sich die Zustimmung bestätigen lassen: Eine Weitergabe durch den für die Verarbeitung Verantwortlichen an Dritte soll zukünftig nur noch mit expliziter Zustimmung des Betroffenen erlaubt sein. Die Dritten müssen von den Verantwortlichen dazu soweit möglich explizit benannt werden, mindestens aber für die Zustimmung so weit spezifiziert werden, dass Betroffene die Dritten mit zumutbarem Aufwand identifizieren können, damit sie auch diesen gegenüber bei Bedarf ihre Rechte auf Auskunft, Löschung oder Berichtigung durchsetzen oder die Einwilligung zu einem späteren Zeitpunkt widerrufen können. Der Empfänger (Dritte) muss gleichzeitig angemessen verifizieren, dass die Einwilligung tatsächlich vorliegt, um die Daten weiterverarbeiten zu dürfen. Dies könnte beispielsweise durch Anfrage bei Betroffenen oder Anfordern einer regelmäßigen Zertifizierung (Datenschutzaudit) der übermittelnden Stelle erfolgen.

Begründung:

Sofern bisher überhaupt eine rechtskonforme Zustimmung für die Weitergabe eingeholt wird, werden oft in den vorformulierten Einwilligungserklärungen Dritte als Empfänger so pauschal benannt, dass Betroffene diese Dritten nicht oder nur mit unverhältnismäßig hohem Aufwand identifizieren können. Zudem kann ein Betroffener eine missbräuchliche Weitergabe der verantwortlichen Stelle nur schwer nachweisen, wenn die zulässigen Empfänger nicht genau genug spezifiziert sind.

Wenn die Zustimmungserklärung schwammig formuliert und nicht klar definiert ist, dass es sich um Missbrauch handelt, wenn die Daten auch ohne Zustimmung weitergegeben werden, dann kann der Empfänger leichter behaupten, dass eine Zustimmung und damit eine legale Übermittlung vorliegt, auch wenn dies aus Sicht des Betroffenen gar nicht der Fall ist.

Handelt es sich bei der verantwortlichen Stelle um eine Privatperson, die z.B. Daten von Bekannten weiter gibt, so kann die entsprechende Rechtskenntnis nur in den seltensten Fällen vorausgesetzt werden. In einem solchen Fall darf die empfangende Stelle nicht mehr pauschal von einer legalen Weitergabe ausgehen. Ein Beispiel sind die Upload-Funktionen von persönlichen Adressbüchern bei der Anmeldung an sozialen Netzwerken, die den Benutzer geradezu verleiten, illegal Daten von Bekannten an die Be-

treiber weiterzugeben. Hier ist eine Bringschuld für Unternehmen erforderlich, die Auftragsdatenverarbeitung oder Erhebung von Daten Dritter durchführen. Diese sind dafür verantwortlich, sich davon zu überzeugen, dass die Einwilligung tatsächlich vorliegt.

Einwilligung zur Datenspeicherung im Internet

Sofern die Zustimmung zu einer Speicherung von über das Internet übermittelter Daten nicht unmittelbar (innerhalb von 7 Tagen) erteilt wird, müssen die Daten ohne vorherige Weiterverarbeitung wieder gelöscht werden.

Für die Erstregistrierung für Internet-Dienste muss das Closed-Loop-Verfahren verpflichtend werden. Im Gegensatz zum einstufigen Opt-in Verfahren wird bei diesem Verfahren zweistufig verfahren. Benutzer müssen im ersten Schritt angeben, welche Daten sie z.B. zur Registrierung bei einer Web-Anwendung oder Mailingliste speichern möchten. In der Folge bekommen sie eine Bestätigungsmail an die angegebene Adresse, die neben den Daten, die gespeichert werden, einen Bestätigungslink enthält. Klickt der Nutzer diesen Link an, so wird der Nutzer auf eine Web-Seite geführt. Dort kann er Richtigkeit seiner Daten überprüfen und mittels eines Buttons bestätigen, dass er mit der Speicherung seiner Daten wirklich einverstanden ist.

Mit diesem zweistufigen Verfahren wird erschwert, dass ein Nutzer wissentlich oder unwissentlich falsche Angaben macht, und dadurch eine andere Person anmeldet, die nicht möchte, dass ihre Daten und ihre E-Mail-Adresse in dieser Liste gespeichert werden. Sobald sie die E-Mail erhält, mit der sie aufgefordert wird, dem Link zu folgen, kann sie durch einfaches Ignorieren der E-Mail verhindern, dass ihre Daten dauerhaft gespeichert werden. Der Anbieter der Anwendung ist verpflichtet, die Daten wieder zu löschen. Der Nutzer erfährt zum einen, dass jemand versucht hat, seine Daten bei einem Anbieter zu speichern, und muss zum anderen nicht umständlich erklären, dass er oder sie der Speicherung widerspricht.

Begründung:

Bei einer Erstregistrierung kann die zustimmende Person nicht eindeutig identifiziert werden. Deswegen lässt sich bei einstufigem Opt-out nicht verifizieren, dass die Zustimmung tatsächlich von der registrierten Person stammt. Das Closed-Loop-Verfahren stellt diese Identität sicher.

Profilbildung über Menschen verhindern

Im Internet verbreitete Daten betreffen die Privatsphäre der Bürger und lassen das Erstellen umfangreicher Persönlichkeitsprofile zu. Sie müssen daher stark geschützt werden. Dies betrifft sowohl die Nutz- als auch die Bewegungsdaten.

Begründung:

Die Zusammenführung von Daten ermöglicht zusätzliche Einblicke in die Privatsphäre der Bürger. Daher soll datenschutzrechtlich dafür gesorgt werden, dass auch für jemanden, der legal Zugriff auf mehrere Datenbanken hat, daraus nicht das Recht auf Zusammenführung der Daten folgt.

Befristete Einwilligung zur Datenspeicherung und -weitergabe

Der Betroffene gibt seine Einwilligung nur befristet, eine Verlängerung erfordert eine aktive Erneuerung der Einwilligung.

Begründung:

Die Häufigkeit der Fälle, in denen personenbezogene Daten verarbeitet werden, führt dazu, dass Betroffene schnell den Überblick verlieren können, wem sie Daten über sich selbst gegeben haben, und erst recht, an wen diese ggf. weiter gegeben wurden. Zudem wirden häufig „vergessen“ Daten zu löschen, wenn der ursprüngliche Zweck der Verarbeitung nicht mehr besteht, und zwar sowohl von der verantwortlichen Stelle als auch vom Betroffenen selbst, der der verantwortlichen Stelle vergisst mitzuteilen, dass etwas zu löschen ist oder dies wegen des Aufwands unterlässt. Die Einwilligung zur Datenspeicherung und Weitergabe sollte daher stets befristet sein, zumindest aber grundsätzlich bei der Einwilligung durch den Betroffenen befristet werden können.

Dies wäre ein wichtiger Schritt in Richtung des aktuell diskutierten „digitalen Radiergummis“ für das Internet. Nach Ablauf einer vorgegebenen Frist verfällt das Einverständnis, und Daten sind zu löschen, wenn nicht explizit eine Verlängerung gewährt wird.

Besonderes Augenmerk ist auf den Kinderschutz zu richten. Informationen, die von Minderjährigen angegeben wurden, müssen grundsätzlich gelöscht werden können, wenn sie selbst oder Erziehungsberechtigte dies einfordern.

Information über Datenweitergabe und deren Adressaten – Auskunftsrecht stärken

Betroffene sind stets unaufgefordert zu informieren, ob, wann und an wen ihre Daten weitergegeben wurden („Datenbrief“). Dies gilt sowohl für den primären als auch für sekundäre Verwender der Daten. Die Information hat zu angemessenen Zeitpunkten (mindestens einmal pro Jahr) in angemessener Weise zu erfolgen und muss selbst datenschutzkonform durchgeführt werden. Durch geeignete Verfahren ist sicherzustellen, dass sensible Daten durch den Datenbrief nicht in falsche Hände geraten.

Das Auskunftsrecht auf Anforderung des Betroffenen bleibt unberührt. Es muss grundsätzlich das Recht auf Auskunft in der eigenen Sprache bestehen.

Um unnötigen Aufwand für Erstellung und Versand der Datenbriefe zu vermeiden, sollte ein Opt-out ermöglicht werden, durch den die Bürger auf die Zusendung des Datenbriefes verzichten können. Haben sich seit dem letzten Datenbrief keine Veränderungen ergeben, kann durch die Daten erhebende Stelle ebenfalls auf die Zusendung eines Datenbriefs verzichtet werden; denkbar wäre in solchen Fällen auch die Beschränkung auf eine kurze Mitteilung. Auf Anforderung ist jedoch stets die entsprechende Auskunft zu erteilen.

Zu den personenbezogenen Daten müssen auch jene Daten und Informationen beigefügt werden, die ein Unternehmen aus den

übermittelten oder aus anderen Quellen bezogenen Daten ableitet, d.h. im Rahmen des Profiling, Scoring oder bei der Ermittlung von „Vorlieben für bestimmte Produkte“ den ursprünglich übermittelten Daten hinzufügt. Dies ist die Mindestforderung, wenn eine Profilbildung nicht vollständig untersagt werden soll.

Das Recht auf vollständige Auskunft soll nur mit unabhängiger richterlicher Prüfung eingeschränkt werden können.

Begründung:

Die Versendung eines kostenlosen Datenbriefs soll mehr Transparenz für den Bürger bringen. Vor allem soll der Datenbrief eine Bringschuld des Unternehmens, der Behörde oder Institution sein, die personenbezogene Daten verarbeitet. Dies gilt vor allem deshalb, weil der Bürger oft gar nicht weiß, wer wie viele personenbezogene Daten von ihm verarbeitet.

Profiling- und Scoringdaten müssen beigefügt werden, da zum Beispiel unrichtige Daten oder falsche Schlüsse/Scorings etc. eine Person stigmatisieren können. Zudem wird der Betroffene bei jedem Erhalt des Datenbriefs angeregt, darüber nachzudenken, ob er nach wie vor der weiteren Speicherung seiner personenbezogenen Daten zustimmt, oder es zum Anlass nimmt, zu widersprechen.

Der Mehraufwand, der für den Versand nötig ist, soll die verantwortlichen Stellen zur Datenvermeidung und -sparsamkeit motivieren.

Recht zur Verbandsklage bzw. Sammelklage

Das Recht zur Klage in datenschutzrechtlichen Fragen ist auch Verbänden und Gruppen einzuräumen, die dieses Recht stellvertretend für Betroffene wahrnehmen.

Begründung:

Kommerziell und womöglich global operierende Anbieter können sehr leicht durch entsprechende Ausgestaltung ihrer Geschäftsprozesse die Rechte aller ihrer Kunden oder im Extremfall sogar großer Teile der Bevölkerung verletzen. Da es sich in solchen Fällen um Grundsatzfragen der Zulässigkeit einer Praxis handelt, ist es schon aus Effizienzgründen sinnvoll, solche Streitfälle rechtlich nicht als Einzelfallentscheidung vor überlasteten Gerichten zu behandeln. Zudem ist der Einzelne insbesondere bei Auseinandersetzungen mit Großunternehmen allein häufig nicht in der Lage, seine Rechte effektiv durchzusetzen. Durch den Mechanismus der Verbands- oder Sammelklage können Datenschutzrechte Betroffener effektiver durchgesetzt werden. Zum Beispiel könnte eine Arbeitnehmervertretung (Betriebsrat) stellvertretend für die Arbeitnehmer klagen.

Recht auf Anonymisierung und Verschlüsselung

Jeder muss das Recht haben, anonym und verschlüsselt über öffentliche Netze zu kommunizieren. Verbot oder Einschränkung technischer Möglichkeiten der anonymen oder vertraulichen Kommunikation lehnen wir ab.

Es ist zu gewährleisten, dass technische Schutzmöglichkeiten wie Verschlüsselung oder Anonymisierungsdienste (Privacy Tools) uneingeschränkt genutzt werden können. Insbesondere darf es grundsätzlich keine Einschränkungen zur Nutzung von starker Kryptographie oder einen Zwang zur Offenlegung von Kryptoschlüsseln geben. Diese werden nicht nur zur Anonymisierung und Verschlüsselung, sondern auch zur Absicherung der Datenintegrität benötigt, da Prüfsummen ebenfalls mit kryptographischen Mitteln gebildet werden.

Ebenso müssen Anonymisierungsdienste und Verschlüsselungstechnologien grundsätzlich frei zugänglich sein und ihre Weiterentwicklung, Verbreitung und Betrieb nicht nur nicht behindert, sondern sogar öffentlich gefördert werden. Die Betreiber von Anonymisierungsdiensten wie z.B. TOR müssen einen besonderen Schutz vor Repressalien und Beschlagnahmung genießen, der eine hohe Eingriffsschwelle erzeugt.

Begründung:

Zusätzlich zum Grundrecht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht 2009 im Urteil zur Online-Durchsuchung das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme formuliert.

Auch für die Sicherung und Aufrechterhaltung weiterer Grundrechte wie u.a. Fernmelde- und Briefgeheimnis muss es grundsätzlich möglich sein, vertraulich zu kommunizieren. Für die Pressefreiheit und freie politische Willensbildung muss es grundsätzlich möglich sein, sich anonym im Internet zu informieren.

Verstöße gegen Datenschutzbestimmungen müssen angemessen sanktioniert werden

Wir fordern, dass Bußgelder in einer Höhe verhängt werden können, mit der eine Gewinnabschöpfung analog §43(3) BDSG möglich ist.

Um eine ausreichende Abschreckung zu gewährleisten, müssen verhängte Bußgelder sich analog dem Prinzip der Tagessätze an Umsatz und Gewinn der speichernden Stelle orientieren, also umso höher ausfallen, je größer der finanzielle Spielraum der speichernden Stelle ist. Durch diese Maßnahmen kann ein angemessener Abschreckungseffekt erzielt werden, der verhindert, dass Datenschutzverstöße vorsätzlich begangen oder billigend in Kauf genommen werden, da keine angemessene Sanktionierung zu befürchten ist.

Eine Anzeigepflicht bei Verstößen muss allgemein (nicht nur für Telekommunikation) eingeführt werden, Verstöße gegen diese einzuführende Pflicht sollen zudem Straftatbestand werden.

Rechtlich verbindliche Unternehmensregeln sollen für die Unternehmen Pflicht und für Betroffene einklagbar werden. (Unternehmensregeln werden durch die Selbstverpflichtung für das Unternehmen rechtlich bindend, analog zu Betriebsvereinbarungen gemäß BetrVG im deutschen Arbeitsrecht.)

Wenn ein Unternehmen wissentlich gegen Datenschutzgrundsätze und öffentlich gemachte Zusagen verstößt, die es sich selbst auferlegt hat, muss dies ebenfalls mit Bußgeldern oder sogar Gefängnisstrafe geahndet werden, da dadurch angenommen werden kann, dass Betroffene arglistig getäuscht werden.

Begründung:

Die Vergangenheit hat gezeigt, dass die bei Datenschutzverstößen verhängten Sanktionen nicht genügend abschreckende Wirkung entfalten, um wirksam zu sein. Darum fordern wir eine angemessene Sanktionierung solcher Verstöße.

Die Veröffentlichung von Datenschutzvorfällen dient der Schadenreduzierung für die Betroffenen, da diese sich auf negative Folgen einstellen oder ausgleichende Vorsichtsmaßnahmen treffen können, z.B. Accounts sperren oder Passwörter wechseln. Gleichzeitig entsteht durch die mit der Veröffentlichung drohenden Imageverluste eine höhere Motivation der verantwortlichen Stellen für Prävention.

Der Versuch, eine Vorfall zu vertuschen, soll eine strafbare Handlung werden. Das hat zum Ziel, das Risiko für die verantwortliche Stelle zu erhöhen, wenn sie dem drohenden Imageverlust zu entgehen versucht und damit höhere Risiken für die Betroffenen in Kauf nimmt, indem sie eine Warnung unterlässt.

Durch Wahrnehmung seiner Datenschutzinteressen darf dem Betroffenen keine wesentliche Benachteiligung entstehen (Diskriminierungsverbot)

Bestimmungen in Verträgen, AGB oder im Verwaltungsrecht müssen untersagt werden, wenn sie zu einer unverhältnismäßigen Benachteiligung von Kunden oder Bürgern führen, die ihre Datenschutzinteressen wahrnehmen wollen.

Wichtige, allgemein benötigte Dienstleistungen, müssen mit dem Prinzip der Datensparsamkeit und Vermeidung genutzt werden können. So muss es z.B. grundsätzlich möglich sein, Produkte oder Dienstleistungen bar zu bezahlen und es dürfen dabei keine wesentlich höheren Kosten entstehen als bei elektronischen Bezahlvorgängen. Eine allgemein benötigte oder nur von einem Anbieter verfügbare Dienstleistung (z.B. aufgrund eines Monopols oder sonstigen Mangels an datenschutzfreundlichen Alternativen) darf nicht durch Werbung finanziert werden, wenn dazu eine Zustimmung zur Verwendung der Benutzerdaten nötig ist. Es soll keine Verleitung oder Nötigung zur Angabe von Informationen geben, die für den eigentlichen Nutzungszweck nicht benötigt werden. Insbesondere wenn Alternativen fehlen, unverhältnismäßig teuer oder aufwendig sind, werden etroffene de facto dazu gezwungen, ihr Grundrecht auf informationelle Selbstbestimmung aufzugeben und können es nicht mehr frei ausüben.

Anwendungen, Hardware und Web-Dienste müssen standardmäßig restriktiv konfiguriert sein, beispielsweise bei Zugriffsrechten

Geräte wie Smartphones, Router, etc. sind häufig so konfiguriert, dass sie über ihre Nutzer mehr Daten preisgeben als für den Zweck des Dienstes erforderlich ist. Zum Beispiel wird bei Smartphones der aktuelle Standort genutzt, um den Wetterbericht oder die nächste Pizzeria anzuzeigen. Diese Features werden dem Nutzer ungefragt zur Verfügung gestellt. Dass der Preis die Aufgabe des Schutzes auf Privatsphäre ist, ist den meisten Nutzern nicht bewußt, ebenso wenig, dass sich von nun an ein Bewegungsprofil erstellen lässt. Die Dienste abzuschalten, ist oft umständlich und unterbleibt deswegen häufig.

Deshalb müssen die Geräte datenschutzkonform ausgeliefert werden. Die Aktivierung eines Dienstes muss explizit durch den Nutzer erfolgen. Der Vorgang muss einfach zu handhaben sein.

Zudem müssen die Nutzer über die Konsequenzen informiert werden. Das heißt, ihnen muss mitgeteilt werden, welche Daten für den Dienst von dem Anbieter abgerufen werden, und für welche Zwecke die Daten verwendet werden. Diesen weiteren Zwecken darf ein Nutzer widersprechen, ohne dass der Anbieter den Dienst verweigern darf. Untersagt ein Nutzer die weitere Verarbeitung, so muss der Anbieter die erhaltenen Daten sofort nach Diensterbringung wieder löschen, falls eine kurzzeitige Speicherung aus technischer Sicht erforderlich war. Ansonsten dürfen die Daten nur in einem flüchtigen Speichermedium verarbeitet werden.

Es dürfen in jedem Fall (auch bei Erteilung einer Erlaubnis) nur jene Daten abgerufen werden, die für die Erbringung des Dienstes unabdingbar sind (strikte Zweckbindung). Alle Geräte müssen entsprechend vorkonfiguriert werden. Nötigenfalls müssen Geräte länderspezifische Konfigurationen anbieten.

Für Software respektive Web-Anwendungen gilt das gleiche. Software muss stets datenschutzkonform ausgeliefert werden. Zum Beispiel müssen Web-Anwendungen wie soziale Netzwerke einen maximalen Schutz der Privatsphäre bieten.

Bei Verlassen eines Netzwerks müssen die personenbezogenen Daten für die anderen Teilnehmer des Netzwerks unsichtbar gemacht werden. Die personenbezogenen Daten müssen nach einer angemessenen Frist vollständig gelöscht werden. Beiträge in Diskussionen müssen vorläufig, falls nicht ohnehin im Netzwerk üblich, pseudonymisiert werden. Nach einer angemessenen Frist müssen Beiträge/Diskussionen archiviert werden. Sie sind nur noch auffindbar, wenn man explizit wie in einem „echten“ Archiv danach sucht.

Besonders zur Erzielung eines effektiven Kinderschutzes ist die datenschutzkonforme Konfiguration als Standard zu fordern.

Begründung:

In den meisten Fällen werden sowohl Hardware als auch Software in einer Konfiguration ausgeliefert, die aus Datenschutzsicht bedenklich erscheint. Gleiches gilt für die initiale Konfiguration von Web-Diensten wie z.B. sozialen Netzwerken. Für unerfahrene Nutzer ist es häufig schwierig, sich einen vollständigen Überblick über die Konfiguration zu verschaffen und die Einstellungen entsprechend dem von ihnen gewünschten Datenschutzniveau vorzunehmen.

Das führt häufig dazu, dass Nutzer unwissentlich Daten von sich preisgeben, vor allem, wenn sie fälschlich davon ausgehen, sich

in einem geschützten, abgeschlossenen Kommunikationsraum zu befinden.

Gerade bei Nutzern, die sich neu in einem Netzwerk anmelden oder sich neue Hardware kaufen, kann man Unerfahrenheit annehmen. Wenn alle Informationen, die solche Nutzer zur Verfügung stellen, für alle Mitglieder oder sogar noch weiterreichend sichtbar sind, lässt man diese Nutzer quasi in ein offenes Messer laufen. Das ist fahrlässig und unverantwortlich.

Hiervon betroffen sind insbesondere Kinder, die von Natur aus offen und ehrlich sind und bereitwillig vieles ausplaudern, ohne, dass ihnen bewusst ist, dass jeder dies lesen kann. Deshalb müssen die Einstellungen restriktiv sein. Persönliche Daten dürfen nur explizit und dediziert freigegeben werden. Bei pauschalen Freigaben (alle Freunde) muss den Nutzern angezeigt werden, wem sie die Daten freigeben. Es muss die Möglichkeit geschaffen werden, weitere Einschränkungen zu machen, zum Beispiel nur für Freunde, die man persönlich (real) kennt. In jedem Fall muss die Möglichkeit bestehen, pro Kontakt eine Freigabe dedizierter Daten zu bestimmen.

Datensparsamkeit und Datenvermeidung für Betreiber und Entwickler

Wir fordern, dass bei der Entwicklung von IT-Systemen die Prinzipien der Datensparsamkeit und Datenvermeidung verpflichtend werden. Am leichtesten lässt sich dies durchsetzen, wenn Anwendungen respektive Software so entwickelt werden, dass nur Daten durch die Anwendung erhoben und verarbeitet werden, die für den Zweck der Anwendung unbedingt erforderlich sind.

Begründung:

Datensparsamkeit und Datenvermeidung sind wichtige Designprinzipien, die bereits bei der Entwicklung berücksichtigt werden müssen, da sonst ein datenschutzkonformer Betrieb nur noch mit erheblichem Aufwand möglich ist.

In den letzten Jahrzehnten hat sich im Zuge der Verbilligung von Speichermedien eine Mentalität entwickelt, die die ehemals sorgsame Verwendung von Speicherplatz ins Gegenteil hat kippen lassen, nämlich möglichst viele Daten zu haben und zu verarbeiten, unabhängig davon, ob sie tatsächlich gebraucht werden. Frei nach dem Motto „vielleicht brauche ich die Daten ja doch noch".

Datenschutzbildung verpflichtend machen

Es müssen Mittel bereitgestellt werden, um Bildungsangebote zum Datenschutz und zu den Gefahren ungewollter Datenpreisgabe zu fördern. Dies umfasst beispielsweise Bildungsangebote zur Sensibilisierung für den Datenschutz (Awareness) und Nutzung von Werkzeugen zum Schutz der Privatsphäre (Privacy Enhancing Tools).

Datenschutz ist in die Curricula an Hochschulen, Schulen und in die berufliche Bildung aufzunehmen.

Bei IT-nahen Berufen ist der Umfang solcher Angebote um Themen wie Datensparsamkeit und datenschutzgerechte Gestaltung von IT Systemen zu erweitern. In jeder Informatik- oder informatiknahen Ausbildung müssen die Prinzipien der Datensparsamkeit und Datenminimierung gelehrt werden.

Begründung:

Das Bewusstsein, dass mehr Daten nicht zwangsläufig zu einer höheren Qualität des oder der Dienste führen, ist unterentwickelt, und führt dazu, dass Bürger, Staat und Unternehmen mehr Daten horten, als sie eigentlich bräuchten. Von daher ist es dringend notwendig, mittels Sensibilisierungskampagnen Bürger, Staat und Unternehmen darüber hinreichend aufzuklären und die in der IT Tätigen über die Anforderungen und Verpflichtungen des Datenschutzes zu unterrichten.

Verbesserung des Binnenmarkts

Verbot von nationalen Ausnahmen zur Vermeidung von Wettbewerbsverzerrungen

Die EU-Datenschutzrichtlinie muss als Minimumstandard für Datenschutz in der gesamten EU etabliert werden. Mitgliedsstaaten dürfen nur strengere Auflagen machen, keine schwächeren Gesetze z.B. mit Ausnahmeregelungen für bestimmte Branchen, Produkte oder Dienstleistungen.

Es darf keine nationalen Ausnahmeregelungen im Datenschutzrecht geben, die dazu führen, dass bestimmte Branchen, Produkte oder Dienstleistungen durch schwächere nationale Datenschutzbestimmungen billiger oder einfacher angeboten werden können als in Mitgliedsstaaten, in denen die Ausnahme nicht gilt und die EU Richtlinie konsequent umgesetzt wird. Ein schlechtes Beispiel dafür ist das Listenprivileg im deutschen Datenschutzrecht, das abgeschafft werden muss. Durch solche Ausnahmeregelungen kann schlechter Datenschutz zu einer Wettbewerbsverzerrung führen und sogar dazu anregen, weitere Ausnahmen zu beschließen.

Revision der Datenschutzbestimmungen bei der Zusammenarbeit von Justiz und Polizei bei der Strafverfolgung

Datenverwendung grundsätzlich unter Richtervorbehalt

Die Verwendung personenbezogener Daten durch Behörden – insbesondere Justiz- und Polizeibehörden – über den vorgegebenen Zweck hinaus ist grundsätzlich unter Richtervorbehalt zu stellen. Davon ausgenommen sind lediglich die auch sonst geltenden Regelungen (z.B. bei Gefahr im Verzug). Darüber hinausgehende Ausnahmetatbestände für Sicherheitsbehörden lehnen wir ab.

Unschuldsvermutung beachten

Die Unschuldsvermutung ist bei jeder Datenerhebung durch Behörden strikt zu beachten. Datensparsamkeit muss auch für Ermittlungsbehörden gelten – auch und gerade bei der Strafverfolgung. Daten dürfen nur zweckgebunden und bei konkretem Verdacht erhoben werden. Eine verdachtsunabhängige Erhe-

bung von Daten, wie bei der Vorratsdatenspeicherung (Data Retention) vorgesehen, lehnen wir grundsätzlich ab. Die Richtlinie 2006/24/EG ist zurückzuziehen. Wir verweisen dafür auf das Urteil des Bundesverfassungsgerichts (1 BvR 256, 263, 586/08 vom 2. März 2010) und die einschlägigen Stellungnahmen, beispielsweise des Arbeitskreises Vorratsdatenspeicherung und des Chaos Computer Club.

Wir verweisen auf die Empfehlungen im Rahmenbeschluss 2008/977/JI vom 27. November 2008, mit dem Ziel, „einen hohen Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihres Rechts auf Privatsphäre hinsichtlich der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen gemäß Titel VI des Vertrags über die Europäische Union sowie gleichzeitig ein hohes Maß an öffentlicher Sicherheit zu gewährleisten." Wir regen an, die Empfehlungen dieses Rahmenbeschlusses bei der Novellierung der Datenschutzrichtlinie zu berücksichtigen.

Berücksichtigen der globalen Dimension des Datenschutzes

Aufrechterhaltung von internationalen Datenschutzstandards

Für die Weitergabe personenbezogener Daten durch Behörden und Wirtschaftsunternehmen muss der gleiche Standard wie innerhalb der EU gelten. Dies ist im Einzelfall gegenüber den Datenschutzbehörden nachzuweisen. Das Safe-Harbour-Abkommen ist in seiner derzeitigen Form unzureichend und muss verbessert werden; insbesondere muss die Einhaltung angemessener Standards regelmäßig nachgewiesen werden.

Referenzen

BVerfG (2010): 1 BvR 256, 263, 586/08 vom 2. März 2010, http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html. Karlsruhe.

Constanze Kurz, Frank Rieger (2009): Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung. Chaos Computer Club, http://ccc.de/de/vds/VDSfinal18.pdf. Berlin.

Deutsche Vereinigung für Datenschutz (2011): Stellungnahme zur Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Gesamtkonzept für den Datenschutz in der europäischen Union. http://www.datenschutzverein.de/Themen/Stellungnahme%20EURiLi%20DVD.pdf. Bonn.

EU (2006): 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. Brüssel.

Europäische Kommission (2010): Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Gesamtkonzept für den Datenschutz in der europäischen Union. KOM(2010) 609. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf. Brüssel.

Europäischer Rat (2008): Rahmenbeschluss 2008/977/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:DE:PDF. Brüssel.

Dialektik der Informationssicherheit – Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit

Jahrestagung 2011 des FIfF e.V. in Zusammenarbeit mit der Hochschule München

11.-13. November 2011 in der Hochschule München, Lothstraße 64 (http://www.hm.edu/).

Die diesjährige FIfF-Jahrestagung (http://fiff.de/2011) findet in München statt, bitte merkt den Termin schon mal vor. Neben dem Sicherheitsthema wird sie sich mit aktuellen Problemen des Datenschutzes befassen.

Weil wir gerade mit der Planung begonnen haben, gibt es erst ein grobes Zeitraster:

- Freitagabend: Hauptvorträge, Podiumsdiskussionen
- Samstag: Arbeitsgruppen (und vielleicht Vorträge), Vergabe des FIfF-Studienpreises
- Sonntagvormittag: Vortrag, vielleicht Podiumsdiskussionen, Mitgliederversammlung mit Wahlen

Die Suche nach Referentinnen und Referenten läuft, bitte meldet Euch mit Euren Ideen für Personen und Arbeitsgruppen. Für die FIfF-Mitglieder steht das Wiki zur Verfügung (http://wiki.fiff.de), wir vom Orga-Team (JT-Orga@lists.fiff.de) freuen uns auf Eure Anregungen und natürlich auch über Hilfsangebote.

Wir Münchner erwarten Euch im November,

Dagmar

Stefan Hügel

Ereignis-Log 1/2011

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.

November 2010

14. November 2010: Der CDU-Politiker und Vorsitzende der Enquête-Kommission Internet und digitale Gesellschaft, Axel E. Fischer, spricht sich für ein „Vermummungsverbot im Internet" aus. Er bemängelt, dass sich Internetnutzer hinter Pseudonymen versteckten und damit der Verantwortung entzögen. Die Forderung zieht Kritik der Opposition und ironische Kommentare im Netz auf sich (Quelle: Badische Neueste Nachrichten, Heise).

15. November 2010: Die neue Verfassungsrichterin Susanne Baer ist besorgt über die digitale Spaltung weltweit und in Deutschland. Sie hält ein Grundrecht auf Netzzugang für erwägenswert. Dies solle in die Verpflichtung zur Sicherung des Existenzminimums eingebettet sein (Quelle: Grünes Blog, Heise).

16. November 2010: Einem NDR-Bericht zufolge arbeiten die am Hamburger Flughafen getesteten Nacktscanner fehlerhaft. In den meisten Fällen müssen die Passagiere von Hand nachkontrolliert werden (Quelle: NDR, Heise).

17. November 2010: Das niedersächsische Innenministerium rechtfertigt den Einsatz von Drohnen zur Überwachung bei den Demonstrationen gegen den Castor-Transport. Es gälten die gleichen Rechtsgrundlagen wie bei allen Videoaufzeichnungen der Polizei. Während der Proteste war vier Mal der unbemannte Quadrokopter md4-200 der Firma Microdrones gestartet (Quelle: Heise).

17. November 2010: Niedersachsens Innenminister Uwe Schünemann fordert das Verbot von Mobiltelefonen und Computern für sogenannte „Gefährder". Dies ist Teil eines 17-Punkte-Sofortprogramms, das verstärkte Kontroll- und Überwachungsmaßnahmen vorsieht (Quelle: Osnabrücker Zeitung, Heise).

17. November 2010: Nach einem Bericht der New York Times hat sich der Direktor des FBI, Robert S. Mueller, mit Vertretern von IT-Unternehmen getroffen und über die Möglichkeiten der Internetüberwachung gesprochen. Genannt werden Google und Facebook. Für 2011 wird ein Gesetzentwurf erwartet, der die Überwachung von verschlüsselten E-Mails, Internet-Telefonaten und Chats erleichtern soll und an dem das FBI und die NSA mitarbeiten (Quelle: New York Times, Heise).

18. November 2010: Eine neue Anwendung für Android-Smartphones soll die dort gespeicherten sozialen Kontakte und Interaktionsmuster auswerten und für Dienste und Werbung nutzbar machen. Bisher werden diese sozialen Graphen, die beispielsweise aus Interaktionen auf Facebook entstehen, noch nicht erfasst (Quelle: Technology-Review, Heise).

18. November 2010: Nach der Terrorwarnung von Bundesinnenminister Thomas de Maizière lebt die Debatte über die Vorratsdatenspeicherung wieder auf. Innenpolitiker von CDU/CSU und SPD fordern erneut die Einführung der verdachtsunabhängigen Protokollierung der Nutzerdaten. Das entsprechende Gesetz war im März 2010 vom Bundesverfassungsgericht für verfassungswidrig erklärt worden (Quelle: Heise).

19. November 2010: Der Justizausschuss des US-Senats billigt einstimmig den umstrittenen Combating Online Infringement and Counterfeits Act (COICA), der die Sperrung von Websites mit „rechtswidrigem Charakter" auf Antrag des Justizministeriums vorsieht. Der Gesetzentwurf stößt auf heftige Kritik von Bürgerrechtsvereinigungen und Konservativen, die vor einer Zensur durch die Bundesregierung warnen. Es seien auch Web-Seiten potenziell betroffen, die selbst keine Rechtsverletzungen begingen, aber darüber informierten (Quelle: Heise).

19. November 2010: Der Testphase für die Arbeitnehmer-Datenbank ELENA soll bis Ende 2014 verlängert werden. Die Kommunen hatten vor erheblichen Kosten gewarnt, denen nur äußerst geringe Entlastungen gegenüberstünden. ELENA steht in der Kritik, weil Arbeitnehmerdaten – insbesondere Entgeltdaten – in erheblichem Umfang in einer zentralen Datenbank gespeichert werden (Quelle: Heise).

21. November 2010: Bundesverbraucherschutzministerin Ilse Aigner kritisiert Google für seinen Umgang mit Einsprüchen im Zusammenhang mit Street View. Sie wirft dem Unternehmen mangelnde Sorgfalt bei der Bearbeitung vor (Quelle: Bild am Sonntag, Heise).

23. November 2010: Gegen zwei Polizeibeamte, die auf der Demonstration „Freiheit statt Angst" am 12. September 2009 einen Mann verprügelt haben sollen, hat die Berliner Staatsanwaltschaft Anklage erhoben. Den Beamten wird gemeinschaftliche Körperverletzung im Amt vorgeworfen, bei der der Geschädigte nicht unerheblich verletzt worden sei. Von der Tat wurden durch Passanten Videoaufzeichnungen angefertigt und ins Internet gestellt. Der Anwalt des Opfers, Johannes Eisenberg, kritisiert die lange Dauer bis zu Anklageerhebung (Quelle: taz, Heise).

23. November 2010: Gegen die Hamburger Sparkasse hat der Hamburger Datenschutzbeauftragte Johannes Caspar ein Bußgeld von €200.000 verhängt. Die Bank habe ohne Einwilligungserklärung der Kunden mobilen Finanzberatern weitgehenden Zugriff auf ihre Daten gewährt. Außerdem habe das Geldinstitut unter Nutzung der Kundendaten Charakterprofile ihrer Kunden erstellt und ebenfalls an die Berater weitergegeben. Mittlerweile sei den Beratern aber der Zugriff entzogen worden (Quelle: Heise).

26. November 2010: Bundesinnenminister Thomas de Maizière fordert die rasche Einführung der Quellen-Telekommunikati-

onsüberwachung. Angesichts der Gefährdungslage dürfe Strafverfolgern der Zugang zu „Bereichen hochkonspirativer Kommunikation“ nicht verwehrt werden (Quelle: Rheinische Post, Heise).

26. November 2010: An den Universitäten Witten/Herdecke und Bielefeld soll untersucht werden, wie Sicherheitsgesetze in Deutschland tatsächlich entstehen. Es sollen Zusammenhänge zwischen Sicherheitsproduzenten und der Sicherheitsgesetzgebung aufgearbeitet und die Probleme herausgearbeitet werden, die sich durch die Einflussnahme von Lobbyisten der Sicherheitsproduzenten ergeben (Quelle: Universität Bielefeld, Universität Witten/Herdecke, Heise).

26. November 2010: In einem 12-Punkte-Papier fordert Kulturstaatsminister Bernd Neumann (CDU) ein Warnhinweismodell zur Durchsetzung „geistiger Eigentumsrechte“. Im Wiederholungsfall müsse es dann eine „ernstzunehmende Reaktion“, beispielsweise eine kostenpflichtige Abmahnung, geben. Von Ausschlusssperren wie beim französischen „Three-Strikes-Modell“ ist vorläufig nicht die Rede (Quelle: Bundesregierung, Heise).

30. November 2010: Einige Banken sperren nach einem Datendiebstahl Kreditkarten ihrer Kunden. Bekannt wurden Fälle bei der Postbank und ING-Diba. Der Online-Shop, bei dem das Datenleck auftrat, wurde aus rechtlichen Gründen zunächst nicht genannt. Laut ING-Diba ist ca. 1% ihrer Kunden betroffen (Quelle: Heise).

Dezember 2010

1. Dezember 2010: Bundesverbraucherschutzministerin Ilse Aigner zeigt sich besorgt wegen der Möglichkeit der Verletzung von Persönlichkeitsrechten durch Gesichtserkennungsdienste im Netz, wie sie beispielsweise Google mit dem Online-Fotodienst Picasa anbietet. Ein internetfähiges Fotohandy sei bereits in der Lage, Passanten durch einen automatischen Abgleich von Internet-Datenbanken zu identifizieren. Die Bildersuche dürfe nur mit ausdrücklicher Genehmigung des Abgebildeten zulässig sein (Quelle: Heise).

1. Dezember 2010: In einem Entschließungsantrag zum 22. Tätigkeitsbericht des Bundesdatenschutzbeauftragten hat der Bundestag die Gefährdung der informationellen Selbstbestimmung durch technische Entwicklungen und das veränderte Kommunikationsverhalten kritisiert. Er zeigt sich besorgt über das „unaufhörliche Anwachsen von Datenbeständen“ (Quelle: Heise).

4. Dezember 2010: Der Internet-Bezahldienst PayPal sperrt das Spendenkonto von Wikileaks. Begründet wird das mit einer „Verletzung der Nutzungsbedingungen“. Auch andere Dienste – Anbieter von Serverkapazität und Kreditkartendienstleister – sperren Wikileaks den Zugang (Quelle: The PayPal Blog, netzpolitik.org, Heise).

4. Dezember 2010: EU-Innenkommissarin Cecilia Malmström hat erklärt, dass die verdachtsunabhängige Vorratsdatenspeicherung von Nutzerdaten nicht zur Diskussion stünde. Die Daten seien in einigen Fällen der einzige Weg, schwere Verbrechen aufzuklären. Die Haltung der Kommissarin wird von Gegnern der Vorratsdatenspeicherung kritisiert. EU-Datenschutzbeauftragter Peter Hustinx verwies auf das laufende Evaluationsverfahren; ein Sprecher des Arbeitskreises Vorratsdatenspeicherung wies darauf hin, dass sich die Aufklärungsquote nach der Einführung nicht verbessert habe (Quelle: Heise).

15. Dezember 2010: Nach einem Bericht von NDR Info hat die Stadtverwaltung von Glücksburg bei einem Flohmarkt, bei dem altes Inventar verkauft wurde, versehentlich auch Festplatten und Server mit vertraulichen Daten – u.a. Steuerbescheide – veräußert. Nachdem sich der Finder bei den Behörden gemeldet hatte, holten Mitarbeiter der Datenschutzbehörde in Kiel die Geräte ab (Quelle: NDR Info, Heise).

16. Dezember 2010: Die Novellierung des umstrittenen Jugendmedienschutz-Staatsvertrags (JMStV) scheitert im Landtag von Nordrhein-Westfalen. Obwohl der damalige Ministerpräsident Jürgen Rüttgers (CDU) dem Vertragtext ohne Einschränkung zugestimmt hatte, lehnte ihn die CDU-Fraktion wie auch FDP und Linke einstimmig ab. Ohne die Unterstützung der anderen Fraktionen stimmten dann auch die Regierungsparteien SPD und Grüne gegen den Vertrag (Quelle: netzpolitik.org, Heise).

16. Dezember 2010: Der Bundestag lehnt mit den Stimmen der Koalitionsfraktionen einen Antrag der Grünen ab, sich in Brüssel für die Aufhebung der Richtlinie für die Vorratsdatenspeicherung einzusetzen. Die Protokollierung sei „dringend notwendig“, so Patrick Sensburg von der CDU/CSU-Fraktion (Quelle: Heise).

18. Dezember 2010: Die französische Nationalversammlung verabschiedet einen Teil des Sicherheitspakets „Loppsi 2“ (Loi d'orientation et de programmation pour la performance de la sécurité intérieure), der Websperren ohne Richterbeschluss vorsieht. Die Bürgerrechtsvereinigung „La quadrature du net“ sieht durch die fehlende Kontrolle durch die Justiz ihre Befürchtungen bestätigt, dass es der Regierung dabei um eine allgemeine Kontrolle des Netzes gehe (Quelle: Heise).

21. Dezember 2010: Das ungarische Parlament beschließt das umstrittene Mediengesetz, das die Einrichtung einer neuen Medienbehörde NMHH vorsieht. Diese kann jetzt neben öffentlich-rechtlichen Anstalten auch private Fernseh- und Rundfunksender, Zeitungen und Internetportale kontrollieren. Diese können bei Verstoß gegen nur vage definierte Regeln mit hohen Geldstrafen belegt werden, die einzelne Medien im Extremfall in den Ruin treiben. Der Vorstand der Medienbehörde besteht ausschließlich aus Vertretern der Regierungspartei FIDESZ. Das Gesetz wird international kritisiert. Ungarn übernimmt am 1. Januar 2011 die Präsidentschaft des europäischen Rats (Quelle: Zeit, Spiegel, taz, Heise).

Stefan Hügel

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

Januar 2011

7. Januar 2011: Die Videoüberwachung an niedersächsischen Schulen wird durch den Landesdatenschutzbeauftragten Joachim Wahlbrink kritisiert. Bei Kontrollen seien Mängel festgestellt worden, beispielsweise fehlende Vorabkontrollen und Verfahrensbeschreibungen, zu lange Speicherfristen und missachtete Mitbestimmungsrechte. 29 Kameras, davon 14 Attrappen mussten abgebaut oder in ihrer Funktion eingeschränkt werden (Quelle: Heise).

8. Januar 2011: Die US-Justizbehörde fordert die Herausgabe personenbezogener Daten von Twitter. Konkret handele es sich dabei um die über den Kurznachrichtendienst verschickten Tweets. Betroffen sind unter anderem Wikileaks-Sprecher Julian Assange und die Isländische Parlamentsabgeordnete Birgitta Jonsdottir (Quelle: Heise).

14. Januar 2011: Bei den sächsischen Radiosendern Radio Chemnitz, Radio Zwickau und Hitradio-RTL konnten zeitweise die Daten von Gewinnspielteilnehmern ausgelesen werden. Dazu gehören Name, Adresse, E-Mail-Adresse, Telefonnummer und IP-Adresse. Entgegen der Datenschutzbestimmungen, die vorsehen, die Daten am Ende des Nutzungsvorgangs zu löschen, waren sie teilweise nach zwei Jahren noch verfügbar. Das verantwortliche Unternehmen BCS Broadcast Sachsen GmbH & Co. hat den Zugriff auf die Daten inzwischen gesperrt (Quelle: Heise).

16. Januar 2011: Bundesjustizministerin Sabine Leutheusser-Schnarrenberger spricht sich für eine verkürzte Vorratsdatenspeicherung aus. Bei dem Quick Freeze plus genannten Verfahren sollen die Verbindungsdaten einige Tage vorgehalten werden. Zuvor hatte bereits Budesdatenschutzbeauftragter Peter Schaar eine solche „Vorratsdatenspeicherung light" befürwortet. Bei den Gegnern der Vorratsdatenspeicherung stößt der Vorstoß auf scharfe Kritik (Quelle: netzpolitik.org, Heise).

17. Januar 2011: Der Bundesdatenschutzbeauftragte Peter Schaar kritisiert eine massive Zunahme der Bankkonten-Abfragen durch Behörden. Nach aktuellen Zahlen stieg die Anzahl der Abfragen von 44.000 im Jahr 2009 auf 58.000 im Jahr 2010 (Quelle: Neue Osnabrücker Zeitung, Heise).

22. Januar 2011: Der Anwalt von Bradley Manning, der im Militärgefängnis Quantico in Virginia festgehalten wird, beschwert sich über dessen Haftbedigungen. Sein Mandant würde im Militärgefängnis misshandelt. Manning wird vorgeworfen, geheime Dokumente an Wikileaks übergeben zu haben; Anklage wurde wegen eines dort veröffentlichten Videos („Collateral Murder") erhoben, das einen Hubschrauberangriff auf Zivilisten im Irak zeigt (Quelle: Heise).

25. Januar 2011: Der Rheinland-Pfälzische Landesdatenschutzbeauftragte Edgar Wagner wirft Unternehmen im Land eklatante Verstöße gegen Datenschutzbestimmungen vor. 400 von 460 Unternehmen setzten Google Analytics ein, dessen aktuelle Version gegen Datenschutzvorschriften verstoße. Sie würden nun angeschrieben und um eine Stellungnahme gebeten (Quelle: Heise).

26. Januar 2011: In Rheinland-Pfalz wurde mit den Stimmen von SPD, CDU und FDP ein umfangreiches Überwachungspaket beschlossen. Heimliche Online-Durchsuchung von Rechnern sowie Quellen-Telekommunikationsüberwachung wurden eingeführt. Die Polizei hat zusätzlich nun die Befugnis, zur Gefahrenabwehr Mobilfunkverbindungen zu unterbrechen oder gar zu verhindern. Grüne, Linke und Piratenpartei kritisierten die Umsetzung scharf (Quelle: netzpolitik.org).

31. Januar 2011: Die Electronic Frontier Foundation wirft dem FBI den Missbrauch von Befugnissen im Anti-Terror-Kampf vor. Die Behörde habe in rund 40.000 Fällen bei der Abfrage von Daten Verdächtiger gegen geltendes Recht verstoßen. Agenten des FBI hätten bei Erklärungen an Gerichte die Unwahrheit gesagt und unrechtmäßig erhaltenes Beweismaterial an Geschworene übergeben (Quelle: EFF, Heise).

31. Januar 2011: Das Landgericht Landshut hat entschieden, dass die monatelange Überwachung des Computers eines Beschuldigten mit einem Trojaner ohne Rechtsgrundlage erfolgt sei. Durch den Trojaner wurden alle 30 Sekunden Bildschirmfotos des Browserinhalts angefertigt; dies war in der Überwachungsanordnung nicht enthalten (Quelle: Heise).

Februar 2011

1. Februar 2011: Nach einem Bericht der Financial Times Deutschland haben die USA im Rahmen des SWIFT-Abkommens tieferen Einblick in europäische Bankdaten als bisher bekannt. Sie können demnach auch auf innereuropäische Überweisungsdaten zugreifen, wenn diese über das System SwiftNet Fin erfolgten. Das wurde durch einen Sprecher von Swift bestätigt (Quelle: Financial Times Deutschland, Heise).

11. Februar 2011: Der Bundesrat hat die Überlegungen der EU-Kommission zur Novellierung der aus dem Jahr 1995 stammenden Datenschutzrichtlinie als zu weitgehend kritisiert. Beanstandet wird vor allem die geplante Einbeziehung des Polizei- und Justizbereichs. Dieser solle auf grenzüberschreitende Sachverhalte beschränkt werden (Quelle: Bundesrat, Heise).

13. Februar 2011: Der oberste Gerichtshof in Zypern erklärt das dort beschlossene Gesetz zur Umsetzung der EU-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung für nicht vereinbar mit der dortigen Verfassung. Die Entscheidung besagt, dass die Daten nur bei bereits Inhaftierten oder bei laufenden Konkursverfahren verwendet werden dürfen; damit sind sie für normale Polizeiarbeit nicht mehr verwendbar (Quelle: netzpolitik.org).

14. Februar 2011: Der Innenausschuss der europäischen Parlaments hat sich mit deutlicher Mehrheit gegen obligatorische Regelungen zur Sperrung von Web-Seiten in der EU ausgesprochen. Gegen Darstellungen von Kindesmissbrauch im Netz soll deren Entfernung vorgeschrieben werden, eine Filterung nur in Ausnahmefällen erfolgen. Trotz des Votums will sich Innenkommissarin Cecilia Malmström weiter für Websperren einsetzen (Quelle: netzpolitik.org, Heise).

19. Februar 2011: Facebook aktiviert nun auch in Deutschland die umgehende Personalisierung, die einer Reihe von Partner-

sites den Zugriff auf Informationen der Facebook-Mitglieder erlaubt (Quelle: Hannoversche Allgemeine Zeitung, Heise).

19. Februar 2011: US-Behörden nehmen im Rahmen von Ermittlungen versehentlich 84.000 Websites für mehrere Tage vom Netz. Das Departement of Homeland Security hatte im Rahmen der Operation Protect our Children zehn Domains beschlagnahmt, von denen eine, mooo.com, die 84.000 – unverdächtigen – Websites versorgt. Empört waren die Betroffenen vor allem, weil es zuvor keine Anhörung gab, sondern eine einfache richterliche Anweisung ausreichend war (Quelle: Heise).

23. Februar 2011: Der AK Zensur erhebt Verfassungsbeschwerde gegen das Zugangserschwerungsgesetz zur Umsetzung von Netzsperren. Das Gesetz wurde von der damaligen Bundesfamilienministerin Ursula von der Leyen trotz einer von 134.000 Menschen unterzeichneten Petition initiiert. Es ist zwar in Kraft, die Anwendung wurde von der Regierungskoalition aber ausgesetzt (Quelle: netzpolitik.org).

24. Februar 2011: Der Grünen-Politiker Malte Spitz lässt seine Vorratsdaten aus einem Zeitraum von sechs Monaten visualisieren und ins Netz stellen (siehe dazu auch den untenstehenden Beitrag). In einer interaktiven Karte kann man nachvollziehen, welche Informationen durch Vorratsdaten über einzelne Personen sichtbar gemacht werden können. Zusätzlich wurden sie mit öffentlich zugänglichen Informationen – beispielsweise aus Tweets oder Blogs – angereichert. Aus Datenschutzgründen wird nicht dargestellt, mit wem Gespräche jeweils geführt wurden. Die ca. 36.000 Datensätze aus einem halben Jahr können auch als Excel-Tabelle heruntergeladen werden (Quelle: Zeit, netzpolitik.org, Heise).

Ralf E. Streibl

IM Handy?

Der exemplarisch gläserne Mobilfunkkunde

Wir dürfen Malte Spitz für seinen Selbstversuch dankbar sein. Der Bundestagsabgeordnete erstritt sich von seinem Mobilfunkprovider Zugriff auf einige im Zuge der Vorratsdatenspeicherung gespeicherte Daten:

> *„Ich habe dazu meinen damaligen Mobilfunkanbieter T-Mobile auf Auskunft verklagt. Grundlage war § 34 des BDSG. Das Verfahren hat sich hingezogen und es gab einen Gerichtstermin. Das Bundesverfassungsgericht hatte jedoch vorher die generelle Ausgestaltung der Vorratsdatenspeicherung für verfassungswidrig und für nichtig erklärt und die Löschung aller gespeicherten Daten angeordnet. Daraufhin haben wir schnell gehandelt und die Herausgabe der Daten außergerichtlich mit T-Mobile geklärt. Die Datensätze, die ich auf diese Einigung hin zu meiner Person erhalten habe, enthalten nicht die Nummern der Menschen die ich angerufen habe oder die mich angesimst haben. Sprich die Hälfte der Daten einer regulären Vorratsdatenspeicherung fehlt.“* [1]

Screenshot der interaktiven Visualisierung der Daten (Quelle 2)

Eine Auswertung dieser reduzierten Daten erlaubt jedoch vielfältige personenbezogene Einblicke, wie die auf der Website der *Zeit* zugängliche interaktive und grafische Aufbereitung eindrucksvoll verdeutlicht. Ob man lokalisiert, in welcher Gegend Malte Spitz sich zu einer bestimmten Zeit befand, ob man sich einfach und schnell darstellen lassen möchte, wann Malte Spitz sich in einer bestimmten Gegend aufgehalten hat, oder ob man durch chronologisches Laufenlassen der gespeicherten Geodaten ein näherungsweises Bewegungsprofil von Malte Spitz auf der Landkarte ansehen kann – es erschreckt gewaltig.

Im Zeitalter von Smartphones und Flatrates fallen immense Datenmengen an. Im einzelnen harmlos und unbedeutend entsteht in der Summe der Daten ein profundes Bild, wie *Die Zeit* schreibt:

> *„Das Profil enthüllt, wann Malte Spitz durch Straßen läuft, wann er Bahn fährt, wann er fliegt. Es zeigt, in welchen Städten und an welchen Orten er sich aufhält. Es zeigt, zu welchen Zeiten er arbeitet und zu welchen er schläft, wann man ihn am besten erreichen kann und wann eher nicht. Es zeigt, wann er lieber telefoniert und wann er lieber eine SMS verschickt und es zeigt, in welchem Biergarten er gerne sitzt. Es zeigt ein Leben.“* [2]

Mögen zukünftig möglichst viele Menschen dieses Interface zu Malte Spitz Leben ausprobieren und daraus erste, vorsichtige Eindrücke entwickeln, wie transparent die Aggregation von „Ich-hab-doch-nichts-zu-verbergen“-Daten einen Menschen machen kann. Truman 2011.

Anmerkungen:

1 http://www.malte-spitz.de/blog/4084981.html

2 http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

FIfF-Studienpreis 2010

Prämierte Arbeiten des FIfF-Studienpreises – Teil II

Bei der FIfF-Jahrestagung 2010 in Köln haben wir zum ersten Mal den FIfF-Studienpreis verliehen. Ein Bericht über die Verleihung haben wir in der Ausgabe 4/2010 der FIfF-Kommunikation abgedruckt.

Dort finden sich auch bereits die Beiträge von *Andrea Knaut: Biometrische Grenzkontrollen und nationale Identität* und von *Michael Prinzinger: Anonymität – Schutzschild der Bevölkerung*, die jeweils mit einem zweiten Preis ausgezeichnet wurden. Hier folgen nun Beiträge der beiden anderen Preisträger:

- *Grenzen der digitalen Anonymität* von *Phillip W. Brunst*. Seine Dissertation wurde mit dem ersten Preis ausgezeichnet.
- *Ein Rollenspiel zum Datenschutz in Netzwerken* von *Jens Jacobi*. Seine Arbeit wurde mit einem zweiten Preis ausgezeichnet.

Das FIfF dankt nochmals allen Teilnehmerinnen und Teilnehmern des Studienpreises für die eingereichten Arbeiten und gratuliert den Preisträgern herzlich.

Phillip W. Brunst

FIfF-Studienpreis 2010 1.Preis

Grenzen der digitalen Anonymität

Die Dissertation „Anonymität im Internet“[1] wurde auf der Jahrestagung des FIfF 2010 mit dem erstmals vergebenen Studienpreis ausgezeichnet. Der Verfasser möchte sich hierfür herzlich bei den Mitgliedern der Auswahlkommission sowie dem Vorstand bedanken. Der nachfolgende Artikel stellt die Arbeit in ihren wesentlichen Grundzügen näher dar.

Einführung

Die Rolle der Anonymität im Internet stellt sich momentan zwiegespalten dar. Seit bekannt wurde, dass zum Beispiel die sog. „Grüne Revolution“ in Iran im Jahr 2009 in weiten Teilen über Twitter koordiniert wurde oder welche Bedeutung die internetbasierte Informationsverbreitung bei der aktuellen „Jasmin-Revolution“ in Tunesien bzw. dem Regierungswechsel in Ägypten gespielt hat, wurde breiten Teilen der Bevölkerung schlagartig klar, welche wichtige gesellschaftspolitische Funktion ein anonymer Zugriff auf das Internet haben kann. Gleichzeitig werden jedoch insbesondere von Industrieverbänden (z.B. im Zusammenhang mit illegalen Musiktauschbörsen) und einigen Politikern (etwa bei der Verbreitung von Kinderpornographie) besonders intensiv die negativen Seiten eines anonymen Internetzugriffs herausgestellt. Besonders drastisch brachte dies der Präsident des Bundeskriminalamtes, *Jörg Ziercke,* auf einer Konferenz im Jahr 2007 auf den Punkt: „Verschlüsselung und Anonymisierung schaffen verfolgungsfreie Räume mit fatalen Wirkungen für die Innere Sicherheit“.

Vor diesem Hintergrund ist es wichtig, das Spannungsfeld zwischen einem gesellschaftlichen Bedürfnis nach Anonymität und seiner gegenwärtig gesetzlich verankerten Reichweite einerseits und den Auswirkungen auf die Strafverfolgung andererseits kritisch zu beleuchten. Die Arbeit „Anonymität im Internet“ soll hierzu einen Beitrag leisten.

Eine wichtige Grundfrage betrifft zunächst die Bedeutung von Anonymität und die Motive, sie aktiv einzusetzen (I.). Darauf aufbauend ist zu fragen, in wie weit Anonymität heute – noch – geschützt ist (II.). Dies betrifft zum einen den rechtlich gewährten Schutz, aber auch die momentan technisch zur Verfügung stehenden Möglichkeiten der Nutzer, aktiv die Entstehung von Spuren ihrer Nutzung zu verhindern oder zumindest zu verschleiern sowie Möglichkeiten von Strafverfolgungsbehörden, trotz derartiger technischer Maßnahmen eine Identifizierung herbeizuführen. Abschließend lassen sich – und zwar nur durch diese Zusammenschau von rechtlichen und technischen Parametern – einige Auswirkungen aufzeigen (III.).

I. Motivation zur anonymen Internetnutzung

Das oben angeführte Beispiel der iranischen Protestbewegung zeigt eines von vielen möglichen Motiven, warum Menschen anonym im Internet agieren möchten: Geschützt seine Meinung kundtun oder sich informieren zu können, ohne befürchten zu müssen, bereits für diesen Vorgang zur Verantwortung gezogen zu werden. Neben diesem Beweggrund gibt es allerdings eine Vielzahl von Gründen, die dazu führen können, dass eine Person der Anonymität vor dem ausdrücklichen Auftreten im eigenen Namen den Vorzug geben kann.

Anders als man zunächst vermuten würde, geht es in den meisten Fällen gar nicht darum, bewusst die eigene Identität zu verheimlichen, sich zu verstecken oder aktiv etwas zu verbergen. Vielmehr spielt die Identität einer Person in vielen Fällen schlicht keine Rolle, sie ist ganz einfach bedeutungslos. So wären die meisten Menschen überrascht, wenn sie vom Kassierer im Supermarkt aufgefordert würden, sich zunächst persönlich vorzustellen und evtl. einen Personalausweis vorzulegen, bevor die eingekauften Waren bezahlt werden können. Vielmehr ist der anonyme Einkauf die Regel, der Austausch von Waren gegen Geld steht im Vordergrund, nicht die Identität der jeweils anderen Person. In anderen Fällen wird die Anonymität bewusst in

den Hintergrund gestellt, etwa wenn bei den „Anonymen Alkoholikern“ das Problem – die Sucht – in den Vordergrund gestellt und der Angst, von anderen erkannt und stigmatisiert zu werden, wirkungsvoll begegnet werden soll. Selbst die physische Sicherheit einer Person kann von der erfolgreichen Wahrung seiner Anonymität abhängen, etwa bei Informanten in Gruppierungen der Organisierten Kriminalität. Es ließen sich viele weitere Motive anführen, warum Personen nicht ihre Identität offenbaren möchten, sondern ein anonymes Agieren vorziehen. Ihnen allen ist gemein, dass regelmäßig nicht das Verbergen der eigenen Identität zur Begehung von Unrecht oder sogar Straftaten im Vordergrund steht, sondern, dass in weiten Bereichen Anonymität als ein Grundbedürfnis angesehen wird, das in der „realen“ (in Abgrenzung zu einer „virtuellen“) Gesellschaft allgemein akzeptiert und sogar weitgehend als selbstverständlich und notwendig wahrgenommen wird.

Im virtuellen Raum ließe sich dieses Grundbedürfnis perfekt umsetzen. Da alle Daten rein digital verarbeitet werden, könnten Identitätsspuren in einer nie zuvor gesehenen Absolutheit vernichtet und Anonymität vorbildlich garantiert werden. Das Gegenteil scheint jedoch der Fall zu sein: selbst in zivilisierten Ländern der westlichen Welt wird über einen „Killswitch“ debattiert, mit dem das Internet bei Bedarf landesweit vollständig abgeschaltet werden können soll[2] und Spuren aller Internetnutzer sollen in weiten Teilen verdachtslos erfasst und für einen längeren Zeitraum gespeichert werden, damit bei Bedarf auch noch Monate später alle Handlungen möglichst lückenlos nachvollzogen werden können.

Nutzer, die dem entgegenwirken wollen, stehen vor mehreren gewichtigen Problemen. Zunächst haben sie keine alleinige Kontrolle über die Preis- und Weitergabe ihrer Daten. Viele Informationen fallen bereits aus technischen Gründen zwangsweise an (etwa die von einem Provider zugewiesene IP-Adresse) und werden nicht nur auf dem eigenen Rechner, sondern im Rahmen der Übertragung bei einer Vielzahl weiterer Stationen erfasst und verarbeitet. Auf das weitere Schicksal dieser Informationen hat der Nutzer keinen Einfluss. Nicht zuletzt aufgrund technischer Pannen und ungenügender Sicherheitsmaßnahmen in vielen Unternehmen sind persönliche Daten immer wieder Dritten zugänglich geworden. Darüber hinaus werden, z.B. zu Marketing-Zwecken, Daten auch bewusst mit anderen Beständen zusammengeführt, um so neue Erkenntnisse über die von Ihnen betroffenen Personen zu gewinnen.

Vor diesem Hintergrund wäre es eigentlich zu erwarten, dass der Staat seine Bürger schützt und versucht, digitale Gefahren weitestgehend einzudämmen, zumindest aber, dass er ihm ausreichende technische Möglichkeiten an die Hand gibt, mit denen Nutzer selbst für ihren Datenschutz sorgen können.

II. Schutz der digitalen Anonymität

A. Rechtlicher Schutz…

Ein erster Blick auf die Rechtslage erscheint ermutigend. Zwar sprechen inter- und supranationale Regelungen Anonymität nur selten ausdrücklich an. Dennoch wird ein weitreichender Schutz dadurch gewährleistet, dass selbst ältere Vorschriften ein allgemeines Datenschutzregime errichten, das auch Internetsachverhalte mit erfassen kann. Die mit der Interpretation dieser Normen befassten Organe und Gerichte legen daher diese Vorschriften regelmäßig weit aus und passen sie so an die Gefahren der heutigen Zeit an. Anonymität ist die stärkste und sicherste Form des Datenschutzes, da sich ohne Personenbezug keine Gefährdung mehr für die durch die Daten betroffene Person ergibt. Ein weit verstandener allgemeiner Datenschutz umfasst daher auch die Anonymität.

Vor diesem Hintergrund mag es zunächst verwunderlich erscheinen, dass das deutsche Grundgesetz keine explizite Regelung zum Datenschutz (geschweige denn zur Anonymität) enthält. Das Bundesverfassungsgericht hat jedoch aus den Vorschriften zur allgemeinen Handlungsfreiheit und der Menschenwürde im Rahmen seines „Volkszählungsurteils“ die Grundlagen des deutschen Datenschutzrechts herausgearbeitet. Dass ein Mensch zum bloßen Objekt degradiert oder auf eine Nummer reduziert wird, könne nur vermieden werden, wenn die betroffenen Personen jederzeit wüssten, wer welche Informationen über sie besitzt. Zudem dürften Daten nicht ohne Grund erhoben oder ohne einen konkreten Zweck weiter verarbeitet werden. Auch ohne explizite Regelung des Datenschutzes im deutschen Grundgesetz ist daher ein weitreichender Schutz gegeben.

Dieser wird in den einfachen Gesetzen auch – so scheint es auf den ersten Blick – konsequent umgesetzt, z.B. als allgemeines Leitprinzip im Bundesdatenschutzgesetz (§ 3a BDSG). Ausdrückliche Vorgaben finden sich etwa in den rechtlichen Vorgaben für Angebote in den „neuen Medien“ (z.B. § 13 Abs. 6 TMG). Danach sollen sowohl die Nutzung von Internet-Diensten als auch deren Bezahlung anonym ermöglicht werden, wenn dies technisch möglich und zumutbar ist. In der Praxis zeigt sich allerdings, dass diese gesetzlichen Forderungen nicht überall Beachtung finden. So ist die Abfrage von Daten, die für die Erbringung einer Dienstleistung nicht zwingend benötigt werden, weithin

Phillip Brunst

Dr. **Phillip Brunst** hat über viele Jahre das Referat ‚Informationsrecht & Rechtsinformatik‘ am Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg i. Br. geleitet. Gegenwärtig arbeitet er wissenschaftlich vor allem für das Cybercrime Research Institute in Köln. Kontakt- und weitere Informationen sind unter *http://www.pbrunst.de* abrufbar.

üblich, was offenbar von den zuständigen Behörden auch toleriert wird. Dies betrifft aber bereits die tatsächliche Gesetzesanwendung und nicht mehr die rechtliche Situation an sich. Diese ist – so kann zusammenfassend sowohl für Deutschland als auch für die inter- und supranationale Ebene festgehalten werden – erst einmal recht erfreulich, da Anonymität in weiten Teilen rechtlich zumindest geachtet, in neuen Vorschriften sogar aktiv gefördert wird.

B. … und seine Grenzen

Dieses positive Bild der rechtlichen Situation trügt allerdings. Notwendig ist es, nicht nur die Vorschriften zu betrachten, die ausdrücklich die Daten und insbesondere die Anonymität einer Person schützen. Vielmehr muss auch die spiegelbildliche Seite berücksichtigt werden, d.h. Normen, die eine Ermittlung der Identität einer Person im Internet erlauben. Betrachtet man auch diese Vorgaben, so ergibt sich nicht nur ein anderes Bild, sondern es wird darüber hinaus auch ein Paradigmenwechsel erkennbar.

Bislang besagte ein rechtlicher Grundsatz, dass auf persönliche Informationen einer Person dann zugegriffen werden darf, wenn ein konkreter Tatverdacht gegen diese vorliegt. Zudem sollen dann die Zugriffe grundsätzlich auch nur diese Person betreffen und andere, unverdächtige, nur soweit dies unabdingbar ist, etwa weil sie als unwissender Mittelsmann dienen. Ein überwachungsfreies Handeln war also bisher die Regel, ein Fokus staatlicher Aufmerksamkeit die Ausnahme.

Von diesem etablierten Grundsatz wendet sich die gegenwärtige Sicherheitsgesetzgebung ausdrücklich ab. Dieser Paradigmenwechsel hat sich bereits seit einiger Zeit auf der europäischen Ebene abgezeichnet und wurde anschließend in Deutschland umgesetzt. Durch die Einführung der Vorratsdatenspeicherung sollen die Daten aller Bürger möglichst lückenlos gesammelt werden, unabhängig davon, ob sie sich verdächtig gemacht haben oder nicht. Für den Fall einer späteren Straftat – und sei sie auch noch so geringfügig – sollen möglichst lückenlose Beweismittel für die Ermittlung herangezogen werden können. Ergänzend kommen weitere invasive Maßnahmen, wie z.B. Online-Durchsuchung oder Quellen-TKÜ hinzu.[3] Wie sich später noch zeigen wird, hat diese rechtliche Entwicklung gravierende Auswirkungen auf die technischen Möglichkeiten der Nutzer zu ihrer eigenen Absicherung.

Durch das Urteil des Bundesverfassungsgerichts aus dem Jahr 2010[4] ist die Vorratsdatenspeicherung zwar gegenwärtig in Deutschland nicht „in Betrieb". Ausdrücklich hebt das Gericht jedoch hervor, dass eine solche Regelung „nicht schlechthin unvereinbar" mit dem Grundgesetz sei. Trotz der Diskussion um Vorratsdatenspeicherung, Quick Freeze oder „Quick Freeze Plus"[5] erscheint eine Wiedereinführung daher gegenwärtig nicht unwahrscheinlich, zumal durch europäische Vorgaben[6] alle Mitgliedsstaaten momentan (noch?) gezwungen sind, eine mindestens sechsmonatige Vorratsdatenspeicherung in nationales Recht umzusetzen. Eine erneute politische Kehrtwende wäre nur dann zu erwarten, wenn der Europäische Gerichtshof, der über die Vereinbarkeit der Richtlinie mit den europäischen Grundrechten bislang noch nicht entschieden hat, zu dem Schluss käme, dass diese einer Vorratsdatenspeicherung generell entgegenstehen, oder wenn sich auf europäischer Ebene eine geänderte politische Meinung etablieren sollte. Zwar ist z.B. in Schweden trotz eines entsprechenden Urteils[7] bislang noch keine Umsetzung der Richtlinie erfolgt und auch in Rumänien hat das dortige Verfassungsgericht die Vorratsdatenspeicherung gestoppt. Ein allgemeines Umschwenken des politischen Denkens ist bislang aber noch nicht erkennbar.

Neben die inzwischen umfassenden Möglichkeiten des Staates auf Informationen seiner Bürger zuzugreifen, treten weitere Möglichkeiten, derartige Daten auszutauschen. Dieser Datenaustausch findet innerstaatlich umfassend statt. Mit der Antiterrordatei ist z.B. eine Datenbank geschaffen worden, in der umfassende elektronische Persönlichkeitsprofile zu einer Person angelegt werden können, auf die anschließend (nicht einmal genau definierte) staatliche Sicherheitsbehörden zugreifen können. Zu diesen rein nationalen Datenübermittlungen kommen internationale hinzu, etwa über den „Grundsatz der Verfügbarkeit" im Rahmen der Europäischen Union, über Finanzdaten im Rahmen des SWIFT-Netzwerks oder über Flugbewegungen im Rahmen des PNR-Austauschs mit den Vereinigten Staaten.[8]

Bezieht man diese Kehrseite zu den datenschutzrechtlichen Regelungen in Deutschland und Europa ein, dann wird deutlich, dass die Kernforderung des Bundesverfassungsgerichts, nach der jeder Bürger wissen können soll, wer welche Informationen über ihn besitzt, damit so eine menschenwürdegerechte Verarbeitung personenbezogener elektronischer Informationen möglich ist, unter diesen Rahmenbedingungen nicht mehr gewährleistet werden kann.

C. Technische Ansätze

Ein Hoffnungsschimmer bleibt für Bürger, die im Rahmen ihres Selbstschutzes auf die technische Umsetzung von Anonymisierungsmaßnahmen setzen. Diese Möglichkeiten werden in der vom FIfF prämierten Arbeit im Rahmen einer kriminalistischen Analyse näher untersucht. Zu unterscheiden sind in diesem Zusammenhang grob drei unterschiedliche Ansätze der Anonymisierung, die sich auch miteinander kombinieren lassen: anonyme Internetzugänge (z.B. über offene WLAN), anonyme Dienstleistungen im Internet (z.B. anonymer Webspace oder anonyme Domainregistrierungen) sowie Anonymisierungsdienste (z.B. offene Proxyserver, zentralisiert arbeitende Anonymisierungsdienste wie JAP/AN.ON/Jondonym und dezentral arbeitende Anonymisierungsdienste wie TOR).

Praktisch sind viele dieser Angebote sehr wirkungsvoll. Bei der Nutzung eines anonymen Internetzugangs, etwa über ein offenes WLAN, lässt sich die Spur später technisch regelmäßig nur bis zum WLAN, nicht aber bis zu der konkreten Person zurückverfolgen. Anonymisierungsdienste, die zudem meist über verschiedene Länder verteilt arbeiten, vertragen selbst die Kollaboration eines oder mehrerer Anbieter mit den Sicherheitsbehörden, ohne dass dadurch die Identität des Anwenders offenbart würde.

Trotz dieser weitreichenden technischen Sicherheit zeigen sich gerade bei den ausgefeilten Anonymisierungsdiensten die dif-

fizilen Wechselwirkungen von Recht und Technik. Durch die Vorratsdatenspeicherung wird den Anbietern derartiger Dienste z.B. eine systemwidrige Speicherpflicht auferlegt, die dazu führen kann, dass Informationen dieses Anbieters zunächst protokolliert und später an die Strafverfolgungsbehörden herausgegeben werden müssen. Da auch andere Länder zwischenzeitlich derartige Speicherpflichten eingeführt haben, hilft auch die verteilte Arbeitsweise von Anonymisierungsdiensten nur noch bedingt. Für einen zuverlässigen Schutz muss ein Nutzer daher sowohl über die technischen Gegebenheiten informiert sein (welches Anonymisierungskonzept schützt welche Daten unter welchen Umständen?) als auch über die rechtlichen Aspekte (durch welche Länder werden die Daten geleitet, welche Speicherpflichten herrschen dort und unter welchen Umständen werden diese Informationen mit anderen Ländern geteilt?).

III. Ausblick

Aufgrund der dynamischen Entwicklung sowohl im Recht als auch in der Technik gibt es keine „einzig wahre" oder „stets sichere" Lösung für eine Anonymisierung. Lösungen, die heute uneingeschränkt empfehlenswert sind, können schon morgen gefährliche Lücken aufweisen, sei es durch neue Speicherpflichten, durch eine falsch verstandene technischen Schutzfähigkeit oder durch eine bislang nicht bekannte Sicherheitslücke. Echte Anonymität wird daher wenigen Experten vorbehalten bleiben.

Möglicherweise sind die Personen, die sich sowohl mit der Technik als auch der rechtlichen Entwicklung am intensivsten auseinandersetzen, gerade diejenigen, deretwegen die Schraube rechtlicher Einschränkungen in letzter Zeit immer weiter gedreht wurde: Terroristen und andere organisiert arbeitende Straftäter, denen der Schutz ihrer Identität und Handlungen aus naheliegenden Gründen besonders am Herzen liegt. Ihnen kann weder mit der gegenwärtigen Gesetzeslage noch mit weiteren Verschärfungen beigekommen werden, denn digitale Daten lassen sich stets so verändern und manipulieren, dass sie von keiner technischen Kontrolle erfasst werden können. Zudem stehen ihnen auch illegale Möglichkeiten offen, die „normalen" Bürgern verwehrt bleiben, etwa die Nutzung von gehackten Rechnern, bei denen sicher ist, dass dort keine weiteren Protokollierungsmaßnahmen greifen.

Lücken in der Strafverfolgung lassen sich daher nur dann vollständig vermeiden, wenn der Absender einer Nachricht, der Empfänger und auch der gesamte Weg dazwischen lückenlos überwacht werden. In einem Rechtsstaat wird das allerdings nicht möglich sein. Verfolgungsfreie Räume sind daher hinzunehmen – im digitalen Lebensraum ebenso wie in der „realen" Welt. Kritikern scheint der Weg zu einer solchen *Orwell'schen* Totalüberwachung dennoch nicht mehr weit. Die Leidtragenden sind daher die rechtstreuen Bürger, denn sie müssen damit leben, dass ihre elektronischen Handlungen umfassend protokolliert und gespeichert werden, selbst wenn sie sich legal verhalten.

Bereits jetzt deuten erste Anzeichen darauf hin, dass es durch die immer weiter voranschreitenden Datensammlungen – sowohl des Staates als auch privater Akteure – in der Bevölkerung zum oft zitierten *chilling effect* kommt, dass Menschen also verunsichert und gehemmt in ihrem Umgang mit modernen Kommunikationsmedien reagieren und aus Überkonformität bestimmte Handlungsweisen von vornherein unterlassen. In einer (allerdings nicht repräsentativen) Umfragen gaben die Befragten zum Beispiel an, Kontakte mit Angehörigen bestimmter Staaten aus Angst vor staatlichen Verdächtigungen nicht weiter zu pflegen oder politische Informationen nicht mehr online abzurufen, um zu verhindern, dass ihre Einstellung bekannt wird.[9]

Um derartige Einschüchterungseffekte zu verhindern und einen Schutz für Bürgerinnen und Bürger für Handlungen im Internet dauerhaft gewährleisten zu können, ist sowohl eine technisch wirksame Anonymisierung als auch ein rechtlicher Rahmen erforderlich, der dies nicht nur duldet, sondern vielmehr sicher verankert und aktiv fördert. Hierzu soll die Arbeit einen Beitrag leisten, indem sie dem Gesetzgeber Denkanstöße gibt und den Nutzern eine Handreichung für den Umgang mit Anonymisierungslösungen zur Verfügung stellt.

Anmerkungen

1 Brunst, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen. Zum Spannungsfeld zwischen einem Recht auf Anonymität bei der elektronischen Kommunikation und den Möglichkeiten zur Identifizierung und Strafverfolgung. Berlin 2009.

2 Vgl. http://www.heise.de/newsticker/meldung/Oesterreich-bereitet-Kill-Switch-fuer-das-Internet-vor-2-Update-1181448.html.

3 Die Online-Durchsuchung zielt auf den umfassenden heimlichen Zugriff auf den Rechner des Verdächtigen ab. Die sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) richtet sich hingegen „nur" auf das Abgreifen von Kommunikationsinhalten bevor diese verschlüsselt oder nachdem diese auf dem Rechner entschlüsselt wurden. Beiden Maßnahmen geht also ein heimliches Eindringen in den Rechner eines Verdächtigen voraus. Vgl. hierzu näher Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 852 ff. und 884 ff.

4 http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html.

5 Vgl. http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-Schaar-schlaegt-Quick-Freeze-Plus-vor-1135898.html.

6 Richtlinie 2006/24 EG des Europäischen Parlaments und des Rates vom 15.03.2006.

7 Vgl. http://taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/trotzige-schweden/.

8 Im Rahmen des Passenger Name Records (PNR) Austauschverfahrens erhalten die Vereinigten Staaten umfassende Informationen über bestimmte Flugbewegungen. Vgl. hierzu näher die Dokumentenübersicht unter http://www.statewatch.org/eu-pnrobservatory.htm.

9 Vgl. http://www.vorratsdatenspeicherung.de/content/view/193/79.

Jens Jacobi

FIfF-Studienpreis 2010
2. Preis

Ein Rollenspiel zum Datenschutz in Netzwerken

Vor dem Hintergrund der Online-Durchsuchung, der zunehmenden Videoüberwachung öffentlicher Plätze und der kurz zuvor in Kraft getretenen Gesetze zur Speicherung der Telekommunikations-Verkehrsdaten (der „Vorratsdatenspeicherung") entstand im Mai 2008 eine schriftliche Hausarbeit im Rahmen der Zweiten Staatsprüfung für das Lehramt an Gymnasien und Gesamtschulen in Nordrhein-Westfalen, die der verbreiteten Mentalität des „Wer nichts zu verbergen hat, der hat auch nichts zu befürchten" entgegenwirken und für den Wert des Schutzes der Privatsphäre und anderer schützenswerter Bereiche sensibilisieren sollte.

Da bereits vermutet wurde, dass die Vorratsdatenspeicherung (zurecht, wie sich später herausstellte – vgl. *http://www.vorratsdatenspeicherung.de/content/view/46/42/lang,de/*) der verfassungsrechtlichen Prüfung nicht standhalten würde, sollte in der Hausarbeit die Datenspeicherung in Netzwerken ganz allgemein im Vordergrund stehen, wobei als Ansatzpunkt die Lebenswirklichkeit der Schülerinnen und Schüler öffentlicher Schulen dienen sollte, denn auch bei der Internetnutzung in Schulen fallen Verkehrsdaten an, die etwas über die Inhalte der Kommunikation der Nutzer aussagen können.

Um nicht lediglich mit dem sprichwörtlichen „erhobenen Zeigefinger" auf ein Missbrauchspotential der persönlichen Daten hinzuweisen, sollte ein *konfrontativer Zugang* gewählt werden, der den Schülerinnen und Schülern die Auswirkungen eines fehlenden Datenschutzes ganz persönlich erfahren lässt. Es wurde ein Konzept entwickelt, das das Sammeln der Daten verdeutlichen und Betroffenheit durch eine offensichtlich missbräuchliche Nutzung der Daten hervorrufen soll, dabei jedoch nicht die persönlichen Daten der Schülerinnen und Schüler offen legt.

Als Ausweg bot es sich an, ein Rollenspiel zu entwickeln, in welchem die Schülerinnen und Schüler einer Rollenvorgabe entsprechend handeln sollten, wodurch zwar „sensible" Verkehrsdaten generiert wurden, diese jedoch keine Rückschlüsse über die involvierten Personen erlaubten, da sie nur im Rahmen einer Rollenvorgabe agierten.

Die Rollenbeschreibungen sind so konstruiert, dass Einblicke in die Privat- bzw. Intimsphäre der Personen, die durch die Rollen dargestellt werden, möglich sind, bzw. dass ein Persönlichkeits- oder Interessenprofil erstellt werden kann. Als Nebeneffekt wird die Existenz von Vereinen und Institutionen wie *Exit* (Ausstiegsberatung aus der rechtsextremen Szene) oder Drogenberatungen ins Bewusstsein der Schülerinnen und Schüler gerufen.

Zu den weiteren gewählten Szenarien gehören *unter anderem*:

- Jemand gerät (zu Unrecht) in den Verdacht, eine Urheberrechtsverletzung begangen zu haben.
- Ein Schüler äußert im Internet „vernichtende Kritik" an einem Lehrer, welcher den „Schuldigen" herausfinden möchte.
- Bei der Analyse der Log-Dateien des Proxy-Servers kann man darüber „stolpern", dass sich Mitschülerin XY über Geschlechtskrankheiten informiert hat – warum bloß?

Details zu den beschriebenen Szenarien und der Konstruktion der Rollen können in der schriftlichen Hausarbeit nachgelesen werden, welche den vollständigen Titel „Entwicklung eines Konzepts zur Umsetzung des Unterrichtsgegenstands Netzwerke unter Einbeziehung datenschutzrechtlicher Fragen vor dem Hintergrund der informatischen Bildung" trägt und über den BSCW-Server der Schulen und des Studienseminars der Stadt Hamm heruntergeladen werden kann *(http://www.ham.nw.schule.de/pub/bscw.cgi/1493228).*

Bevor der Ablauf des Rollenspiels und die einzelnen Szenarien und Rollen beschrieben werden, geht es in der Arbeit zunächst um die Einordnung des beschriebenen Konzepts vor dem Hintergrund informatischer Bildungstheorien und -konzepte. Anschließend wird ein Überblick über die bereits bestehenden Umsetzungsvorschläge und Unterrichtskonzepte zu den Inhalten „Netze" und „Datenschutz" gegeben – von den Richtlinien und Lehrplänen des Landes Nordrhein-Westfalen bis hin zu fertig entwickelten Unterrichtsmaterialien wie dem Planspiel „Jugend im Datennetz" und seinen Weiterentwicklungen, welche eine maßgebliche Inspirationsquelle für das in der Hausarbeit beschriebene Rollenspiel darstellten.

Weitere Aspekte der Hausarbeit sind die Lernziele, die mithilfe des Rollenspiels erreicht werden sollen, die erforderlichen Lernvoraussetzungen und die Möglichkeiten zur Einbettung des Rollenspiels in Unterrichtsreihen zu Netzen oder zum Datenschutz.

Jens Jacobi

Jens Jacobi, Jahrgang 1981, ist seit 2009 Lehrer für Informatik und Physik am Albert-Martmöller-Gymnasium in Witten. Nach seinem Ersten Staatsexamen im Jahr 2006 an der Universität Dortmund war er von Februar 2007 bis Januar 2009 Referendar am Städtischen Gymnasium in Selm bzw. am Studienseminar Hamm.

Andere Abschnitte beschäftigen sich mit der Rechtslage sowie mit den technischen Anforderungen (im Wesentlichen muss ein Proxy-Server vorhanden sein, auf dessen Log-Dateien man Zugriff hat).

Das Rollenspiel kann nach den eigenen Bedürfnissen weiterentwickelt werden, da es im Rahmen einer Creative Commons-Lizenz („Namensnennung, keine kommerzielle Nutzung, Weitergabe unter gleichen Bedingungen 3.0 Unported") entwickelt wurde. Rückmeldungen und Verbesserungsvorschläge sind willkommen (z. B. per Mail an *jjenspatri@seminar.ham.nw.schule.de*).

Das FIfF verleiht auch in diesem Jahr den

FIfF-Studienpreis 2011

für herausragende Abschlussarbeiten aus dem Bereich Informatik und Gesellschaft.

Wir wollen damit Studierende sowie Wissenschaftlerinnen und Wissenschaftler in der Qualifikationsphase zur fundierten und differenzierten Auseinandersetzung mit den gesellschaftlichen Auswirkungen der Informatik ermutigen.

Das FIfF möchte mit der Einrichtung dieses Studienpreises herausragende Leistungen des wissenschaftlichen Nachwuchses in diesem Bereich würdigen und die Aufmerksamkeit der Öffentlichkeit auf das Thema der Arbeit sowie die besonderen Leistungen des Autors bzw. der Autorin lenken.

Wir laden dazu ein, geeignete Arbeiten bis 31. Mai 2011 einzureichen.

Das Preisgeld beträgt:

- 1. Preis: €333
- 2. Preis: €222
- 3. Preis: €111

Es können Qualifikationsarbeiten (Bachelor-, Master-, Diplomarbeiten oder Dissertationen) eingereicht werden, die in den letzten zwei Jahren vor Nominierungsschluss abgeschlossen wurden. Die Ausschreibung bezieht sich zwar schwerpunktartig auf Abschlussarbeiten in Informatik, jedoch wird auch zur Einreichung thematisch einschlägiger Arbeiten anderer Fachgebiete ausdrücklich eingeladen.

Einreichungen bitte bis zum 31. Mai 2011 an:

FIfF-Geschäftsstelle
– Studienpreis 2011 –
Goetheplatz 4
28203 Bremen

oder per E-Mail an *studienpreis@fiff.de*. Weitere Details unter *http://www.fiff.de/studienpreis*.

Der Preis wird in einer Feierstunde im Rahmen der **FIfF-Jahrestagung am Samstag, 12. November 2011 in München** verliehen.

Rolf Gössner

Rechtsstaatswidrige Dauerüberwachung

Vier Jahrzehnte unter geheimdienstlicher Beobachtung des Verfassungsschutzes

Nach 38 Jahren geheimdienstlicher Überwachung und fünf Jahren Verfahrensdauer hat das Verwaltungsgericht Köln am 3. Februar 2011 in dem Gerichtsverfahren Dr. Gössner ./. Bundesrepublik Deutschland ein sensationelles Urteil gesprochen: Die Dauerüberwachung des Klägers durch den bundesdeutschen Inlandsgeheimdienst, konkret: durch das beklagte Bundesamt für Verfassungsschutz (BfV), und die während dieses Zeitraums erfolgte Erhebung und Speicherung von personenbezogenen Daten über den Kläger waren von Anfang an bis zur Beendigung der Beobachtung Ende 2008 rechtswidrig. Die Beklagte trägt die Kosten des Verfahrens.

Dieses Urteil ist eine herbe Niederlage für den Inlandsgeheimdienst, es bescheinigt ihm einen rekordverdächtigen, vier Jahrzehnte währenden Rechtsbruch. Die Internationale Liga für Menschenrechte fordert nach der skandalösen und rechtswidrigen Langzeitüberwachung und auf Grundlage des vorliegenden Urteils drastische politische und gesetzliche Konsequenzen, vor allem, weil es sich hier um keinen Einzelfall handeln dürfte.

Gössners Anwalt Dr. Udo Kauß (Freiburg) bezeichnet die Entscheidung des Verwaltungsgerichts Köln als „Meilenstein": „Dem Schutz der BürgerInnen vor staatlicher Überwachung wurde nach fünfjährigem Rechtstreit zumindest rückwirkend Geltung verschafft. Die im Prozess vom Bundesamt für Verfassungsschutz für sich in Anspruch genommene Deutungshoheit über das, was in diesem Staat zulässiger Weise gesagt und geschrieben werden darf, ist dem Geheimdienst entzogen worden. Eine schallende Ohrfeige mit hoffentlich nachhaltiger Wirkung für die Erfassungspraxis nicht nur des Bundesamtes für Verfassungsschutz, sondern aller bundesdeutschen Geheimdienste. Das Amt wird seine Beobachtungs- und Erfassungspraxis gründlich ändern müssen."

Dieses Urteil hat nach Auffassung der Internationalen Liga für Menschenrechte über den Einzelfall hinaus grundsätzliche Bedeutung, denn es geht um ein brisantes Problem, das auch andere Publizisten, Rechtsanwälte und Menschenrechtler betrifft: Welche Grenzen sind den kaum kontrollierbaren Nachrichtendiensten und ihren geheimen Aktivitäten gezogen – speziell im Umgang mit Berufsgeheimnisträgern und im Rahmen unabhängiger Menschenrechtsarbeit von Nichtregierungsorganisationen?

Rekordverdächtige Überwachungsgeschichte – aus der Sicht des Betroffenen

In eigener Sache zu reden oder zu schreiben, bedeutet zwangsläufig, persönlich zu werden. Wie inzwischen gerichtsbekannt und nachgewiesen, bin ich seit 1970 fast vier Jahrzehnte lang ununterbrochen vom Bundesamt für VS beobachtet und ausgeforscht worden – eine der längsten dokumentierten Überwachungsgeschichten in der Bundesrepublik. Geheimdienstlich beobachtet wurde ich als Jurastudent, später als Gerichtsreferendar und seitdem ein ganzes Arbeitsleben lang in allen meinen beruflichen und ehrenamtlichen Funktionen – also als Publizist, Buchautor, Rechtsanwalt, Parlamentarischer Berater, Vorstandsmitglied der Internationalen Liga für Menschenrechte, Mitherausgeber des alljährlich erscheinenden *Grundrechte-Reports* und der Zweiwochenschrift *Ossietzky* sowie auch als Mitglied der Jury zur Verleihung des Negativpreises „BigBrotherAward".

Ich erlebe es immer wieder, dass viele Menschen in ungläubiges Staunen verfallen, wenn sie von dieser rekordverdächtigen Überwachungsgeschichte erfahren. Kann das wirklich wahr sein, oder leidet da einer an Verfolgungswahn? Redet der von Stasi-Methoden oder vom bundesdeutschen Rechtsstaat? Und tatsächlich: Womit hat jemand in diesem Land der freiheitlich demokratischen Grundordnung verdient, sein gesamtes Studenten-, Ausbildungs- und Arbeitsleben – vier von sechs Lebensjahrzehnten hindurch – ununterbrochen von einem Geheimdienst beobachtet und ausgeforscht zu werden? Das muss doch gute Gründe im bösen Tun haben. Warum sonst wird ein Bürger dieses Landes quasi als gefährlicher Staats- und Verfassungsfeind einer solch „fürsorglichen Belagerung" (Heinrich Böll) unterzogen?

Tatsächlich geht es um mein gesamtes bewusstes Leben – und um das, was der Verfassungsschutz aus seiner selektiven, ideologisch motivierten Sicht aus diesem Leben macht: Er zeichnet in Personenakten und Schriftsätzen ein aus zeitgeschichtlichen Zusammenhängen herausgerissenes Bild, konstruiert abstruse Anschuldigungen und bedient sich einer geradezu inquisitorischen Beweisführung. Heraus kommt ein denunziatorisches Feind- und Zerrbild, in dem ich mich nicht wieder erkenne und vor dem ich, auf den ersten Blick zumindest, selbst erschrecken würde. Letztlich geht es um die Deutungshoheit über ein politisches Leben, über politisches Handeln und berufliche Kontakte, deren sich der Verfassungsschutz mit seiner obsessiven Gesinnungsschnüffelei und seiner amtlichen Interpretation oder besser: Fehlinterpretation bemächtigte. Nun versuche ich, mir diesen Teil meiner eigenen Lebensgeschichte wieder anzueignen, um die Deutung politischer Vorgänge und Entwicklungen nicht einem letztlich unkontrollierbaren und skandalträchtigen Geheimdienst zu überlassen. Und ich musste mich dabei auch der bangen Frage stellen, was das Wissen um meine Beobachtung und die Negativbewertung durch den Verfassungsschutz mit mir und aus mir gemacht hat, ob sich mein Verhalten dadurch etwa verändert, ob ich mich womöglich schleichend anpasse, Themen oder Kontakte meide – ob also die Schere im Kopf seitdem klammheimlich ihr zerstörerisches Unwesen treibt.

Diese Aufarbeitung und Selbsthinterfragung muss öffentlich geschehen. Denn auch die bundesdeutsche Gesellschaft und ihre kritischen Mitglieder müssen sich angesichts eines solch exemplarischen Falles die dringliche Frage stellen, was all dies für die Meinungs- und Pressefreiheit, für Mandatsgeheimnis und Informantenschutz, für Dialogbereitschaft und Offenheit in diesem Land bedeutet. Insofern handelt es sich um ein brisantes Lehr-

stück in Staatskunde, ein Lehrstück in Sachen Bürgerrechte und Demokratie. Selbstverständlich ist dies kein Einzelfall, schließlich gab und gibt es zahlreiche andere Fälle von Bespitzelung mit zum Teil weit gravierenderen Folgen, und zwar in allen Jahrzehnten seit Bestehen der Bundesrepublik: ob in den Zeiten der Kommunistenverfolgung der 1950er und 60er Jahre, in Zeiten des Deutschen Herbstes der 70er Jahre oder erstarkender politisch-sozialer Bewegungen der 80er Jahre; auch nach dem offiziellen Ende des Kalten Krieges bis heute sind Parteien, Gewerkschaften und politische Organisationen bespitzelt und infiltriert worden. Die Überwachungs- und Skandalgeschichte des Verfassungsschutzes ist jedenfalls ellenlang.

Was wirft mir dieser euphemistisch „Verfassungsschutz" titulierte Geheimdienst durch die Jahrzehnte hindurch eigentlich vor? Zunächst legte er mir meine beruflichen und ehrenamtlichen Kontakte zu angeblich linksextremistischen und „linksextremistisch beeinflussten" Gruppen zur Last. Dazu zählen politische Parteien wie die DKP, Organisationen wie die Rechtshilfegruppe „Rote Hilfe" oder die Vereinigung der Verfolgten des Naziregimes (VVN), aber auch Presseorgane wie *Demokratie und Recht*, *Blätter für deutsche und internationale Politik*, *Geheim*, *junge Welt* oder *Neues Deutschland*, in denen ich neben vielen anderen Medien veröffentliche oder interviewt werde.

Nun, jeder Autor und jeder Referent freut sich über eine treue und kritische Leser- und Zuhörerschaft. Und so nahm ich durchaus mit Genugtuung zur Kenntnis, dass Bedienstete des Bundesamtes über mehrere Beamten-Generationen hinweg zu meinen treuesten Mitlesern und Mithörern gehörten – leider auch zu den verständnislosesten und böswilligsten.

So wurde durch die Jahrzehnte hindurch alles registriert, was ich von mir gegeben habe: ob in gedruckter Form, als Artikel oder im Interview. Selbst Berichte über mich und meine Bücher wurden gesammelt und mir zur Last gelegt, wenn sie in besagten inkriminierten Medien erschienen sind. Desgleichen interessierte sich der Geheimdienst für meine Äußerungen, wenn ich referierte und diskutierte, etwa in öffentlichen Veranstaltungen und auch geschlossenen Sitzungen. Das Bundesamt identifizierte mich dabei unzulässigerweise mit den Medien, in denen ich publizierte, mit den Veranstaltern, bei denen ich referierte und Diskussionen führte, und mit meinen Mandanten, die ich beraten habe.

Vorwurf »Kontaktschuld«

Eigene verfassungsfeindliche Ziele und Beiträge wurden mir zunächst nicht unterstellt. Also: Nicht was ich sagte oder schrieb, war für die Beobachtung entscheidend, sondern in welchem politischen Umfeld dies geschah. Meine diesbezüglichen Kontakte verdichtete das Amt zu einem regelrechten Kontaktprofil, das mir als eine Art „Kontaktschuld" angelastet wird. Hieraus folgert das BfV schließlich messerscharf eine „nachhaltige Unterstützung" solcher nicht verbotenen, aber als „linksextremistisch" geltenden Personenzusammenschlüsse und Presseorgane, die ich – so wörtlich –, als „prominenter Jurist" aufgewertet und gesellschaftsfähig gemacht haben soll.

Dabei haben die Verfassungsschützer alle Not, die jahrzehntelange Überwachung einer Einzelperson, die in keiner politischen Organisation oder Partei organisiert war, nur auf deren berufliche Kontakte zu stützen und mit „nachhaltiger Unterstützung" zu rechtfertigen. Deshalb verstieg sich das Bundesamt zu folgender abenteuerlichen Konstruktion: „Dabei agiert er ganz bewusst nicht als Mitglied einer offen extremistischen Partei oder Organisation. Nicht etwa, weil er sich von den verfassungsfeindlichen Zielen der unterstützten Organisationen distanziert, sondern weil er so seine Glaubwürdigkeit nach Außen als vermeintlich unabhängiger Experte zu wahren versucht."

Darin steckt die diffamierende Behauptung, ich sei seit Jahrzehnten taktisches Nichtmitglied diverser, durchaus disparater extremistischer Parteien oder Organisationen – sozusagen als ideeller Gesamtlinksextremist.

Doch dabei blieb es nicht. Das Bundesamt ließ im Laufe der Zeit die Anschuldigungen gegen mich stufenweise eskalieren – so mit dem Vorwurf, ich sei nicht nur Unterstützer, sondern zeitweise doch auch Mitglied in „linksextremistischen Personenzusammenschlüssen" gewesen: nämlich im Sozialdemokratischen/Sozialistischen Hochschulbund (SHB) und in der Redaktion des geheimdienstkritischen Magazins *Geheim*. Die letzte Eskalationsstufe: Das BfV zieht auch das von mir Geschriebene und Gesagte in Misskredit und setzt es dem Verdacht der Verfassungsfeindlichkeit aus – neue Vorwürfe, die zuvor keinerlei Rolle gespielt hatten, die aber nun nachträglich die unglaubliche Überwachungsgeschichte zusätzlich rechtfertigen sollen. Mit meiner „diffamierenden" Kritik der bundesdeutschen Sicherheitspolitik, der Sicherheitsorgane und besonders des Verfassungsschutzes, darüber hinaus mit meiner Kritik am KPD-Verbot und an den Berufsverboten (die es in der Bundesrepublik nach offizieller Lesart nie gab), so der Geheimdienst-Tenor, wolle ich den Staat wehrlos machen und den linksextremistischen Bestrebungen und der revolutionären Umwälzung schutzlos ausliefern. Außerdem wird mir meine fehlende Distanzierung von der DDR, der Stasi, der UdSSR, dem Gulag und allen Verbrechen des Kommunismus zur Last gelegt – gleichzeitig werde ich der einseitigen Kritik am Westen bezichtigt. Brauchen wir dazu einen Inlandsgeheimdienst? Das BfV maßt sich damit eine Deutungshoheit über meine Texte (und auch über Nichtgeschriebenes) an und übt sie in geradezu inquisitorischer Weise aus – etwa nach dem Motto: *„Was der Kläger da äußert, klingt zwar auf den ersten Blick ganz demokratisch – aber gemeint hat er etwas ganz Anderes"*. Diese ideologischen Textinterpretationen führen weit zurück in die tiefsten 1960er/70er Jahre des Kalten Krieges, dessen überwunden geglaubter Geist hier traurige Urstände feiert.

Von meiner Überwachung habe ich erfahren, weil ich 1996 beim Bundesamt einen Antrag auf Auskunft über die dort zu meiner Person gespeicherten Daten gestellt hatte. Als Antwort bekam ich ein Personendossier mit einer Sündenliste – Artikel, Interviews und Reden in den falschen Zeitungen oder Veranstaltungen –, die bis 1970 zurückreichte. Etwa alle zwei Jahre fragte ich erneut nach, um das jeweils neueste Sünderregister kennenzulernen, das mir dann auch prompt zugeschickt wurde.

Da die Überwachung munter weiterging, auch in Zeiten der rot-grünen Bundesregierung, reichte ich Ende 2005 über meinen Freiburger Anwalt Dr. Udo Kauß beim zuständigen Verwaltungsgericht Köln Klage gegen die Bundesrepublik Deutschland

ein, um vollständige Einsicht in meine Personenakten zu bekommen sowie die jahrzehntelange Überwachung gerichtlich für rechtswidrig erklären zu lassen.

Der fünf Jahre dauernde Prozess hat einiges zu Tage gefördert. Das Gericht hat das Bundesamt dazu verdonnert, meine gesamte Personenakte seit 1970 bis 2007 vorzulegen, was inzwischen geschehen ist – zum überwiegenden Teil allerdings mit geschwärzten Textstellen; ganze Seiten sind entnommen. Von allen über 2.000 mir vorgelegten Aktenseiten sind circa 1.750 Seiten ganz oder teilweise unleserlich oder manipuliert oder gar nicht vorgelegt worden, also etwa 85 Prozent; nur rund 15 Prozent sind offen und vollständig lesbar.

Abb. 1: Solche Akten sind Grundlage für die richterliche Wahrheitsfindung im verwaltungsgerichtlichen Verfahren »Dr. Goessner ./. Bundesrepublik Deutschland«

Die Verheimlichung ganzer Aktenteile geht auf umfangreiche Sperrerklärungen des Bundesinnenministeriums als oberster Aufsichtsbehörde des Bundesamtes zurück. Begründung: Würde ihr Inhalt bekannt, könnte dies dem „Wohl des Bundes oder eines Landes Nachteile bereiten"; die Funktionsfähigkeit des VS würde beeinträchtigt, wenn verdeckte Arbeitsweise und operative Interessen bekannt werden (das nennt sich dann „Ausforschungsgefahr"). Und die Geheimhaltung diene in erster Linie dem Schutz der Informationsquellen, deren Identität nicht enttarnt werden dürfe („Quellenschutz"); denn eine Enttarnung dieser „Quellen" könne zu einer „Gefährdung von Leben, Gesundheit oder Freiheit" von V-Leuten, Hinweisgebern und VS-Bediensteten führen. Als ob die – wohl von mir und meinesgleichen – Repressalien zu befürchten hätten.

Höherrangiges Geheimhaltungsinteresse

Gegen diese Aktenverweigerung klagte ich parallel vor dem Bundesverwaltungsgericht, um Sperrerklärungen und Geheimhaltung in einem sogenannten In-camera-Verfahren überprüfen zu lassen. Dabei handelt es sich um ein rechtsstaatlich hoch problematisches Geheimverfahren – eine zwangsläufige Folge von Geheimdienstarbeit, die sich bis hinein in justizielle Verfahren verlängert. Nach ihrer Auswertung der gesperrten Aktenteile in geheimer Sitzung in einem abhörsicheren Raum und ohne meine Mitwirkung kamen die höchsten Verwaltungsrichter zu dem Ergebnis, dass diese Aktenteile weiterhin aus Gründen des Quellenschutzes, der Ausforschungsgefahr und des Staatswohls geheim gehalten werden müssten. Somit konnte das Verwaltungsgericht Köln nur auf dieser äußerst eingeschränkten Beweisgrundlage seine Entscheidung über Rechtmäßigkeit oder Rechtswidrigkeit der Dauerbeobachtung treffen. Und das soll rechtsstaatlich sein?

Trotz dieser höchstrichterlich abgesegneten amtlichen Beweismittelunterdrückung im staatlichen Geheimhaltungsinteresse ist die verbleibende Dokumentensammlung dennoch recht aufschlussreich. So hat mich sehr erstaunt, wie viele Behörden, andere Stellen und Personen sich in meinem Fall als denunziatorische Zuträger für den Verfassungsschutz betätigt haben und wie viele Spitzelberichte über meine Referate und sonstigen Aktivitäten angefertigt worden sein müssen.

Wenige Tage vor dem ersten Verhandlungstermin vor dem Verwaltungsgericht Köln Ende 2008 teilte das BfV dem Gericht

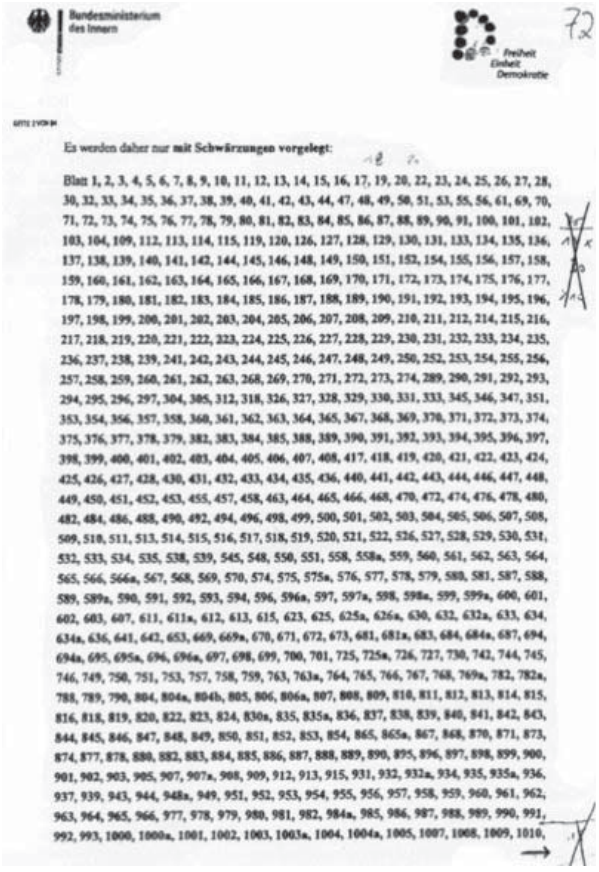


Abb. 2: Auszug aus dem Sperrvermerk des Bundesinnenministeriums

überraschend mit, dass meine Beobachtung „nach aktuell erfolgter Prüfung“ durch das Bundesinnenministerium und das Bundesamt eingestellt worden sei und die zu mir erfassten Daten „löschungsreif“ seien und ab sofort bis zum rechtskräftigen Abschluss des Verfahrens gesperrt würden, also nicht mehr verwendet werden dürfen. Ohne Klage wäre ein Ausstieg aus dieser Überwachungsgeschichte wohl kaum erfolgt, so dass ich womöglich weiterhin, bis ins hohe Rentenalter, unter Beobachtung stünde. Ob man jedoch der lapidaren Mitteilung Glauben schenken kann, bleibt erstmal abzuwarten, zumal eine Wiederaufnahme der Überwachung jederzeit möglich wäre.

Noch wenige Monate vor der Einstellung hatte das Amt auf meiner weiteren Beobachtung bestanden – selbst auf die besorgte Nachfrage des Vorsitzenden Verwaltungsrichters hin, ob meine zwischenzeitlich erfolgte Wahl zum Stellvertretenden Richter am Staatsgerichtshof der Freien Hansestadt Bremen nicht daran etwas ändern müsse. Nein, erklärte das Bundesamt forsch, auch Richter könnten unter gewissen Voraussetzungen, die bei mir vorlägen, beobachtet werden – trotz ihrer verfassungsrechtlich garantierten Unabhängigkeit. Also ein vom Verfassungsschutz beobachteter „Verfassungsfeind“ als Verfassungsrichter? Bei so viel Widersprüchlichkeit kann man leicht die Verfassung verlieren.

Erst kurz vor der mündlichen Verhandlung kam dann die Kehrtwende. Einer der Gründe, weshalb ich jetzt plötzlich nicht mehr beobachtet werden müsse, war höchst hörenswert: Die Bedrohungslage in der Bundesrepublik habe sich geändert, die knappen Ressourcen müssten nun für andere Schwerpunkte eingesetzt werden. Nach 38 Jahren, in deren Verlauf die DDR unter- und der Kalte Krieg zu Ende ging sowie der internationale Terrorismus als neue Gefahr erkannt wurde, gibt es also jetzt plötzlich eine neue Bedrohungslage, die eine Umorientierung und Umschichtung im BfV erforderlich macht! Wahrlich ein Fall für den Bundesrechnungshof wegen des Verdachts auf jahrzehntelange Verschwendung öffentlicher Gelder.

Im Übrigen behauptete das Amt, ich sei nicht mehr so viel in linksextremistischen Kreisen unterwegs. Die teils merkwürdige, teils unglaubwürdige, teils lächerliche Begründung der Beobachtungseinstellung lässt eher darauf schließen, dass nach einem Notausstieg gesucht wurde, um eine unhaltbare Situation zu beenden. Jedenfalls frage ich mich, was sich an meiner Arbeit, meinen beruflichen Aktivitäten und (inkriminierten) beruflichen Kontakten derart änderte, dass es nach vier Jahrzehnten zu einer solchen Kehrtwende kam. Habe ich doch immer noch die gleichen oder ähnlichen Kontakte wie bisher – sowohl in höchste staatliche Ämter und Funktionen als auch in Bereiche, die dem Verfassungsschutz als „linksextremistisch/beeinflusst“ gelten, die ihm also weiterhin missfallen müssten und ihn zu erneuter Überwachung reizen könnten. Eher sind noch weitere, auch internationale Kontakte hinzugekommen. Und auch meine Texte sind – so hoffen ich und meine Leserschaft – keinesfalls harmloser geworden.

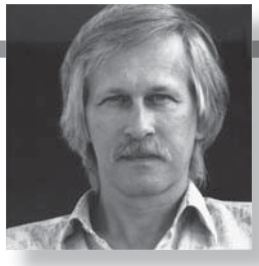
Es war schon ein eigenartiges Gefühl, nach so langer Zeit fürsorglicher Dauerüberwachung plötzlich zu erfahren, dass man nicht mehr unter geheimdienstlicher Beobachtung stehe, sozusagen außer Kontrolle und staatsschutzlos. Doch ich fühlte mich zunächst erleichtert und war erfreut. Denn ich hatte immer damit rechnen müssen, dass es letztlich keine Vertraulichkeit mehr gab, ein Umstand, der auch mein gesamtes soziales Umfeld erheblich irritierte; wie sich herausstellte, war diese Irritation nicht unberechtigt. Ein ganzes Netzwerk von V-Leuten, Informanten und anderen Zuträgern versorgte den Verfassungsschutz mit unzähligen Informationen, die von Bediensteten des Bundesamtes fleißig gesammelt, gespeichert und bewertet wurden – im diensteifrigen Bemühen, ein Phantom-Persönlichkeitsbild von mir zu zeichnen.

Ich musste immer befürchten, dass bei meiner publizistischen Arbeit meine oft heiklen Recherchen und Kontakte zu bestimmten Informanten ausgespäht und meine Informanten dadurch gefährdet würden. Und tatsächlich habe ich mehrfach erlebt, dass meine Kontakte etwa mit dem einen oder anderen Informanten aus den Polizei- oder Geheimdienst-Apparaten ausgeforscht und observiert wurden – die jeweiligen Whistleblower kannten schließlich die Zuträger ihrer Behörde. Um meine Informanten dennoch so gut wie möglich zu schützen, bedurfte es oft anstrengender Klimmzüge. In Einzelfällen mussten Kontakte deshalb unterbleiben oder abgebrochen werden.

Seid Sand, nicht Öl im Getriebe …

Auch als Rechtsanwalt und Strafverteidiger musste ich mit geheimdienstlicher Ausforschung rechnen. Seit meine geheimdienstliche Überwachung nicht mehr zu verheimlichen war, sah ich mich genötigt, meine Mandanten darüber aufzuklären. Ich hatte immer wieder mit besorgten Ratsuchenden zu tun, die verständlicherweise Probleme hatten, sich mir unbefangen anzuvertrauen. Manche sind abgesprungen; wie viele den Kontakt zu mir deshalb erst gar nicht suchten, kann ich selbstverständlich nicht ergründen.

Rolf Gössner



Dr. **Rolf Gössner** ist Vizepräsident der Internationalen Liga für Menschenrechte (Berlin). Er lebt als Rechtsanwalt, Publizist und parlamentarischer Berater in Bremen. Seit 2007 stellvertretendes Mitglied des Bremischen Staatsgerichtshofs der Freien Hansestadt Bremen sowie Mitglied/stellvertretender Sprecher der Deputation für Inneres der Bremischen Bürgerschaft (Landtag) und der Stadtbürgerschaft. Autor zahlreicher Bücher und Aufsätze zum Thema „Innere Sicherheit“ und Bürgerrechte, zuletzt: „Menschenrechte in Zeiten des Terrors. Kollateralschäden an der ‚Heimatfront‘“ (Hamburg 2007).

Das Mandatsgeheimnis und der Informantenschutz waren jedenfalls so nicht mehr durchgängig zu gewährleisten, die verfassungsrechtlich geschützten Vertrauensverhältnisse zwischen Anwalt und Mandant sowie zwischen Journalist und Informant waren erschüttert, meine Berufsfreiheit und berufliche Praxis damit mehr als beeinträchtigt.

Dass ein Geheimdienst wie der Verfassungsschutz über vier Jahrzehnte unkontrolliert und rechtswidrig eine unabhängige Einzelperson, zudem einen Berufsgeheimnisträger beobachten, personenbezogene Daten erfassen, sammeln, auswerten und übermitteln kann und dass er dann auch noch den größten Teil der Personenakte geheim halten darf, beweist die These, dass es sich letztlich um eine demokratieunverträgliche Institution handelt, für die das Prinzip demokratischer Transparenz und Kontrollierbarkeit praktisch nicht gilt.

Der Vorsitzende Richter hat in der zweiten mündlichen Verhandlung festgestellt, dass in dem Verfahren „zwei Denkwelten" aufeinander prallten. Das Gericht problematisierte dabei auch, dass durch die einseitige Auswahl des erfassten Materials durch den Verfassungsschutz „zwangsläufig ein falsches Bild" vom Kläger und von dessen beruflichen und rechtspolitischen Aktivitäten entstehen müsse. Schon deshalb hätte ich ein berechtigtes „Rehabilitierungsinteresse", dem das Urteil in vollem Umfang entspricht.

In einer persönlichen Stellungnahme habe ich in der letzten mündlichen Verhandlung vor Gericht zum Abschluss mein Bedauern zum Ausdruck gebracht, dass durch diese unsinnige, geradezu absurde Überwachungsgeschichte so viel Lebenszeit und -kraft vergeudet wurde und dass zwei Gerichte mit aufwändigen Verfahren belästigt werden mussten. Aber dieser Aufwand ist leider notwendig gewesen, um wenigstens zu versuchen, ein wenig Licht ins Dunkel zu bringen und solch ausufernde Geheimdiensttätigkeit künftig zu unterbinden.

Meines Erachtens prallen in diesem Streitfall tatsächlich zwei unterschiedliche Denkwelten, politische Kulturen und Grundhaltungen aufeinander: auf der einen Seite die Kultur oder eher Unkultur des Ausspähens, Stigmatisierens und Ausgrenzens im Namen von Sicherheit und Staatswohl, auf der anderen die Kultur der demokratischen Transparenz, des offenen und kritischen Dialogs im Namen von Demokratie und Freiheit, den ich in allen meinen beruflichen und ehrenamtlichen Tätigkeiten suche und führe – nicht selten gegen den Mainstream und gesellschaftliche Ausgrenzungsbereitschaft und ohne allzu große politische Berührungsängste; gerade auch gegenüber Personen und Gruppen, die nicht verboten sind, ihrerseits aber unter Beobachtung des Verfassungsschutzes stehen und die allein deswegen in den Augen vieler als verfemt oder geächtet gelten und mit denen man tunlichst nicht diskutiert – etwa bestimmte sozialistische, kurdische oder iranische Gruppen, islamische Gemeinschaften, Muslime oder sonstige Migranten, die durch den staatlichen Antiterrorkampf ihrerseits unter Generalverdacht geraten sind.

Ich kann es jedenfalls nicht hinnehmen, dass verfassungskonforme und bürgerrechtliche Kräfte als Unterstützer extremistischer Kreise stigmatisiert werden, sobald sie in ihrer Arbeit bestimmte politische Spektren nicht ausgrenzen und gesellschaftlich isolieren, sondern sie bewusst in den politisch-demokratischen Willensbildungsprozess mit einbeziehen. Eine offene und liberale Demokratie lebt von Kritik und kontroverser politischer Diskussion auch und gerade mit Andersdenkenden – und nichts anderes ist mir letztlich vorzuwerfen. Es ist Gift für eine demokratische Gesellschaft, wenn solches unter geheimdienstliche Beobachtung und Kuratel gestellt wird.

Ich möchte im Zusammenhang mit meiner Überwachungsgeschichte an einen Ausspruch des Schriftstellers und Hörspielautors Günther Eich erinnern, den ich in meinem Abitur 1967 mit Bedacht als Aufsatzthema ausgewählt hatte und der in gewisser Weise zu meinem Lebensmotto wurde:

„Seid unbequem, seid Sand,
nicht Öl im Getriebe der Welt."

Aktualisierte und überarbeitete Fassung eines Vortrags des Autors, den er am 3.10.2010 im Haus der Demokratie und Menschenrechte in Berlin gehalten hat. Erstmals erschienen in der Zweiwochenschrift für Politik / Kultur / Wirtschaft „OSSIETZKY" Nr. 22 v. 30.10.2010: Die Akte Gössner und andere Geheimdienst-Geheimnisse: „Verfassungsschutz in Aktion". Darin weitere Beiträge zum Thema Geheimdienste von Ulla Jelpke, Manfred Wekwerth, Wolfgang Wippermann und Eckart Spoo.

Ossietzky
Zweiwochenschrift
für Politik / Kultur / Wirtschaft

www.sopos.org/aufsaetze/4cd2964854b77/1.phtml

Näheres zu Ossietzky, einzelnen Ausgaben und Texten unter: www.ossietzky.net sowie www.sopos.org/ossietzky

»Der Krieg ist ein besseres Geschäft als der Friede. Ich habe noch niemanden gekannt,
der sich zur Stillung seiner Geldgier auf Erhaltung und Förderung des Friedens geworfen hätte.
Die beutegierige Canaille hat von eh und je auf Krieg spekuliert.«

Carl von Ossietzky
in der Weltbühne vom 8. Dezember 1931

Wolfgang Hesse

Milliarden für Schilda 21

Ein Monsterprojekt, Bürgerwut, Schlichtung und wie weiter?

„Stuttgart 21" hat die bundesdeutsche Politik-Landschaft im Jahr 2010 bewegt wie kaum ein innenpolitisches Thema in den letzten Jahren. Wie konnte es dazu kommen, dass ein (scheinbar) lokales, vor 15 Jahren beschlossenes Verkehrsprojekt die gesamte Republik über Wochen und Monate hinweg in Atem halten, Zigtausende auf die Straße und Millionen vor die Fernsehschirme bringen konnte? Was steckt hinter dem Projekt, warum betrifft es weit mehr als ein paar Stuttgarter Bürger und was können wir aus dem Schlichtungsprozess für die Zukunft unserer Demokratie lernen? Und schließlich: Was ist daran von speziellem Interesse für uns als Informatiker? Diesen Fragen möchte ich in dem folgenden Artikel nachgehen.

Mythen zu „Stuttgart 21"

Zunächst sollen das Projekt, seine Vorgeschichte und einige daran geknüpfte Mythen beleuchtet werden.

Mythos 1: „Stuttgart 21" ist ein lokales Projekt. Die Projektidee stammt aus den 1990-er Jahren, geht auf den damaligen Bahnchef Heinz Dürr und dessen Umfeld zurück und läuft darauf hinaus, Großbahnhöfe in Deutschland wie Frankfurt, München und eben Stuttgart ganz oder teilweise unter die Erde zu verlegen. Da solche Großbahnhöfe vorrangige Netzknoten und Umschlagplätze für den Fern- und Nahverkehr sind und damit eine große Fernwirkung haben, ist keinesfalls nur die Stadt oder Region Stuttgart, sondern das gesamte Bahnnetz im süd- (wenn nicht gesamt-) deutschen Raum betroffen. Damit sind wir schon beim

Mythos 2: „Stuttgart 21" ist (nur) ein Bahnhofs-Neubauprojekt. Oft wird die Tragweite des Projekts mit dem Argument heruntergespielt, es handele sich doch „nur" um einen städtischen Bahnhofsneubau. Tatsächlich werden hier (unter dem gemeinsamen Projektnamen) *zwei* Projekte miteinander verknüpft, nämlich der geplante Tiefbahnhof und die daran anschließende ICE-Neubaustrecke (NBS) über die Schwäbische Alb nach Ulm. Dabei spielen die (Mit-) Finanzierung durch den Bund und das Futtertrog-Gerangel der Bundesländer eine nicht unerhebliche Rolle. So wurde in Stuttgart von Seiten der Landesregierung mehrfach argumentiert, man könne allein deshalb nicht von dem Projekt zurückstehen, da sonst die (Bundes-)Mittel womöglich in andere Bundesländer fließen würden.

Mythos 3: „Stuttgart 21" ist vorrangig ein Verkehrsprojekt. Der verkehrliche Nutzen des Projekts ist – gelinde gesagt – äußerst umstritten, viele halten es für das Bahnsystem für eher schädlich (vgl. dazu unten). Unbestritten ist jedoch der Nutzen, den sich Stadtentwickler und Immobilien-Spekulanten von den frei werdenden Grundstücken in Zentrallage erwarten, wenn das gesamte bisherige Bahnhofs- und Gleisvorfeldgelände geräumt werden sollte.

Als ein Haupt-Argument haben dagegen die Befürworter seit Heinz Dürr immer wieder ein Bahn-Dogma ins Feld geführt:

Mythos 4: Durchgangsbahnhöfe sind grundsätzlich besser als Kopfbahnhöfe. Dieses Dogma ist spätestens seit Einführung der Wendezüge (sowohl im Fern- wie im Nahverkehr), die ohne Lokwechsel fahrplanmäßig in 4 Minuten wenden können, zumindest für Bahnhöfe mit großem Fahrgastaufkommen überholt, wo eine solche Haltezeit allein schon aus Komfortgründen notwendig und angemessen ist. Bei den Stuttgarter Gesprächen wurde von Seiten der Deutschen Bahn (DB) listig argumentiert, große europäische Kopfbahnhöfe wie Zürich oder Leipzig seien schon längst zu Durchgangsbahnhöfen umgebaut worden – ohne allerdings dabei zu erwähnen, dass diese Bahnhöfe Durchgangsgleise *zusätzlich* zu den bestehenden Kopfgleisen (in Längsrichtung) bekamen, während in Stuttgart der neue Tiefbahnhof *quer* zum alten Kopfbahnhof liegen und dieser in Gänze abgerissen werden soll!

Mythos 5: Ein Durchgangsbahnhof leistet (angeblich 30%) mehr Verkehrs-Durchsatz als ein Kopfbahnhof mit doppelt so vielen Gleisen. Diese Behauptung wurde anhand von mathematischen Flussmodellen gestützt, die von einem gleichmäßigen Verkehrsfluss, d.h. pausenlos ein- und ausfahrenden Zügen ausgehen und daraus die Maximalzahl durchzuschleusender Züge berechnen. Solche Berechnungen mögen ihren mathematischen Reiz haben, an der Praxis eines kunden- und umsteigefreundlichen Bahnbetriebs gehen sie jedoch vorbei. Züge sollten nicht dann abfahren, wenn zufällig Gleise frei sind (z. B. nachts oder kurz vor der Ankunft eines wichtigen, selten verkehrenden Fernzugs) sondern *dann, wenn sie gebraucht werden*.

Das bringt uns zu dem auch für Informatiker interessanten Thema des *Integralen Taktfahrplans (ITF)* und zu

Mythos 6: Ein ITF ist in Stuttgart nicht zu verwirklichen und deshalb auch für den Rest von (Süd-)Deutschland vernachlässigbar. Nun ist es eine unbestrittene Tatsache, dass das mit Abstand erfolgreichste und kundenfreundlichste Bahnsystem (mit mehr als doppelt soviel zurückgelegten Bahn-Km pro Person im Vergleich zu Deutschland) im Nachbarland Schweiz genau mit Hilfe des ITF and des darauf aufbauenden Bahnkonzepts „Bahn 2000" geschaffen wurde. Der Schlüssel zum Erfolg liegt im sogenannten *Rendezvous-Prinzip* (und dem dazu erforderlichen Infrastruktur-Ausbau) für die (Umsteige-)Knotenbahnhöfe, wo zu bestimmten vorgegebenen Zeiten (aus merktechnischen Gründen vorzugsweise zur Minute 00 oder 30) möglichst viele Fern- und Regionalzüge zusammen kommen, um nach der Knotenzeit in verschiedene Richtungen wieder abzufahren und damit optimales Umsteigen zu ermöglichen.

Natürlich ist ein solches System von vernetzten Bahnknoten nicht zum Nulltarif zu haben. Es erfordert gezielte (aber in der Regel vergleichsweise moderate) Investitionen in die Netz-Infrastruktur (z.B. um bestimmte gewünschte Fahrzeiten zwischen einzelnen Knoten zu erreichen) und vor allem: es erfordert *intelligente Planung*. Hier sind Informatiker gefragt. Am Beginn einer Bahn-

Netzkonzeption sollte die Frage nach einem optimalen Fahrplan stehen. Aus Theorie-Sicht ist das ein NP-vollständiges Problem [Guc 97], aber es gibt mittlerweile ausgefeilte Heuristiken, mit deren Hilfe man schon gut brauchbare Lösungen für mittelgroße Systeme (mit ca. 50-60 Knoten) generieren kann [Hes 07]. Aus Sicht der Praxis sind Werkzeuge interessant, mit denen man größere Netze entwerfen, interaktiv bearbeiten und die Güte von Fahrplänen bewerten kann [HGH 05]. Aufgrund solcher Analysen kann man ein (oder mehrere alternative) Betriebskonzept(e) erstellen und daran die Infrastruktur-Planung ausrichten.

In Deutschland – und speziell im Fall Stuttgart – geht man leider nach wie vor den umgekehrten Weg: Erst wird gebaut (bzw. die Bauplanung festgezimmert) und dann sucht man nach Betriebskonzepten. Entsprechend dürftig sah das in Stuttgart präsentierte Betriebskonzept der DB aus. Danach sollen sich für den künftigen Tiefbahnhof die mittleren Umsteigezeiten im Fernverkehr bzw. zwischen Fern- und Nahverkehr um jeweils ca. 20 %, im Nahverkehr sogar um 55 % gegenüber den aktuellen Werten *verschlechtern*! Dem haben die Projektgegner ein Konzept gegenübergestellt, in dem sie diese Werte für einen ausgebauten Kopfbahnhof noch um 19 bzw. 14 % verbessern können.

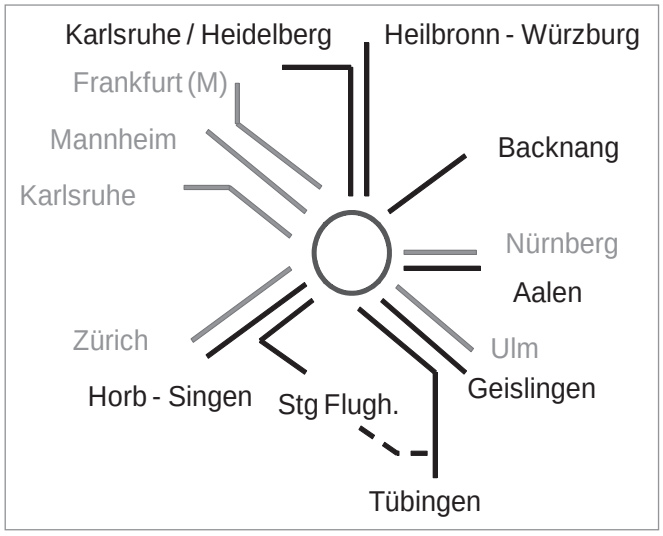


Abb. 1: Der Bahnknoten Stuttgart

Dreh- und Angelpunkt aller dieser Konzepte ist die *Anzahl der Gleise* im Bahnhof: Für einen guten ITF braucht man in Stuttgart mindestens 14 Gleise gleichzeitig (6 für den Fern- und 8 für den Regionalverkehr, vgl. Abb. 1), eine Kapazität, die der geplante 8-gleisige Tiefbahnhof niemals erbringen könnte. D.h. die oben erwähnten Kapazitätsberechnungen und auch der angekündigte „Stresstest" der DB sind (zumindest aus ITF-Sicht) reine Makulatur. Trotz der etwas schwierigen Fahrplansituation in Stuttgart ließe sich sogar (mit relativ geringen Investitionen) ein nahezu idealer ITF erreichen – aber eben nur für den dazu bereits gut ausgestatteten Kopfbahnhof [Hes 11].

(Zwischen-)Fazit

Bund, DB und die Stadt Stuttgart planen, für z.Zt. geplante 4,5 Mrd. (bzw. realistisch geschätzte 7 Mrd. oder mehr) Euro einen gut ausgestatteten und relativ störungsfreien Großstadtbahnhof unter die Erde zu legen und dabei dessen Gleiszahl auf weniger als die Hälfte zu reduzieren. Damit ist „Stuttgart 21" kein Zukunftsprojekt für das 21. Jahrhundert, sondern ein gigantisches *Bahn-Rückbauprojekt*, das dem Denken der US-Autobarone der 1930-er Jahre verhaftet ist, als Bahnstrecken kannibalisiert und Bahnhöfe unter die Erde verbannt wurden, um Platz für Immobilien und Straßen zu schaffen. Wie einst die Bürger von Schilda ihr neues Rathaus ohne Fenster und Türen planten, so wollen die Stuttgart 21-Planer ihren neuen Hochglanz-Bahnhof ohne die notwendigen Bahnsteige, Zu- und Ablaufgleise ins Erdreich vergraben.

Beim Gesamtprojekt (incl. der geplanten Neubaustrecke nach Ulm) ist es ähnlich: Während die Schweiz ca. 10 Mrd. Euro investiert, um am Gotthard den Scheitelpunkt der Alpenquerung um 500 m zu senken, will man in Deutschland eine ähnliche Summe aufwenden, um mit zwei Bergquerungen (Filder und Schwäbische Alb) die Scheitelpunkte um insgesamt mehr als 300 m zu *erhöhen*!

Bürgerproteste, Schlichtung und ein fataler Schlichterspruch

Wie konnte es geschehen, dass trotz dieser verheerenden Bilanz (bei der ich weitere gravierende Probleme wie die schwierigen geologischen Verhältnisse, die bedrohten Stuttgarter Mineralquellen und eklatante Sicherheitsrisiken – z.B. aus der Schräglage des geplanten Bahnhofs, die um 500 % über dem zulässigen Wert liegt – noch gar nicht erwähnt habe) das Projekt in ca. 20-jähriger Planungs- und Vorbereitungszeit vor sich hindümpelte und erst im Sommer 2010 richtig ins öffentliche Bewusstsein drang? Um das zu verstehen muss man sich etwas näher mit der Genese von Großprojekten und ihren Planungsprozessen in Deutschland befassen.

Hierzulande gibt es praktisch kaum eine Bürgerbeteiligung bei Großprojekten. So wurden in Stuttgart nach den ersten Projektvorschlägen von Prof. Heimerl Anfang der 1990-er Jahre Varianten in geschlossenen Zirkeln diskutiert, 1994 eine Machbarkeitsstudie in Auftrag gegeben und 1995 die Öffentlichkeit über eine zwischen Bund, Land und Bahn geschlossene Rahmenvereinbarung informiert. Einspruchsmöglichkeiten gegen das Projekt haben nur direkt betroffene Bürger im Planfeststellungsverfahren, ein von den Bürgern initiierter Bürgerentscheid wurde 2007 mit formaljuristischen Finessen unterbunden. Die lange Vorbereitungszeit von ca. 15 Jahren ist keineswegs nur den Einsprüchen renitenter Bürger geschuldet, sondern ebenso

Abb. 2: Protestaktion im Stuttgarter Schlosspark, Foto: B. Schroeder

dem Zögern der Projektverantwortlichen – so sorgte z.B. der frühere Bahnchef Ludewig selbst dafür, dass das Projekt jahrelang auf Eis lag.

So ist es kein Wunder, dass große Teile der Bürgerschaft sich von den Projektbetreibern überrumpelt und selbst jeglicher Mitsprachemöglichkeit beraubt fühlten – was schließlich zu den Demonstrationen im Sommer 2010, dem gewaltsamen Polizeieinsatz vom 30. September 2010 und zu den Stuttgarter Schlichtungsgesprächen mit dem Schlichter Heiner Geißler führte. Die Schlichtungsgespräche fanden vom 22.10. bis 30.11.2010 im Stuttgarter Rathaus statt und stellen ein absolutes Novum in der bundesdeutschen Demokratiegeschichte dar. Ich war bei drei dieser Gespräche als Sachverständiger geladen und habe den Rest fast lückenlos am Fernseher verfolgt.

Nach acht (Fach-)Gesprächen meinte ich um den 25.11. herum ein insgesamt sehr positives Zwischenfazit ziehen zu können:

- Die Gespräche entpuppten sich als politischer Vorgang *ohne Vorbild* in Deutschland – ein Lehrstück für eine *lebendige Demokratie*.

- Hier saßen Vertreter der Zivilgesellschaft und etablierte Politiker *gleichberechtigt* am runden Tisch und befassten sich intensiv und zum Teil bis ins letzte Detail mit Sachfragen. In der Regel hatten beide Seiten ausreichend Zeit und Gelegenheit zur Darstellung ihrer Positionen.

- Alle Gespräche (abgesehen von einer Sitzung) und alle präsentierten Unterlagen waren *öffentlich*. Die Fernseh-Direktübertragungen fanden (trotz ihrer Länge und der z.T. recht „trockenen" fachspezifischen Themen) eine ungeahnte Resonanz und brachten unerwartete Einschaltquoten – ein Zeichen für den „Hunger" der Bürger nach Sach-Information und Beteiligung.

- Eine Schlüsselrolle kommt (natürlich) dem Schlichter zu. Der Erfolg solcher Gesprächsrunden hängt sehr stark von seiner *Autorität* und allseits anerkannten *Unabhängigkeit* ab.

- Das Procedere bei der Schlichtung könnte ein Vorbild für künftige öffentliche Meinungsbildung (z.B. im Zusammenhang mit *direkter Demokratie* und bei der Vorbereitung von Volksabstimmungen) sein.

- Mein persönlicher Gesamteindruck war: Mit dieser Debatte *vor Projektbeginn* (und gefolgt von einer Volksabstimmung) hätte das Projekt „Stuttgart 21" *keine Chance* gehabt.

Das war jedoch nicht das Ende vom Lied. Es folgte die Schlusssitzung vom 30.11. mit dem „Schlichterspruch" von Heiner Geißler. Dieser Spruch enthielt viel (berechtigte) Kritik an dem Vorhaben, eine Reihe von (mehr oder weniger praktikablen) Verbesserungsvorschlägen sowie die Aufforderung zu einem „Stresstest", der die erhöhte Leistungsfähigkeit des geplanten Bahnhofs demonstrieren soll. Er enthielt allerdings auch den Satz: *„Ich halte das Projekt »Stuttgart 21« grundsätzlich für richtig."* Mit diesem entscheidenden Spruch, der den Verlauf der bis dahin geführten Gespräche konterkarierte, hat Herr Geißler vielleicht seinen früheren Parteifreunden, aber weder der Stuttgarter Sache noch der Demokratieentwicklung in Deutschland einen guten Dienst erwiesen.

So sehr man den Schlichtungsprozess für sich genommen als „Wiederentdeckung des Bürgers" (so Heribert Prantl in der *Süddeutschen Zeitung*) feiern kann, so wenig ist sein Ergebnis geeignet, das Vertrauen in eine gerechte, gut funktionierende Demokratie zurückzugewinnen. Schade – denn Herr Geißler hätte ein *salomonisches* Urteil fällen können. Dazu hätte gehört, eine einseitige Parteinahme zu vermeiden und seine Auflagen für das Projekt mit der Aufforderung an die Projektträger (Bahn, Bund, Land) zu verbinden, das alles noch mal durchzukalkulieren und dann selbst zu entscheiden – oder besser: das Volk entscheiden zu lassen – ob es das wert ist. Und natürlich: Bis zu dieser Entscheidung *nicht* weiter zu bauen.

Stattdessen hat er sich auf die Vorbedingungen der Projektbetreiber eingelassen, die Kritiker des Projekts mit wunderbar offenen und sachlichen Gesprächen beruhigt, sich dann zum obersten Richter der Nation gemacht und das von Anfang an feststehende Ergebnis als „Schlichterspruch" verkündet. Damit glich er einem Ringrichter, der nach sieben (von insgesamt acht) eindeutig verlaufenen Kampfrunden den Unterlegenen zum Sieger ausruft und all die schönen vorgebrachten (Gegen-)Argumente mit einem *K.o. ex cathedra* niederstreckt.

Warum er das tat? Da kann man nur mutmaßen. Offenbar war die Nähe zu seiner alten Partei größer als der Ansporn, durch einen ausgewogenen und unabhängigen Spruch als überparteilicher Schiedsmann in die Geschichte einzugehen. Diese Chance hat er leider vertan. Die Gegner haben sich (wohl etwas zu naiv) auf einen Prozess eingelassen, der ihnen ihre guten Karten aus der Hand geschlagen und stattdessen den schwarzen Peter zugespielt hat. Denn nun sollen sie auch noch als weitere Preistreiber für ein eigentlich ungewolltes und für schädlich erachtetes Projekt dastehen.

Wolfgang Hesse

Prof. Dr. **Wolfgang Hesse** lebt in München und war bis 2008 als Hochschullehrer für das Fach Softwaretechnik am Fachbereich Mathematik und Informatik der Universität Marburg aktiv. Seine Arbeitsschwerpunkte sind die Softwaretechnik, Modellierung, interdisziplinäre und gesellschaftliche Bezüge der Informatik. Daneben ist er Bahn-Vielfahrer und hat u.a. Projekte zur Fahrplan-Optimierung im öffentlichen Verkehr durchgeführt. Er ist Gründungsmitglied des FIfF und Mitglied bei der Bahnfachleutegruppe "Bürgerbahn statt Börsenbahn" sowie der Initiative "Bahn für Alle".

Fazit

Der Schlichtungsprozess war gut, das Ergebnis war deprimierend. Herr Geißler hat (ohne erkennbare Notwendigkeit) einem Projekt das Wort geredet, das nicht ins 21. Jahrhundert, sondern in die Bahn-Rückbau-Mentalität der Autobarone und Neo-Liberalisierer des vergangenen Jahrhunderts passt. Er hat eine Weichenstellung in der Verkehrspolitik bekräftigt, die weiter auf Marginalisierung (und letztlich Privatisierung) der Bahn, Konzentration auf Konsumpalast-Bahnhöfe und Hochgeschwindigkeitsstrecken setzt, statt endlich intelligente Lösungen für flächendeckenden öffentlichen Verkehr, Netzverknüpfung und Deutschland-weite Taktfahrpläne zu entwickeln.

Nun ist die Gefahr groß, dass alle (mit Recht) Politik-Verdrossenen sagen: Das Spiel läuft weiter wie gehabt – und Verhandlungen wie die in Stuttgart sind nichts als ein raffinierter Trick, um Aufmüpfige zu beruhigen und Projekten wie Stuttgart 21 zur (Pseudo-)Legitimation zu verhelfen.

Literatur:

[Guc 97] Michael Guckert: Anschlußoptimierung in öffentlichen Verkehrsnetzen – Graphentheoretische Grundlagen, objektorientierte Modellierung und Implementierung (Dissertation, Univ. Marburg, 1997)

[Hes 07] Roland Hesse: Ein Hybrid-Verfahren zur Bearbeitung kombinatorischer Optimierungsprobleme (Dissertation, TU München, 2007)

[Hes 11] Wolfgang Hesse: Stuttgart: Nullknoten ist möglich – Betriebskonzepte und Integraler Taktfahrplan in der Diskussion. In: Eisenbahn-Revue International, Heft 3/2011, S. 150-152, Minirex-Verlag, Luzern 2011

[HGH 05] Wolfgang Hesse, Michael Guckert, Roland Hesse: OptiTakt – A tool for developing and evaluating periodic timetables, Proc. 1st Int. Sem. on Railway Operations Modelling, RailDelft 2005; http://www.uni-marburg.de/fb12/informatik/homepages/hesse/publikationen/dateien/hgh_05.pdf

Jürgen Altmann

Rüstungskontrolle für Roboter

In der modernen Kriegsführung bieten unbemannte Fahrzeuge – in der Praxis handelt es sich meist um unbemannte Flugzeuge – aus rein militärischer Sicht viele Vorteile. Werden aber die Folgen für Frieden, Kriegsvölkerrecht und die Sicherheit in Gesellschaften genauer beleuchtet, kommt man zum Schluss, dass der Menschheit durch Begrenzungen und Verbote besser gedient wäre.

Unbemannte Luftfahrzeuge (UAVs, uninhabited/unmanned air vehicles, im Deutschen auch »Drohnen«, bei der Bundeswehr als UAS bezeichnet) nutzen Streitkräfte schon lange, aber seit einigen Jahren steigt ihre Bedeutung massiv an. Für ihre Kriegsführung in Afghanistan, Irak und Pakistan haben die USA bewaffnete UAVs eingeführt, mit denen sie ferngesteuert angreifen. Ein Ziel der weiteren Forschung und Entwicklung ist erhöhte Autonomie, bis zur vollautomatischen Entscheidung, wer oder was angegriffen wird. Andere Länder folgen diesem Trend. Hohe Aufwendungen gehen auch in die Entwicklung unbemannter Fahrzeuge (UVs – uninhabited/unmanned vehicles), die sich auf dem Boden bzw. auf oder unter Wasser bewegen.[1]

Geschichte und Gegenwart: Aufklärung und Überwachung

Experimente mit unbemannten Flugzeugen gab es schon zu Beginn des 20. Jahrhunderts, aber im Krieg wurden sie zum ersten Mal systematisch durch Nazi-Deutschland eingesetzt, mit der Flügelbombe V1, einem Vorläufer des modernen Marschflugkörpers.[2] Später wurden Luftabwehr-Zielflugkörper für Aufklärungszwecke umgerüstet und weiterentwickelt und durch die USA im Vietnamkrieg erstmalig routinemäßig eingesetzt. Seit den 1970er Jahren haben viele Streitkräfte UAVs für solche Zwecke eingeführt. Zunächst hatte Israel die Führung, wurde aber bald von den USA überholt. Heute stellen mehr als 50 Länder UAVs her, 20 exportieren sie.[3]

Es gibt verschiedenartige UAV-Typen: Kleine »Modellflugzeuge« werden von Hand gestartet und kommen einige Kilometer weit (z.B. die deutsche ALADIN). UAVs mittlerer Größe können von einem LKW-Katapult aus gestartet werden und haben Reichweiten bis zu einigen hundert Kilometer (z.B. der französische Sperwer). Größere Flugzeuge starten und landen auf Flugplätzen; sie können viele Stunden fliegen. Beim größten Typ, dem Global Hawk (USA, 40 m Spannweite), sind es 36 Stunden; er fliegt mit bis zu 640 km/h in bis zu 20 km Höhe. Neben solchen propeller- oder düsengetriebenen Flächenflugzeugen gibt es auch Hubschrauber verschiedener Größen. Diese Arten von UAVs tragen Sensoren (Videokameras für sichtbares oder Infrarot-Licht, Radar) und übermitteln ihre Bilder und Signale über Funk. Für größere Entfernungen (z.B. zwischen dem Mittleren Osten und Europa bzw. den USA) dienen Satelliten als Übertragungsknoten.

Da Navigation auf Land, insbesondere im Gelände, erheblich schwieriger ist als in der Luft, sind unbemannte Landfahrzeuge in der Entwicklung deutlich weniger weit als Luftfahrzeuge, mit der Ausnahme kleiner Roboterfahrzeuge zum Entschärfen von Sprengkörpern, die aus kurzer Entfernung ferngesteuert werden – hiervon haben die USA viele tausend im Einsatz. Für unbemannte Landfahrzeuge von klein bis groß wird intensive Forschung und Entwicklung betrieben, nicht nur in den USA. Auf See gibt es erste ferngesteuerte bewaffnete Motorboote, und unter Wasser geht es u.a. um autonome(re) Torpedos.[4]

Trend zur Bewaffnung unbemannter Fahrzeuge

Seit fast zehn Jahren gibt es einen Trend, Aufklärung mit Angriff zu kombinieren, indem UAVs mit Waffen ausgerüstet wer-

den, wobei die USA führen (unbemannte Land- und Wasserfahrzeuge zu bewaffnen, ist ebenfalls vorgesehen).[5] 2000 setzte der US-Kongress das Ziel, 2010 solle ein Drittel der weitreichenden Kampfflugzeuge in der operativen US-Luftwaffe unbemannt sein und 2015 ein Drittel der Bodenkampffahrzeuge der US-Armee.[6]

Im Rahmen ihres »Kriegs gegen den Terror« rüsteten die USA einige ihrer Aufklärungs-UAVs des Typs Predator nachträglich mit zwei Hellfire-Flugkörpern aus (laser- oder radargesteuert, zum Einsatz gegen Bodenziele). Diese sind seit 2001 in Afghanistan im Einsatz; breiter bekannt wurde ein Angriff gegen ein Auto 2002 im Jemen, bei dem sechs mutmaßliche Al-Kaida-Mitglieder getötet wurden. Seitdem sind Flugkörperangriffe von ferngesteuerten UAVs Routine geworden. Ein größeres UAV wurde gebaut und ab 2007 stationiert – der MQ-9 Reaper, mit 1.700 kg Zuladung (z.B. vier lasergesteuerte 230-kg-Bomben und vier Hellfire-Flugkörper). Anfang 2009 waren 195 bewaffnete MQ-1 Predator und 28 MQ-9 Reaper für Angriffe in Afghanistan, Irak und Pakistan stationiert.

Start und Landung werden von Basen in der Region gesteuert, aber dann wird die Flugüberwachung und Waffenauslösung von britischen und US-Piloten übernommen, die u.a. in der Creech Air Force Base in Nevada, USA, »arbeiten«. Sie gründen ihre Zielentscheidungen auf Videobilder der Kameras in den UAVs, die für eine Personenidentifikation zu ungenau sind; auch die Entscheidung, ob jemand eine Waffe trägt, ist nicht immer zuverlässig.[7] In vielen Fällen wurden die falschen Personen angegriffen, Zivilisten wurden getötet, in einigen Fällen waren die Zielpersonen (Taliban- und Al Kaida-Führer) gar nicht anwesend. So wurden allein in Pakistan seit 2004 mehr als 1.000 Kämpfer und einige hundert Nicht-Kämpfer mittels UAVs getötet.[8] Insbesondere die Angriffe in Pakistan werden nicht durch die Streitkräfte, sondern durch den Geheimdienst CIA durchgeführt, und der UN-Berichterstatter für außergerichtliche Tötungen hat Aufklärung gefordert.[9]

Kampfdrohnen werden kein Monopol der USA oder einiger westlicher Länder bleiben. Der Iran beispielsweise kündigte 2010 die Massenproduktion von zwei Typen langreichweitiger »unbemannter Bomber« an.[10] Für die Zukunft werden UAVs für alle Formen von Kampf und Kampfunterstützung, die bisher mit bemannten Flugzeugen durchgeführt werden, in den Blick genommen. So sieht die »Unmanned Systems Roadmap« des US-Verteidigungsministeriums UAVs zur Luftbetankung für 2024 und für den Luftkampf für 2032 voraus.[11] Prototypen solcher unbemannter Kampfflugzeuge (uninhabited combat air vehicles, UCAVs) werden entwickelt und gebaut in den USA (UCAS-D/X-47B), Frankreich (nEuron, mit Schweden, Griechenland, Schweiz, Spanien, Italien), Deutschland (Barracuda, mit Spanien), Großbritannien (Taranis) und Russland (Skat).

Trend zu autonomem Angriff

Schon jetzt werden viele UAVs mit Bord-Navigations- und -Flugsteuerungssystemen gesteuert, mittels Wegpunkten, die im Vorhinein oder in Echtzeit durch eine Bodenkontrollstation angegeben werden. Dem menschlichen Bediener wird so die Aufgabe erspart, die Flughöhe und den Kurs zu halten. Er oder sie kann sich auf die Aufklärung und ggf. den Angriff konzentrieren. Einige militärische Motive sprechen dafür, UAVs, insbesondere bewaffneten, mehr Autonomie zu geben: Die Kommunikationsverbindung kann defekt sein oder gestört werden. Man könnte Geld sparen, wenn ein Soldat nicht ein, sondern mehrere UAVs kontrolliert. Die Zeitverzögerung durch die Satellitenverbindung plus der menschlichen Reaktionszeit kann für den Kampf zu lang erscheinen – für das Überleben der eigenen Systeme kann man die örtliche Reaktion in Sekundenbruchteilen für nötig halten. Aus diesen Gründen wird für autonome Zielauswahl und autonomen Angriff geforscht und entwickelt.

Das US-Verteidigungsministerium schreibt:

> *„Die Bewaffnung unbemannter Systeme ist eine hoch kontroverse Frage, die ein geduldiges »Kriechen-Gehen-Laufen«-Herangehen erfordern wird in dem Maß, wie sich die Zuverlässigkeit und Leistungsfähigkeit jeder Anwendung erweist. […] Anfängliche Anwendungen der Bewaffnung eines unbemannten Systems können einen »Menschen in der Schleife« erfordern. […] In dem Maß, wie das Vertrauen in die Systemverlässlichkeit, Funktion und Zielalgorithmen wächst, kann man mehr autonome Operationen mit Waffen in Erwägung ziehen."*[12]

Töten auf Beschluss einer Maschine?

Es ist offensichtlich: Die Möglichkeit, dass ein Computer die Entscheidung trifft, einen Menschen zu töten, wirft ein tiefes moralisches Problem auf.[13] Forschung zu den ethischen und rechtlichen Fragen, die sich durch den Einsatz bewaffneter autonomer Systeme stellen, wurde von der US-Marine und der US-Armee in Auftrag gegeben.[14] Besonders wichtig ist die Frage, ob autonome Waffensysteme die Anforderungen des Kriegsvölkerrechts erfüllen können. Darin sind die zentralen Prinzipien die Diskriminierung (zwischen legitimen und illegitimen Angriffszielen) und die Proportionalität (zwischen dem errungenen militärischen Vorteil und dem angerichteten Schaden).

Um seine Arbeit an Algorithmen für ethisches Töten zu rechtfertigen, verweist ein Robotikforscher auf jüngere Umfragen durch den obersten Militärarzt der USA und auf allgemeine Literatur, die zeigen, dass menschliche Soldaten die Regeln des Kriegsvölkerrechts oft brechen.[15] Sein Ziel ist es, Roboterprogramme zu erstellen, die sich gesetzeskonformer verhalten. Mit wissenschaftlicher Strenge schlägt er einen »ethischen Regler« für die Bewertung einer beabsichtigten tödlichen Handlung vor. Wenn der ein Veto abgäbe, würde kein Angriff stattfinden (mit der einzigen Ausnahme, wenn sich ein menschlicher Bediener darüber hinweg setzte, der dann die Verantwortung übernähme). Allerdings kann man bezweifeln, ob ein Künstliche-Intelligenz-System eine komplexe Kriegssituation auf der Höhe menschlicher Intelligenz beurteilen kann, wenigstens für die nächsten ein bis zwei Jahrzehnte. Ein britischer Robotikforscher hat solche Pläne lautstark kritisiert. Er fragt die Künstliche-Intelligenz-Gemeinschaft, *„ob wir bereit sind, Entscheidungen über Leben oder Tod Robotern zu überlassen, die zu schwer von Begriff sind, um dumm genannt zu werden"*.[16] Er verweist auf die geringen Fähigkeiten heutiger künstlicher Intelligenz und stellt sich beispielhafte Situationen vor: *„Ich kann mir eine städtische Umgebung vorstellen, in der ein kleines Mädchen einem Roboter*

ein Eis entgegen hält, nur um abgeknallt zu werden, weil es versucht hat, seine Süßigkeit mit ihm zu teilen."

Kriterien der präventiven Rüstungskontrolle

Neben Fragen des Kriegsvölkerrechts werfen bewaffnete U(A)Vs Probleme in Bezug auf einige andere Kriterien der präventiven Rüstungskontrolle auf.[17] Rüstungskontrollverträge könnten gefährdet werden, wenn UAVs als neue Kernwaffenträger fungieren oder die Kategorien des Vertrags über Konventionelle Streitkräfte in Europa (KSE) umgehen würden.

Destabilisierung der militärischen Lage kann sich durch UAVs in mehrerlei Hinsicht ergeben: Da sie schwer zu entdecken sind, können sie für tiefes Eindringen und präzisen Überraschungsangriff genutzt werden. Weil sie keine Mannschaft an Bord haben, könnte man sie für riskantere Einsätze verwenden. Wenn sich in einer Krise zwei UAV-Flotten bei kurzem Abstand gegenseitig intensiv beobachten würden, könnten plötzliche unklare Ereignisse und ungesteuerte Rückkopplungsschleifen zur schnellen Eskalation in den Krieg führen. Schwärme von hoch genauen, kleinen UAVs könnten sogar in der Lage sein, nuklearstrategische Ziele auszuschalten; solch ein Szenario könnte zu sehr gefährlichem Verhalten führen. Dass bewaffnete UAVs technologisches Wettrüsten und Weiterverbreitung bringen werden, ist offensichtlich. Kleine, technisch ausgefeilte UAVs – die nur von Staaten entwickelt werden könnten, die aber in die Hände nichtstaatlicher Akteure gelangen könnten – würden neue Möglichkeiten für terroristische Anschläge bieten.

Daher würden bewaffnete UAVs in verschiedener Hinsicht Gefahren bringen. Um diese einzudämmen, sollten vorbeugende Begrenzungen diskutiert und eingeführt werden. Das hat sich das International Committee for Robot Arms Control (ICRAC) zum Ziel gesetzt, das wir (zwei Philosophen aus Australien und USA, ein Robotikforscher aus Großbritannien und der Autor) im September 2009 gegründet haben und das 2010 um sechs internationale Wissenschaftler/innen erweitert wurde.[18]

Konzepte für präventive Rüstungskontrolle

Die Diskussion über vorbeugende Begrenzungen bei bewaffneten UAVs hat in der Wissenschaft erst begonnen[19] und Regierungen noch kaum erreicht.

Es ist klar, dass bewaffnete, unbemannte Land- und Luftfahrzeuge unter die Definitionen des KSE-Vertrags fallen – diese wurden 1989/1990 bewusst so angelegt, dass sie unabhängig davon sind, ob eine Besatzung an Bord ist. Jedoch gibt es keine Begrenzungen konventioneller Streitkräfte außerhalb Europas (und die Vertragsstaaten USA und Großbritannien haben ihre Predator- und Reaper-UAVs nicht gemeldet, weil sie nicht im Vertragsgebiet – Europa vom Atlantik bis zum Ural – stationiert sind). Der Vertrag – gegenwärtig suspendiert – sollte dringend reaktiviert werden. Insbesondere sollte das Protokoll über vorhandene Typen konventioneller Waffen und Ausrüstungen aktualisiert werden.[20] Solange keine neuen Kategorien leichterer Kampfflugzeuge mit zusätzlichen Obergrenzen eingeführt werden, zählen auch kleine bewaffnete UAVs als ein Kampfflugzeug, so dass die bisherigen nationalen Obergrenzen für eine wirksame quantitative Begrenzung in Europa sorgen würden. Bei Landfahrzeugen würden unbemannte Fahrzeuge als »Kampfpanzer« bzw. »Kampffahrzeuge mit schwerer Bewaffnung« zählen, wenn sie die entsprechenden Kriterien erfüllen (u.a. Kanone von mindestens 75 mm Kaliber und Leermasse mindestens 16,5 bzw. 6,0 Tonnen). Leichtere bewaffnete unbemannte Fahrzeuge sind nicht erfasst (wenn sie nicht zum Transport einer Infanteriegruppe gebaut sind) und könnten daher unbegrenzt eingeführt werden.

Der Mittelstreckenwaffen- (INF-) Vertrag zwischen den USA und Russland verbietet diesen Ländern landgestützte Langstrecken-Marschflugkörper mit Reichweiten von 500 bis 5.500 km, andere Länder sind nicht einbezogen. Um Unterlaufen und weltweiten Aufwuchs zu vermeiden, sollte der Vertrag auf alle relevanten Länder erweitert werden,[21] und andere nuklear bewaffnete U(A)Vs sollten ganz verboten werden.

Der Haager Verhaltenskodex gegen die Proliferation ballistischer Raketen (HCOC – Hague Code of Conduct against Ballistic Missile Proliferation) verpflichtet die Mitgliedsländer politisch zu Exportkontrolle und vertrauensbildenden Maßnahmen, gilt aber nur für Raketen. Marschflugkörper und andere UAVs werden bisher nicht erfasst.[22]

In Bezug auf autonom angreifende Waffensysteme gilt eigentlich, dass sie nicht eingeführt werden dürfen, solange nicht demonstriert ist, dass sie die Regeln des Kriegsvölkerrechts einhalten können. Außer in eng begrenzten Szenarien mit wenigen, leicht unterscheidbaren Zielen wie z.B. bei Luftabwehr wird das auf lange Zeit nicht gelingen. Jedoch kann man sich auf die allgemeine Regel nicht verlassen – die militärischen Motive für autonomes Schießen werden dafür wahrscheinlich zu stark. Folglich sollte ein explizites Verbot beschlossen werden.

Das ICRAC hat im September 2010 den ersten internationalen Experten-Workshop »Rüstungskontrolle für Roboter« durchgeführt. In der Abschlusserklärung heißt es:[23]

„Wir glauben:

- *Dass die Langzeitrisiken durch Proliferation und weitere Entwicklung dieser Waffensysteme schwerer wiegen als kurzfristige Nutzeffekte gleich welcher Art, die sie zu haben scheinen.*

- *Dass es nicht akzeptabel ist, dass Maschinen die Anwendung von Zwang oder Gewalt in Konflikten oder Kriegen steuern, bestimmen oder darüber entscheiden. In jeder Situation, in der eine solche Entscheidung zu treffen ist, muss zumindest ein Mensch für diese Entscheidung und deren vorhersehbare Folgen persönlich verantwortlich und juristisch rechenschaftspflichtig sein.*

- *Dass das sich derzeit beschleunigende Tempo der Kriegsführung durch diese Systeme weiter gesteigert wird und die Fähigkeit von Menschen, in Militäroperationen verantwortungsbewusste Entscheidungen zu treffen, unterminiert.*

- *Dass die Asymmetrie der Kräfte, die diese Systeme möglich machen, sowohl Staaten als auch nicht-staatliche Akteure ermutigt, Formen der Kriegsführung zu verwenden, die die Sicherheit der Bürger der Besitzerstaaten verringern.*

- *Dass die Tatsache, dass ein Fahrzeug unbemannt ist, nicht das Recht verleiht, die Souveränität von Staaten zu verletzen."*

Die Erklärung verlangt ein Rüstungskontrollregime mit mehreren Bestandteilen. Verboten werden sollen:

- *„Die weitere Entwicklung, Beschaffung, Stationierung und Nutzung autonomer Roboterwaffen.*

- *Die Bestückung neuer Arten von autonomen oder ferngesteuerten Systemen mit Nuklearwaffen.*

- *Die Entwicklung, Stationierung und Nutzung von Roboter-Weltraumwaffen."*

Eingeschränkt werden sollen:

- *„Die Reichweite und Nutzlast von bewaffneten ferngesteuerten unbemannten Fahrzeugen.*

- *Die Anzahl – aufgeschlüsselt nach Art und Leistungsfähigkeit – bewaffneter ferngesteuerter unbemannter Systeme, die von einem Staat stationiert werden dürfen.*

- *Die Höchstflug- bzw. -fahrtdauer dieser Systeme.*

- *Die Entwicklung, Beschaffung und Stationierung bewaffneter unbemannter Systeme unterhalb einer Mindestgröße."*

Diese Regeln sollten weltweit gelten. Das erste Verbot sollte als neue globale Konvention beschlossen werden, wobei genaue Definitionen und auch bestimmte Ausnahmen festzulegen sind.[24] Das zweite sollte in Verhandlungen zur Reduzierung und schließlichen Abschaffung der Kernwaffen eingehen. Das dritte sollte mit dem lange angestrebten allgemeinen Verbot von Weltraumwaffen realisiert werden.

Details für die verschiedenen vorgeschlagenen Beschränkungen festzulegen, wird intensive Überlegungen und Verhandlungen brauchen. Dabei können die Ziele des KSE-Vertrags[25] als Richtschnur gelten, und seine Methodik[26] kann als allgemeines Vorbild dienen. Grundsätzlich sind globale Regeln anzustreben, da das aber in den bekannten Krisenregionen (wie Naher/Mittlerer Osten, Südasien, Ostasien) schwierig werden wird, ist es sinnvoll, in anderen Regionen anzufangen. Insbesondere Europa könnte hier eine Vorbildrolle spielen.

Schlusswort

Die Bewaffnung von UAVs hat gerade erst begonnen, und die von unbemannten Land- und Wasserfahrzeugen steht noch weitgehend bevor. Daher gibt es die prinzipielle Möglichkeit, die nächste große Welle militärtechnischer Innovation zu stoppen, bevor sie sich in großem Umfang entfaltet und praktisch unumstößlich wird. Die Länder sollten ihre Sicherheit aus aufgeklärter Sicht betrachten, das heißt im weiten, internationalen Rahmen. Stabilität, Frieden und internationaler Sicherheit wäre durch kooperativ ausgehandelte Begrenzungen besser gedient als durch einen unbeschränkten Aufwuchs aller Arten bewaffneter unbemannter Fahrzeuge. Forscher/innen in Robotik und künstlicher Intelligenz sollten sich der Gefahren von Roboter-Waffen bewusst sein und vorbeugende Begrenzungen unterstützen.

Anmerkungen

1 *Für Übersichten siehe A. Krishnan (2009):, Killer Robots – Legality and Ethicality of Autonomous Weapons. Farnham Surrey/Burlington VT: Ashgate. P. Singer (2009): Wired For War – The Robotics Revolution and Conflict in the 21st Century. New York: Penguin. P. Singer: Der ferngesteuerte Krieg, Spektrum der Wissenschaft, Nr. 12, Dez. 2010, S. 70-79. Siehe auch L. Wirbel, Kriegsführung mit Drohnen, W&F 3/2010, S. 42-45.*

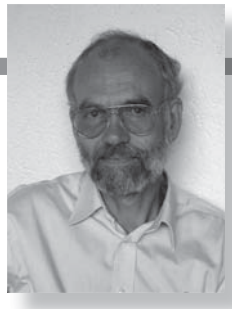
2 *L.R. Newcome (2004): Unmanned Aviation – A Brief History of Unmanned Aerial Vehicles. Reston VA: AIAA.*

3 *Jane's Unmanned Vehicles and Aerial Targets (2007). Coulsdon: Jane's.*

4 *Auch an bewaffneten unbemannten Flugkörpern für den Weltraum wird gearbeitet, jedoch stellt dieses Medium besondere Bedingungen, und es gibt noch eine gewisse Zurückhaltung bei den Weltraummächten. Solche Systeme sollten durch das von der großen Mehrheit der Staaten geforderte allgemeine Verbot von Weltraumwaffen erfasst werden.*

5 *US Department of Defense (2009): FY2009-2034 Unmanned Systems Integrated Roadmap. Washington DC.*

6 *Diese Ziele werden nicht erreicht werden, insbesondere für Landfahrzeuge. Das große Programm »Future Combat Systems« der US-Armee,*



Jürgen Altmann

PD Dr. **Jürgen Altmann** (Experimentelle Physik III, Technische Universität Dortmund) ist Physiker und Friedensforscher. U.a. hat er das Forschungsprojekt »Unbemannte bewaffnete Systeme – Trends, Gefahren und präventive Rüstungskontrolle« bearbeitet, gefördert durch die Deutsche Stiftung Friedensforschung (DSF). In der FIfF-Kommunikation 4/2009 erschien von ihm ein Beitrag zur Nanotechnik und in der FIfF-Kommunikation 1/2009 unter dem Titel „Bomben, Chips und Algorithmen" eine verschriftlichte Fassung seines Vortrages auf der FIfF-Jahrestagung 2008 in Aachen

das eine Reihe unbemannter Land- und Luftfahrzeuge umfasste, wurde 2009 eingestellt. Jedoch sind die Ausgaben für Beschaffung und Einsatz unbemannter Systeme unter der Obama-Administration deutlich angestiegen.

7 *Allerdings kann ein Ziel über längere Zeit beobachtet werden als mit einem Flugzeug mit Pilot.*

8 *http://counterterrorism.newamerica.net/drones.*

9 *J. Mayer: The Predator War – What are the risks of the C.I.A.'s covert drone program? The New Yorker, October 26, 2009. Auszüge aus dem Bericht des UN-Sonderberichterstatters Alston sind in der Ausgabe 1/2011 von W&F abgedruckt; der vollständige Bericht in deutscher Übersetzung steht unter www.un.org/depts/german/menschenrechte/a-hrc14-24add6-deu.pdf.*

10 *Iran Starts Mass Production of Advanced Unmanned Bombers, Tehran: Fars News Agency, 8 Febr. 2010; http://english.farsnews.com/newstext.php?nn=8811191064.*

11 *US Department of Defense (2009), op.cit. S. 18.*

12 *US Department of Defense (2007): Unmanned Systems Roadmap 2007-2032, Washington DC. S. 54.*

13 *In einem gewissen Sinn machen Minen schon etwas Ähnliches. Dass sie nicht unterscheiden können und auch nach einem bewaffneten Konflikt weiter funktionieren, hat zu ihrem Verbot geführt. Bewaffnete autonome U(A)Vs wären anders: Sie wären beweglich, und sie würden eine Situation bewerten und dann nach einem Algorithmus entscheiden, ob eine Person getötet bzw. ein Objekt zerstört werden soll. Vorläufer (automatische Flug-/Raketenabwehrsysteme, umher fliegende Anti-Radar-Flugkörper) sind auf eine spezifische Zielklasse mit klaren Eigenschaften beschränkt, aber sogar hier sind Fehler vorgekommen, wie der Abschuss eines iranischen Passagierflugzeugs vom US-Schiff Vincennes 1988.*

14 *P. Lin, G. Bekey, K. Abney: Autonomous Military Robotics: Issues of Risk and Ethics. In R. Capurro, M. Nagenborg (eds.) (2009), Ethics and Robotics. Heidelberg: AKA/IOS. R.C. Arkin (2009): Governing Lethal Behavior in Autonomous Robots. Boca Raton FL: Chapman&Hall/CRC.*

15 *Arkin (2009), op.cit.*

16 *N. Sharkey (2007), Automated Killers and the Computing Profession. Computer, 40 (11), S. 124ff.*

17 *J. Altmann, Preventive Arms Control for Uninhabited Military Vehicles. In: Capurro et al. (2009), op.cit.*

18 *www.icrac.co.cc.*

19 *Altmann, op.cit. R. Sparrow (2009): Predators or Plowshares? Arms Control of Robotic Weapons. IEEE Technology and Society, 28 (1), S. 25-29. Krishnan (2009), op.cit.*

20 *Vertragstexte z.B. unter www.armscontrol.de, Dokumente bzw. unter www.armscontrol.org, Treaties & Agreements*

21 *Das würde auch die ballistischen Raketen mit 500-5.500 km Reichweite erfassen, was einen großen Teil der (zukünftig befürchteten) Raketenbedrohung mit aus der Welt schaffen würde. Weitere Reduzierungen der Langstreckenraketen bei den offiziellen Kernwaffenstaaten wären dafür hilfreich, wenn nicht sogar notwendig.*

22 *www.bmeia.gv.at/aussenministerium/aussenpolitik/abruestung/massenvernichtungswaffen/hcoc.html; auf die Regeln des HCOC haben sich gegenwärtig 130 Länder verpflichtet. Das mit 34 Staaten erheblich kleinere Missile Technology Control Regime schreibt Exportbeschränkungen für Marschflugkörper und bestimmte andere UAVs vor; www.mtcr.info.*

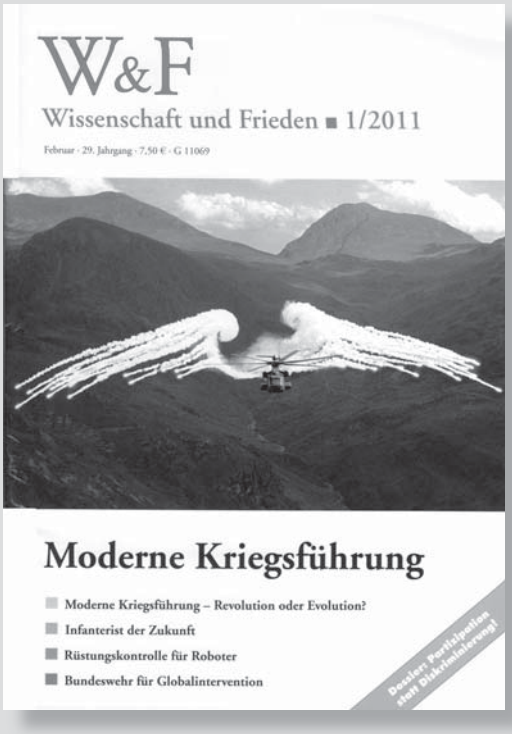
23 *Erklärung des Expertenworkshops 2010 über die Begrenzung bewaffneter ferngesteuerter und autonomer Systeme, Berlin, 22.September; http://e3.physik.tu-dortmund.de/P&D/Workshop-Erklaerung_22_September_2010_deutsch.pdf.*

24 *„Es ist klar, … dass gewisse Ausnahmen gemacht werden können, wo die Automatisierung von Waffen und Sicherheitssystemen seit langem eingeführt ist oder wo zwingende Gründe für die Notwendigkeit der Automatisierung vorliegen, damit menschliches Leben vor unmittelbaren Bedrohungen geschützt wird." (Aus der Workshop-Erklärung, op.cit)*

25 *„… in Europa ein sicheres und stabiles Gleichgewicht der konventionellen Streitkräfte auf niedrigerem Niveau als bisher zu schaffen, Ungleichgewichte, die für Stabilität und Sicherheit nachteilig sind, zu beseitigen und – besonders vorrangig – die Fähigkeit zur Auslösung von Überraschungsangriffen und zur Einleitung groß angelegter Offensivhandlungen in Europa zu beseitigen;" (aus der Präambel des KSE-Vertrags vom 19.11.1999).*

26 *Definitionen von Kategorien der begrenzten Waffen und Ausrüstungen, Listen vorhandener Typen, regelmäßiger Informationsaustausch, Inspektionen usw.*

Der vorliegende Beitrag erschien zuerst in *Wissenschaft und Frieden*, Heft 1/2011 (Schwerpunkt: Moderne Kriegsführung). Weitere Informationen zu dieser Zeitschrift sowie Bestell- und Abonnementmöglichkeiten unter *www.wissenschaft-und-frieden.de*. Das FIfF ist Mitherausgeber von *Wissenschaft und Frieden*.



Eva Dworschak

Die Volkszählung 2011

Was sie beinhaltet und was man dagegen tun kann

Im Mai 2011 findet die Volkszählung ihren Höhepunkt. Bisher wurde darüber wenig berichtet, doch es ist zu erwarten, dass sich bis dahin der Widerstand ausbaut und noch weitere Verfahren zu den bereits erhobenen Klagen hinzukommen, ja es ist sogar abzusehen, dass sich einige Weitere an das Bundesverfassungsgericht wenden. Grund hierfür ist die erneute Frage nach der Vereinbarkeit der Volkszählung mit den geltenden Rechten und insbesondere unserer Verfassung. Vor allem das Grundrecht auf informationelle Selbstbestimmung ist betroffen. Im Folgenden wird daher dargestellt, wie die Volkszählung ausgestaltet ist und auf welche Weise der Betroffene sich in den jeweiligen Stadien der Zählung wehren kann.

Verlauf der Datenerhebung und Inhalt der Register

Bis zum Mai wurden und werden die ersten Daten ohne explizite Mitteilung an die Betroffenen von etlichen Behörden generiert, um aus den Registern neue zusammenzufassen und die Datensätze mitsamt den Daten aus der Zensusvorbereitung (nach dem Zensusvorbereitungsgesetz) zur weiteren Verwendung aufzubauen. Sodann werden anhand dieser sich in den Landesstatistikstellen und Erhebungsstellen befindlichen Grunddaten die persönlichen Befragungen ab Mai 2011 durchgeführt; dies geschieht mittels Stichprobenverfahren, Haushaltsbefragungen, Befragungen in Sonderbereichen und weiterer Befragungen, bei denen die Auskunftspflichtigen durch Erhebungsbeauftragte persönlich besucht werden. Die Daten werden auch aus den erlangten Daten des Mikrozensus ergänzt.

Aufkleber zur Volkszählung 2011, (cc) by-nc-nd Michael Ebeling

Die letztendlich als Metadaten feststehenden Register werden an das Bundesstatistikamt weitergeleitet, um dort zentral und gebündelt für die weitere Verwendung gespeichert zu werden. Sie beinhalten nun ein erhebliches Maß an persönlichen und personenbezogenen Daten, beispielsweise aus den Meldebehörden, Katasterämtern, Bundesagenturen für Arbeit und anderen Behörden. Zusätzlich auch Gebäude- und Wohnungsangaben, erwerbsstatistische Daten (Erwerbsbeteiligung, berufliche Auszeiten, Schulabschlüsse, Stellung im Beruf, Wirtschaftszweig des Unternehmens, Migrationshintergrund, Religionszugehörigkeit (soweit Auskunft erteilt wurde) und weitere. Dann werden bei Unklarheiten weitere Schlüssigkeitsprüfungen durchgeführt und Nacherfassungen durch persönliche Befragungen vorgenommen.

Hintergrund

Der Zensus 2011 stellt damit einen Methodenwechsel dar, da die Befragungen nun durch den sog. „registergestützten Zensus" ergänzt werden. Die Vollerfassung wird aber nunmehr auch durch die Ausweitung der Merkmale gründlicher ausgestaltet. Sie basiert in Deutschland auf der rechtlichen Grundlage dem „Gesetz über den registergestützten Zensus im Jahre 2011", dem Zensusgesetz, welches nach der vorgebenden „Verordnung der der Europäischen Union über Volks- und Wohnungszählungen vom 09.07.2008" erlassen wurde.

Aber die direkte Verpflichtung aus der europäischen Verordnung verlangt den jeweiligen Ländern weit weniger Erhebungsmaterial ab. Dort ist ein Grundkatalog festgelegt, den Deutschland gründlich mit zusätzlich zu erhebenden Daten erweitert hat. Zudem wurden die Erhebungsmerkmale als tiefer greifende Detailfragen ausgestaltet, die weit mehr Information liefern als die in der europäischen Vorgabe grob umrissenen Erhebungsmerkmale.

Historie

Die bisherigen Volkszählungen im Jahre 1981 und 1987 haben nicht zu einer Vollerfassung in dieser Gründlichkeit geführt. Und im Jahre 1983 wurde sie durch Protest und höchstrichterliche Entscheidung sogar gestoppt. Aus diesem Jahr stammt das sogenannte „Volkszählungsurteil" des Bundesverfassungsgerichts, welches erstmalig die Eckpfeiler des Grundrechtes „auf informationelle Selbstbestimmung" setzte.

Gefahren

Die Auslegung des Zensusgesetzes mit all seinen Regelungslücken erlaubt Vorgehensweisen und birgt Gefahren, die zu einer Verfassungswidrigkeit der Maßnahme und damit des zugrundeliegenden Gesetzes führt.

Die größte Gefahr liegt darin, dass ein *zentraler Datenpool* geschaffen wird, der eine Vielzahl von personenbezogenen und persönlichen Daten aufeinander bezogen erfasst. Diese zentral gespeicherte Vollerfassung birgt erhebliche Sicherheitsrisiken und füttert weitere Begehrlichkeiten.

Schwerwiegend ist, dass dabei der Datensatz einer Person eine personenbezogene Ordnungsnummer erhält, die auch erhalten bleiben soll und eine Personenkennziffer darstellt. Wenn im Nachhinein die personenbezogenen Hilfsmerkmale gelöscht werden, was noch nicht einmal ausnahmslos gewährleistet wird, ist eine Zuordnung schlicht durch die Ordnungsnummer und Bezugnahme möglich.

Hinzu kommt die technisch einfach durchzuführende Reidentifizierung, die auch noch mit wenigen Datenangaben, mit einfach zu erhaltender Software und mit kurzem zeitlichen Aufwand zu bewerkstelligen ist. Das Verbot der Reidentifizierung nach §21 BStatG ist damit unterhöhlt. Selbst wenn also der Datensatz nicht mehr die entsprechenden personenbezogenen Hilfsmerkmale enthält, genügen wenige personen- oder wohnortbezogene Angaben, um mit dem Stand der heutigen Internettechnologie und Software eine Deanonymisierung der Daten durchzuführen. Das bedeutet, dass auch noch Jahre später anhand einzelner Angaben im Datensatz Rückschlüsse auf die einzelne Person hergestellt werden können.

Es besteht die Gefahr der *Zweckentfremdung* der Daten in mehrfacher Hinsicht. Die sich zunächst in den behördlichen Registern befindlichen Daten wurden ursprünglich für eine andere Aufgabenwahrnehmung des Staates gesammelt. Bei der nunmehr erfolgten Abfrage und Verbindung mit anderen Daten erfahren sie eine völlig neue Zweckbestimmung und auch Aussagekraft. Die Einhaltung der Zweckbindung ist verfassungsrechtlich vorgegeben; sie kann nur bei Vorliegen ganz besonderer, erheblicher Gründe eine Änderung erfahren. Die weitere Zweckentfremdung liegt darin, dass die Daten später auch anderen staatlichen Zwecken zugeführt werden können, sofern hierfür eine gesetzliche Regelung geschaffen wird oder vorliegt (bspw. Antiterrorgesetze). Eine Ausweitung der Nutzung ist folglich durchaus denkbar.

Das *Verbot der Datenweitergabe* wird an unterschiedlichen Stellen unterlaufen, beispielhaft genannt sei hier nur die Übermittlung der Datensätze zurück an die Erhebungsstellen und Erhebungsbeauftragten, um die Nacherfassungen durchzuführen. Auch bei Vollzug des Bußgeldverfahrens und durch Regelungslücken in den Ausführungsgesetzen erhält die Datenweitergabe weitere Möglichkeiten.

Weitere Gefahrenquellen ergeben sich aus dem Vollzug der Vollerfassung durch die *Erhebungsbeauftragten* und durch mangelnde Regelungen in den jeweiligen Ausführungsgesetzen der Länder. Die Erhebungsbeauftragten, die durch die Erhebungsstellen selbst rekrutiert werden, können jeglicher spezifischer Ausbildung entbehren, lediglich eine kurze Schulung soll sie auf die verantwortungsvolle Tätigkeit einstellen. Dabei wird in einigen Bundesländern bereits an Gymnasien und Universitäten nach ehrenamtlichen Helfern gesucht. Teilweise wird angestrebt diese aus dem sonstigen Verwaltungsbetrieb zu entleihen. Eine weitere Entwicklung in der Bestellung der Erhebungsbeauftragten sollte nicht unbeachtet bleiben, denn es haben sich bereits andere Interessengruppen, wie beispielsweise die NPD, organisiert, um dieses Feld zu bestücken.

Das *Gebot der Datensparsamkeit* wird durch die Vielzahl und durch eine derart in den Merkmalen tiefgreifende Vollerfassung ausgehöhlt.

Das *Trennungsgebot* oder Abschottungsgebot der Behörden untereinander wird nicht strikt eingehalten. Zwar ist bisher nach derzeitigem Kenntnisstand die Einrichtung der Erhebungsstellen räumlich autark von den übrigen Verwaltungsbehörden erfolgt, doch ergeben sich dennoch faktisch Berührungspunkte. Die Berührungsproblematik geht darüber hinaus, denn soweit Beamte und Angestellte im öffentlichen Dienst an die Erhebungsstellen ausgeliehen werden, kehren sie nach Abschluss des Zensus mit den neu gewonnenen Erkenntnissen wieder an ihren ursprünglichen Arbeitsplatz zurück. Ein Verstoß gegen das Verbot der Rekrutierung von Erhebungsbeauftragten aus „unmittelbarer Nähe" der Befragten ist daher zugleich anzunehmen.

Rechtliche Möglichkeiten der Betroffenen

Im Prinzip ist jeder Bürger betroffen, nur manche sogar mehrfach. Daher ergeben sich unterschiedliche Abwehrmöglichkeiten, die auch noch durch die verschiedenen Stadien der einzelnen Datenbezüge ihre jeweilige Modalitäten aufweisen. Aufgrund der Fülle der Möglichkeiten, kann aber nur ein grober Überblick gewährt werden.

Plakat-Entwurf (cc) by 2.0 Ak-Zensus
http://wiki.vorratsdatenspeicherung.de/Zensus11/Materialien

Eva Dworschak

Eva Dworschak ist Rechtsanwältin und beschäftigt sich seit Jahren mit der grundrechtlichen Relevanz vieler Problemfelder und Bürgerrechte. Ihre beruflichen Schwerpunkte liegen im Medizin- und Patientenrecht, sowie im Presse- und IT/Medienrecht. Dieser Text ist ein Auszug aus einem demnächst von der Autorin erscheinenden juristischen Ratgeber. Dieser wird in vertiefender Darstellung und Beispielgebung die rechtlichen Möglichkeiten und das Ausmaß der Volkszählung in vielerlei Hinsicht darstellen.

Bisherige Klagen und Verfahren

Bereits im Sommer wurden zwei Gesetzes-Verfassungsbeschwerden eingelegt, wobei eine als nicht zulässig und die andere als nicht ausreichend begründet abgelehnt wurden. Das heißt, bei Überzeugung der Rechtswidrigkeit der Maßnahme muss nun zunächst der gerichtliche Weg gegen die Einzelmaßnahme gewählt werden und abermals vor das hohe Gericht getreten werden, um das Zensusgesetz anhand der Grundrechtsverletzungen prüfen zu lassen und um es zu einer verfassungsgemäßen Ausgestaltung zu verhelfen.

Weitere Verfahren werden derzeit von einzelnen Bürgern vorbereitet. Die Autorin vertritt zudem zwei Genossenschaften, die in Hamburg und Berlin eine Überprüfung der Volkszählung und des Zensusgesetzes anstreben.

Rechtliche Möglichkeiten

Neben der Verfassungsbeschwerde, die nach Abschluss eines Verwaltungsverfahrens statthaft ist, wenn nicht vorher das jeweils zuständige Gericht die Vorlage des Gesetzes zur Prüfung an das hohe Gericht direkt beschließt, besteht auch die Möglichkeit, ein sogenanntes Eilverfahren vor dem Bundesverfassungsgericht durchzuführen, um die Volkszählung bei bestehenden erheblichen Gefahren zu stoppen.

Generell ist jedem Bürger jederzeit möglich, Auskunft über die Datenerhebung und deren Weitergabe und auch die zugrundeliegenden landesrechtlichen und behördlichen Regelungen zum Vollzug (z.B. Verwaltungsanweisungen) Auskunft zu verlangen, dies klagweise durchzusetzen und vor allem: Die Generierung der Daten vor Beginn der Befragungen kann ebenfalls schon gestoppt werden, indem man Klage erhebt. Dies hat sich trotz aller Warnungen gerade aus IT-Fachkreisen bisher noch kein Betroffener getraut, was unverständlich bleibt. Schließlich wird mit Erstellung und dem schrittweise durchgeführten Aufbau der Register die Datenanzahl stetig erhöht und damit vollendete Tatsachen geschaffen. Bereits hier ergeben sich die meisten der oben erwähnten Gefahren.

Plakat-Entwurf (cc) by 2.0 Ak-Zensus
http://wiki.vorratsdatenspeicherung.de/Zensus11/Materialien

Sollten Sie direkt von der Auskunftspflicht per Verwaltungsbescheid betroffen sein, ist ein Widerspruch (nach §68 VwGO) einzulegen. Da dieser nach §15 Abs. 6 BStatG keine „aufschiebende Wirkung" hat, hemmt er die Wirkung des Verwaltungsbescheides nicht und Sie sind weiterhin verpflichtet, Angaben zu machen, bis in der Rechtsangelegenheit abschließend entschieden ist. Dies kann nur verhindert werden, wenn mit dem Widerspruch ein „Antrag auf Wiederherstellung der aufschiebenden Wirkung" (nach §80 V VwGO) gestellt wird.

Sollten Sie die Aufforderung schlicht ignorieren und/oder die Auskunft verweigern, ist der Erhebungsstelle die Möglichkeit geboten, ein Bußgeld zu erheben und letztendlich sogar ein Zwangsverfahren durchzuführen, was bedeutet, dass weitere Zwangsmittel durchgeführt werden. Gegen den Bußgeldbescheid (und auch die Zwangsmittel) sind eigenständige Verfahren möglich (beginnend mit dem Einspruchsverfahren), die wiederum (wie in den anderen Verfahren) die Überprüfung der zugrundeliegenden Rechtsgrundlage ermöglichen.

Auskunftspflichtige, die Angaben über andere Personen machen sollen und/oder über deren Wohnungen oder Häuser Auskunft zu erteilen haben, können sich ebenfalls zur Wehr setzen. Hier ist aber auch derjenige, über den ein Anderer Auskunft erteilen soll, gefragt. Dieser kann sich mittels Drittwiderspruch oder Unterlassungsanspruch zur Wehr setzen, vorausgesetzt er erfährt davon.

Sollte sich ein Erhebungsbeauftragter angekündigt haben, können sie natürlich auch dagegen vorgehen.

Das mildeste Mittel, die Gefahren einzudämmen ist sicherlich die Geltendmachung des Anspruchs auf Löschung der Hilfsmerkmale, nachdem diese nicht mehr für die Schlüssigkeit gebraucht werden. Dies ist aber erst frühestens nach Abschluss der Erhebung im Jahre 2011 möglich; dann ist zudem zu klären, ob die Löschung nicht erst nach weiteren vier Jahren oder weiteren zwei Jahren durchzusetzen ist, wenn die Löschung der Hilfsmerkmale nach Behördenauffassung noch angezeigt ist und sie bei Anzeige oder im gerichtlichen Verfahren nachgewiesen hat, vorher noch Prüfungen durchführen zu müssen.

Ich rate generell bei allen Verfahren die Vertretung durch eine/n Anwältin/Anwalt an. Vor den Kosten braucht man sich nicht unbedingt zu scheuen. Hier besteht auch die Möglichkeit Prozesskostenhilfe im Vorfeld zu beantragen, bei einem Sieg jedenfalls sind die Kosten aber nicht vom Klagenden zu tragen.

Christiane Schulzki-Haddouti

(Alp-)Traum WikiLeaks

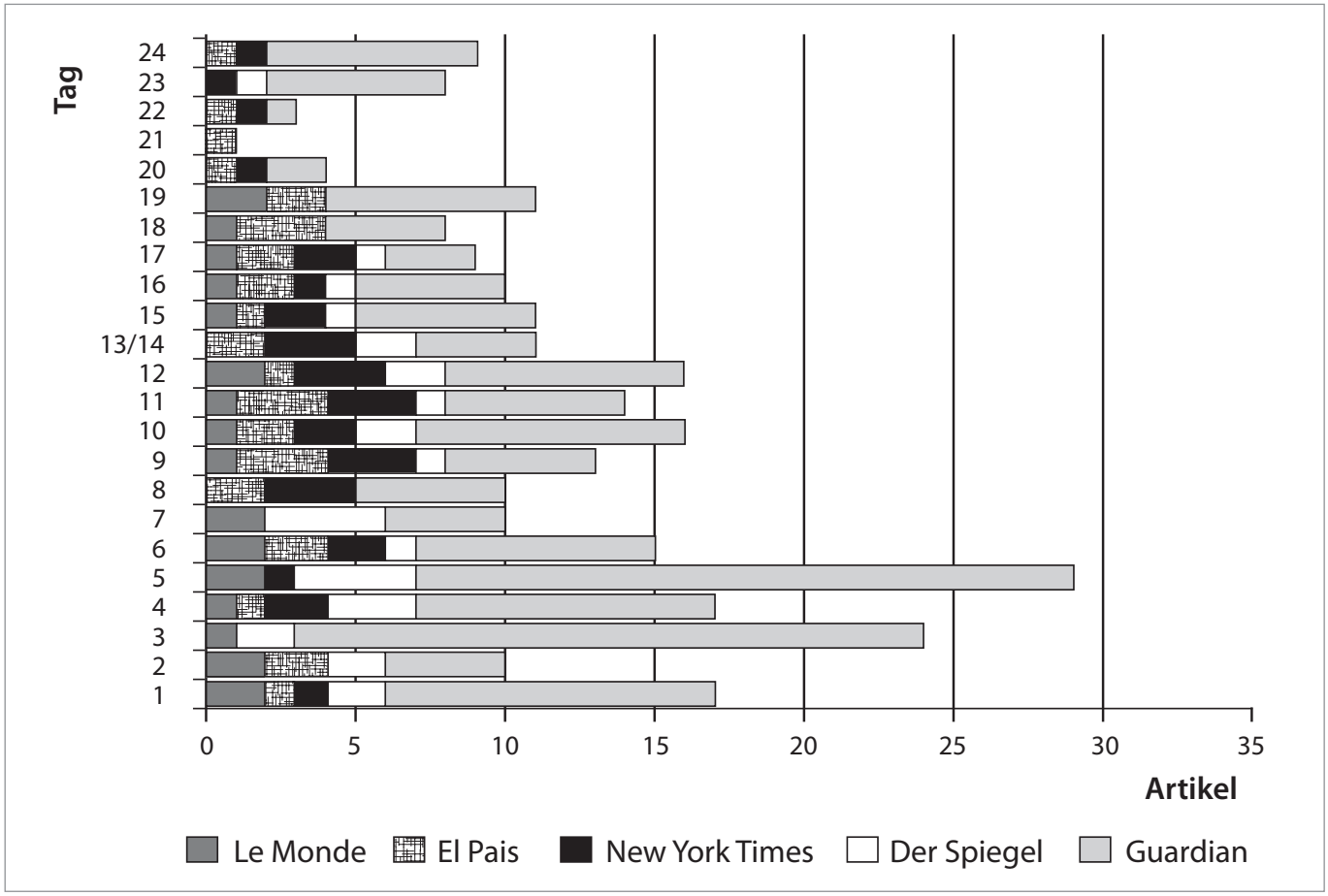
Welche Redaktion träumt nicht davon, auf einen Schlag eine Masse hochbrisanter Dokumente aus höchsten Machtzirkeln in der Hand zu halten? Als WikiLeaks-Gründer Julian Assange das über 251.000 Dokumente umfassende Konvolut aus dem US-Außenministerium ausgesuchten Redaktionen anbot, dürfte diesen etwas schwummerig geworden sein. Denn das Problem ist nicht nur das der Klasse – vermutlich hochwertige Informationen müssen fachkundig bewertet werden –, sondern auch der Masse: Wie sind die Daten journalistisch und organisatorisch auf verantwortliche Weise zu bewältigen?

24 Tage protokollierte die britische Tageszeitung The Guardian auf ihrer Website, was die New York Times, Der Spiegel, Le Monde, El País und sie selbst über die 251.000 Depeschen des US-Außenministeriums veröffentlichten. Am 22. Dezember schließlich der letzte Eintrag, der unter anderem auf ein Interview des Spiegels mit Bundesinnenminister Thomas de Maizière hinwies, der WikiLeaks als „ärgerlich, aber keine Bedrohung" bezeichnete. Einen Tag zuvor hatte US-Vize-Präsident Joe Biden WikiLeaks-Chef Julian Assange noch als „Hightech-Terrorist" bezeichnet.

Eine Auswertung dieser Chronologie zeigt, dass der Guardian mit Abstand das Meiste aus den Depeschen machte: Er veröffentlichte in den ersten 24 Tagen 158 Artikel, das sind 7 Artikel täglich. Etwa auf einer Augenhöhe befinden sich der Spiegel mit 30 Beiträgen, die New York Times mit 32 Beiträgen und El País mit 33 Beiträgen – und etwa 1,4 Artikeln pro Tag im Schnitt. Deutliches Schlusslicht ist Le Monde mit 23 Beiträgen – mit gerundet etwa einem Beitrag täglich. Allerdings sind etliche Artikel des Spiegels dabei nicht berücksichtigt. Nach Auskunft des Spiegel-Sprechers Hans Ulrich Stoldt veröffentlichte der Spiegel im Heft, online sowie Special-Heft in diesem Zeitraum insgesamt 143 Beiträge. Damit ist der Guardian aber immer noch ungefochtener Spitzenreiter.

Die meisten Beiträge wurden in der ersten Woche veröffentlicht, in der zweiten Woche ging die Frequenz zurück, in der Woche vor Weihnachten stellten einige Redaktionen die Berichterstattung ganz ein. Der Spiegel veröffentlichte laut der Zählung des Guardian nur noch eine einzige Geschichte. Von Weihnachten bis zum 18.1. veröffentlichte er nach Angaben von Stoldt nur noch weitere 5 Beiträge. Eine Planung, in welchem Tempo weiterhin veröffentlicht werden soll, gebe es nicht.

Keine Auswertung gibt es darüber, in welchem Ausmaß diese Berichte von anderen Medien aufgegriffen und weiter recherchiert wurden. Vielleicht eine Aufgabe für künftige Journalistik-Studien. Unzählig hingegen sind die Berichte über den Fall des WikiLeaks-Gründers Julian Assange.



Aus der Auswertung wird jedenfalls die Führungsrolle des Guardians bei der redaktionellen Auswertung der US-Depeschen deutlich. Dies zeigt sich nicht nur an der Menge der bearbeiteten Informationen, sondern auch an der Art, wie diese präsentiert werden: Nämlich möglichst übersichtlich für die Leser – und im Sinne der vom Guardian seit Jahren offensiv propagierten „Open Data"-Philosophie, die bereits zahlreiche aufsehenerregende Datenjournalismus-Projekte inspirierte.

In diesem Zusammenhang ist es auch erwähnenswert, dass der Guardian die Metadaten der WikiLeaks-Cables in einer offenen Datenbank zur Auswertung frei gegeben hat – während etwa der Spiegel die Depeschen lediglich in einer von außen unzugänglichen Flash-Grafik aufbereitet hat. Auf diese Weise entstanden auf Grundlage der Guardian-Daten einige interessante Auswertungen. Unter anderem visualisierte eine Grafik Themenstränge für die Jahre 2001 bis 2003 und zeigt damit den Impact des 11. September auf Amerikas Diplomatie *(http://www.closr.it/show/LIkJxaoZVbI)*. Gefährdet wird durch die Freigabe der Metadaten niemand, doch nicht nur für Journalisten, sondern auch für Politikwissenschaftler und Historiker können solche Auswertungsmöglichkeiten wertvoll sein.

Exklusive Themenauswahl

Wie gingen die von WikiLeaks bedachten Redaktionen bislang mit den Depeschen um? Auffallend ist, dass sie darauf achteten, eigene Themen zu setzen. Eine Geschichte des Guardian mit Deutschlandbezug, die kurz vor Weihnachten erschien, wurde beispielsweise vom Spiegel nicht aufgegriffen. Darin ging es um das zeitweise Engagement des Energiekonzerns RWE in einem Kernkraftwerkprojekt in Bulgarien, das laut der Depeschen von ständigen Sicherheitsproblemen begleitet war. Für die Briten war es offenbar deshalb eine Geschichte, weil RWE Besitzerin von Großbritanniens größtem Energieversorger npower ist, der das Projekt durchführte.

Es scheint, als wäre die große Enthüllungswelle erst einmal zum Erliegen gebracht. Seit Weihnachten werden die Depeschen auf der WikiLeaks-Website denn nur noch tröpfchenweise veröffentlicht. Der stete Enthüllungsstrom, auf den man sich ursprünglich einstellte, scheint zum Stillstand gekommen zu sein. Woran dies liegt, darüber lässt sich spekulieren. Da diesen Redaktionen alle Depeschen vorliegen und auch in der Regel nur Depeschen von WikiLeaks veröffentlicht wurden, deren Inhalte mit einer veröffentlichten Geschichte korrelierten, könnte es daran liegen, dass der Sprengstoff der Depeschen schlicht verbraucht ist.

Aftenposten sprengt Kreis der Auserwählten

Dass dies nicht der Fall ist, zeigen die jüngsten Veröffentlichungen der norwegischen Tageszeitung „Aftenposten". Sie hat seit Ende Dezember laut eigenen Angaben Zugriff auf alle Dokumente – durch ein Leck innerhalb von WikiLeaks. Offenbar gibt es innerhalb von WikiLeaks Personen, die die bisherige Veröffentlichungspolitik torpedieren. Von diesem Leck profitierte inzwischen auch „Die Welt", die dank einer Kooperation mit der Aftenposten seit Mitte Januar ebenfalls „ohne jede Beschränkung" Zugriff auf alle Depeschen hat.

Die ersten Veröffentlichungen der Aftenposten lösten internationale Resonanz aus. So erläuterten Dokumente der US-Botschaft in Oslo die Verhandlungen zwischen Norwegen und Russland über die gemeinsame Grenze im Barents-Meer. Eine AFP-Meldung griff einen weiteren Aftenposten-Bericht auf, wonach Deutschland und die USA für rund 205 Mio. Euro gemeinsam ein hochauflösendes Satellitensystem unter dem Projektnamen HiROS gegen Widerstände aus Frankreich entwickeln wollten. Dieser Satellit soll unter der Kontrolle des Bundesnachrichtendienstes und des Deutschen Zentrums für Luft- und Raumfahrt (DLR) stehen. Etliche Tage später berichtete auch Spiegel Online über das Projekt – und dass die Bundesregierung es nicht unterstützen wolle. Dabei wurde die entsprechende Depesche weder verlinkt, noch wurde der Bericht der Aftenposten erwähnt.

Die Redaktionen scheinen mit den Depeschen mit einer nahe liegenden Methode umzugehen: Sie recherchieren die Themen, die sie kennen. Werden sie fündig und erscheint das Material interessant genug, berichten sie darüber. Es ist offensichtlich, dass auf diese Weise noch längst nicht alles publiziert wurde, was Nachrichtenwert besitzt. Die bislang veröffentlichten Geschichten reflektieren damit vermutlich vor allem die aktuelle Interessenslage und Themenkompetenz der jeweiligen Redaktion.

Exklusivvertrag mit WikiLeaks?

Die Aftenposten gehört nicht zu dem erlauchten Kreis der vier großen Publikationen, dem Guardian, Le Monde, El País und

Christiane Schulzki-Haddouti

Christiane Schulzki-Haddouti, Jahrgang 1967. Medienwissenschaftlerin und Journalistin. Als freie Journalistin schreibt sie vor allem für heise online, die VDI-Nachrichten, Stuttgarter Zeitung und Futurezone. Ihr Schwerpunkt liegt auf den Themen Bürgerrechte, Informationsfreiheit, Datenschutz und Medienethik. Sie ist seit 2000 Jury-Mitglied der „Initiative Nachrichtenaufklärung" (INA), für die sie viele Jahre Recherche-Seminare an den Universitäten Dortmund und Bonn durchführte und koordinierte. Begleitend zu der Studie "Kooperative Technologien in Arbeit, Ausbildung und Zivilgesellschaft" gründete sie im Sommer 2007 gemeinsam mit Lorenz Lorenz-Meyer die Plattform KoopTech unter *http://blog.kooptech.de*. Ihre Website: *http://schulzki-haddouti.de*.

Spiegel, die mit WikiLeaks die Veröffentlichung vereinbart hatten. Die New York Times selbst hat die Dokumente vom Guardian bekommen. Aftenposten-Redaktionsleiter Ole Erik Almlid sagte laut der Nachrichtenagentur dapd: "Wir haben diese Dokumente ohne Auflagen und ohne etwas dafür zu bezahlen bekommen". Die Zeitung werde die ihr wichtig erscheinenden Depeschen veröffentlichen und unter Umständen heikle Informationen wie Namen unkenntlich machen.

Die Äußerung von Almlid wirft aber auch ein interessantes Licht auf die mutmaßliche Vereinbarung zwischen WikiLeaks und den vier Redaktionen. Spiegel-Sprecher-Stoldt jedenfalls sagt: „Es gibt keinerlei Vereinbarungen mit Wikileaks. Ausnahme: Der Termin zur ersten Veröffentlichung der Depeschen war mit Wikileaks und den anderen Medienpartnern abgesprochen." Der US-Fernsehsender CNN und das Wallstreet-Journal hatten nach eigenen Angaben eine Zusammenarbeit jedoch abgelehnt, da sie nicht bereit waren, die von WikiLeaks geforderten Vertragsklauseln zu unterzeichnen. Diese sollen unter anderem eine nicht mit WikiLeaks abgestimmte Publikation verbieten. Außerdem ist die Rede von einer Vertragsstrafe von 100.000 Dollar bei Zuwiderhandlung.

Ob eine mindestens mündlich getroffene Vereinbarung zwischen den Verlagen und der Enthüllungsplattform presserechtlich ebenfalls als Exklusivvertrag zu werten ist, darüber wird der Presserat im März entscheiden müssen. Im Falle des Spiegels geht es immerhin um einen exklusiven Zugang innerhalb des deutschsprachigen Raums. Nach Ansicht der Beschwerdeführerin verstößt der Spiegel gegen die Richtlinie 1.1. des Pressekodex. Sie untersagt Exklusivverträge mit Informanten über „Vorgänge oder Ereignisse, die für die Meinungs- und Willensbildung wesentlich sind". Weiter heißt es: „Wer ein Informationsmonopol anstrebt, schließt die übrige Presse von der Beschaffung von Nachrichten dieser Bedeutung aus und behindert damit die Informationsfreiheit."

Eine Frage der Masse

Das Besondere an den WikiLeaks-Depeschen ist ganz offensichtlich die schiere Masse: Um sie auswerten zu können, muss eine Redaktion nicht nur über genügend Manpower und Know-How verfügen. Sie sollte auch in der Lage sein, mit anderen journalistischen Organisationen vertrauensvoll zu kooperieren. Trotz des angeblich fehlenden Vertrags ist der Spiegel dazu aber anders als die Aftenposten nicht bereit. Stoldt zu dieser Frage: „Es sind keine Kooperationen mit anderen Redaktionen vorgesehen."

Aus Sicht der Journalisten als Protagonisten der Meinungs- und Pressefreiheit muss das Hauptinteresse darin bestehen, die Informationen einzuordnen, zu bewerten – und dann erst Öffentlichkeit bei einem Optimum an Transparenz herzustellen. Aus Sicht der Whistleblower muss der Informantenschutz gewahrt – und eine größtmögliche Öffentlichkeitswirkung erzielt werden.

Weil in den Datennetzen von Behörden und Unternehmen immer mehr Dokumente gespeichert werden, werden künftig immer wieder Whistleblower massenhaft Daten an die Öffentlichkeit bringen wollen. Für Journalisten ist das sowohl Anlass zur Freude, als auch zur Sorge. Einerseits erhält man brisantes Material für aufsehenerregende Geschichten. Andererseits müssen die Dokumente wie andere auch auf Authentizität und Echtheit überprüft werden. Außerdem müssen Sicherheitsmaßnahmen ergriffen werden, um den Informanten samt Material zu schützen. Eine Aufgabe, der sicherlich nicht jeder Journalist und auch nicht jede Redaktion gewachsen ist.

Auch muss eine Redaktion sich mit der Frage auseinandersetzen, wie weit das eigene Veröffentlichungsinteresse tatsächlich reicht. Die Masse der Dokumente reicht aus, um die Berichterstattung auf Jahre hinaus zu versorgen. Doch darauf wird sich kein Verlag einlassen, da es immer auch konkurrierende Themen gibt, die möglicherweise von größerer Relevanz sind. Im Ergebnis sind die Archive der jeweiligen Redaktionen um eine wertvolle zusätzliche Quelle erweitert. Im Sinne einer informierten Öffentlichkeit stellt sich jedoch die Frage, ob eine Privatisierung dieses Informationsschatzes richtig ist. Auf dies würde es nämlich hinauslaufen, wenn WikiLeaks das aktuelle Veröffentlichungstempo beibehält – und dies stünde der ursprünglichen Intention der Whistleblower-Plattform entgegen.

Ganz offenbar müssen Journalisten und Whistleblower neue Prozeduren entwickeln, um verantwortlich mit dem Material umzugehen. Einerseits müssen sie Informanten schützen, andererseits müssen sie so viele Informationen wie möglich strukturiert veröffentlichen. Dabei müssen sie viele, sich widerstreitende Interessen austarieren.

Nüchtern betrachtet besteht das Neue an WikiLeaks vor allem in der Masse der Veröffentlichungen, ihrem weltweiten Erfolg und darin, der Weltöffentlichkeit einen tragischen Helden zu liefern. Seit Jahrzehnten gibt es nämlich schon die Website Cryptome.org des New Yorker Architekten John Young, die ebenfalls vertrauliche Dokumente aus aller Welt im Internet veröffentlicht. Er musste ebenfalls bereits mehrere Gerichtsprozesse durchstehen – erfolgreich. Denn die Presse- und Meinungsfreiheit werden in den USA von den Gerichten so hoch bewertet, dass Young bislang immer durchkam.

Ob ein Prozess gegen WikiLeaks in den USA erfolgreich sein wird, ist zweifelhaft. Man müsste Assange schon nachweisen, dass er den verhafteten Whistleblower Bradley Manning zum „Verrat" von Staatsgeheimnissen anstiftete. Dies würde dann in die Kategorie „Spionage" fallen, was zu ahnden wäre. Dafür könnte es genügen, Manning zu einer entsprechenden Aussage zu bringen. Assange äußerte selbst diese Vermutung gegenüber dem britischen Nachrichtenmagazin New Statesman: „Bradley Manning zu knacken, ist nur der erste Schritt. Ganz offensichtlich ist es das Ziel, ihn zu brechen und ein Geständnis zu erzwingen, dass er sich in irgendeiner Weise mit mir verschworen hat, um die nationale Sicherheit der USA zu verletzen."

Nächste Schritte

Immer wieder betonten die Macher von Wikileaks, dass ihre Technik so ausgestaltet ist, dass die Identitäten der Whistleblower gegenüber der Plattform unbekannt bleiben. Anonymität ist damit nicht nur ein Schutz der Quelle, sondern auch automatisch ein rechtlicher Schutz für die Empfänger.

Angesichts des unbestreitbaren Erfolgs der Plattform ist es erstaunlich, dass es im Zeitalter innovativer Zeitungsausgaben für das mobile Internet nicht schon längst auf allen Verlagswebsites anonyme digitale Wurfkästen für Informanten gibt. Die Technik dafür gibt es nicht erst seit heute. Schon seit etwa zehn Jahren unterstützen etwa das Kryptoprogramm „Pretty Good Privacy" und das Anonymisierungstool JAP kostenlos die sichere und anonyme Kommunikation. Dass ehemalige Wikileaks-Mitarbeiter nun mit OpenLeaks ein handliches Tool für Whistleblower anbieten wollen, dass dies aus einer Hand bietet, ist überfällig. Diese Initiative hätte aber auch von professionell-journalistischer Seite kommen können.

Ein weiterer nächster Schritt könnte darin bestehen, sich in Deutschland für die rechtliche Absicherung von Informanten einzusetzen. Einen gesetzlichen Whistleblower-Schutz gibt es nämlich ebenfalls bis heute nicht.

Christiane Schulzki-Haddouti

Datenberge und Nachhaltigkeit

Nach der ereignishaften „Enthüllung" Ende Dezember durch die Massenmedien SPIEGEL, Guardian, New York Times, Le Monde und El País ist die Auswertung der Depeschen ins Stocken geraten. Ich vermute, der Grund liegt in der Strategie, die bei der Erschließung des Datenbestands nahe liegt. Ein großer Vorteil der digital vorliegenden Depeschen besteht in ihrer digitalen Durchsuchbarkeit. Die Redaktionen haben eine so nahe liegende wie effiziente Strategie angewandt: Sie haben zunächst nach den Personen, Institutionen und Themen gesucht, mit denen sie sich bereits beschäftigt haben. Spiegel und Guardian haben auf diese Weise bis Ende Dezember rund 150 Geschichten veröffentlicht. Das ist eine ganze Menge. Gemessen an dem zur Verfügung stehenden Material jedoch ist das aber nur ein kleiner Bruchteil.

Ich vermute, dass die rund 3900 Dokumente, die bis heute (22.2.2011) auf WikiLeaks veröffentlicht wurden, von den Redaktionen verarbeitet wurden. Dies vorausgesetzt, lässt sich im Hinblick auf die noch bevorstehende Auswertungsphase eine einfache Rechnung anstellen. Bislang wurden in einem Zeitraum von 2,5 Monaten 1,5 Prozent der Depeschen ausgewertet. Dieses Veröffentlichungstempo vorausgesetzt, würde es also noch sieben Jahre dauern, bis alle Depeschen redaktionell bearbeitet und veröffentlicht sind. In dieser Zeit gibt es jedoch viele Faktoren, die zu einer Beschleunigung oder Verlangsamung der Veröffentlichungsrate beitragen können.

So hat etwa der SPIEGEL ein großes Expertenteam aufgestellt, das sich ausschließlich mit WikiLeaks beschäftigt. Es ist aus rein wirtschaftlichen Gründen unwahrscheinlich, dass dieses Team auch noch in sieben Jahren die Depeschen bearbeitet. Ein weiterer Risikofaktor ist der Prozess von Julian Assange und der weitere Fortbestand der Organisation WikiLeaks. Obwohl er ja in ein privat motiviertes Verfahren verwickelt ist, hat er dies inzwischen so eng mit der WikiLeaks-Strategie verknüpft, dass hiervon ein erheblicher Einfluss auf WikiLeaks selbst zu erwarten ist.

Komplexe Themen vs. Nachrichtenwert

Ich habe keine systematische Auswertung vorgenommen, von daher kann ich im Hinblick auf möglicherweise vernachlässigte Themen nur meinen Eindruck wiedergeben, den ich angesichts der Zusammenstellung des Guardian bekommen habe. Aufgegriffen wurden die Themen, die einen klassischen Nachrichtenwert haben. Auffällig war dies bei der Auswahl der Titelgeschichte des Spiegel, die die Bewertung bekannter Politiker durch die US-Diplomaten skandalisierte. Die Personalisierung ist eine erfolgreiche Strategie, um das Interesse der Rezipienten zu steigern. Ein weiterer Nachrichtenfaktor war natürlich die Überraschung.

Die Enthüllung der Depeschen selbst war eine Nachricht wert. Unerwartete Ereignisse lösen meist ein besonderes Interesse aus und könnten publikumswirksam inszeniert werden. Die Geschichte über den Auftrag des US-Außenministeriums, UNO-Mitarbeiter auszukundschaften, thematisierte eine gesellschaftliche Normverletzung, die auf eine rechtswidrige Handlung zurückging. Das heißt, die Entscheidung basierte auf einer Suchstrategie, die sich an den Nachrichtenfaktoren orientierte.

Eine komplexe Geschichte hingegen wie die Liste der kritischen Infrastrukturen wurde erst sehr viel später publiziert. Aufgegriffen wurde sie von der Tagespresse, die aber nicht die Bedeutung der der Liste hinsichtlich ihrer politisch-strategischen Bedeutung analysierte. Dies hätte in die komplexe Diskussion um die Strategiefindung für den Schutz kritischer Infrastrukturen geführt, die aktuell auf EU- und Bundesebene geführt wird, die aber nur fachlich interessierten Lesern vermittelbar ist.

Ich vermute daher, dass komplexe Themen bei der Auswertung insgesamt vernachlässigt wurden. Sie verlangen deutlich mehr Nachrecherche und Einordnung, sind also aufwändiger in der Aufarbeitung. Ich vermute auch, dass Themen, die nur für Fachöffentlichkeiten interessant sind, ausgeklammert wurden. Aufgefallen ist mir das am Beispiel des Themas "Cyber Security". Es spielt immer wieder eine Rolle, lässt sich jedoch nur über eine Vielzahl von Depeschen erschließen.

Den Exklusivitätskreis durchbrechen

Für Journalisten, die jedoch keinen Zugriff auf das gesamte Material haben, ist das zum gegenwärtigen Zeitpunkt nicht möglich. Verschiedene Strategien stehen JournalistInnen in dieser Situation zur Verfügung: Beispielsweise könnte man anfangen, die vom Guardian veröffentlichten Metadaten auszuwerten. Das könnte Hinweise auf interessante Policy-Änderungen ge-

ben. Für den Zeitraum rund um den 11. September 2001 wurde dies ja bereits vorgenommen. Das zeigt, dass sich eine solche Analyse lohnen würde. Allerdings müsste man dann anschließend auch in das Material eintauchen können. Und das ist bei der gegenwärtigen Datenlage nur dem exklusiven Kreis von gegenwärtig sieben Redaktionen möglich. Das sind der Spiegel, der Guardian, die New York Times, Le Monde und El País sowie die Aftenposten und Die Welt.

Vor diesem Hintergrund könnten FachjournalistInnen und WissenschaftlerInnen versuchen, eine Kooperation mit den Redaktionen einzugehen, die den Exklusivitätskreis der „Fantastischen Fünf" durchbrochen haben, also mit der Aftenposten und der Welt. Dabei sollte von vornherein eine klare Fokussierung auf bestimmte Themen und Fragestellungen erfolgen. Allein das Meta-Thema Policy-Making wäre für Politikwissenschaftler und Historiker hoch relevant. Da in letzter Zeit auch weitere Leaks wie etwa die Palästina-Papiere bei Al-Dschasira und dem Guardian entstanden, könnte man hier verschiedene Positionen und Strategien vergleichen und nach ausgesuchten Fragestellungen analysieren.

Die „Palästina-Papiere" allein bieten Stoff für mehrere Dissertationen. Aus medienwissenschaftlicher Sicht könnte man untersuchen, inwieweit sich die Sicht der Diplomaten von der Sicht der Journalisten unterscheidet und in welchem Ausmaß sie Themen aufgreifen und vertiefen, die nicht auch von der Presse abgedeckt werden. Damit ließe sich feststellen, inwieweit sich Informationsflüsse im staatlichen Sektor vom öffentlichen Sektor unterscheiden. Frühere Studien haben etwa zum Thema "Open Intelligence" festgestellt, dass 95 Prozent der Informationen, die Nachrichtendienste verarbeiten, aus öffentlichen Quellen stammen. Bei etwas längerem Nachdenken könnte man sicherlich noch auf viele weitere Themen kommen.

Im Dezember 2010 reichte Christiane Schulzki-Haddouti beim Deutschen Presserat eine Beschwerde gegen den SPIEGEL ein. Sie begründet den Schritt folgendermaßen:

> *»Am 12.12. wurden erst 1.344 Depeschen veröffentlicht. Die Redaktionen werden daher – das gegenwärtige Veröffentlichungstempo vorausgesetzt – über Monate hinweg einen exklusiven Zugang zu dem Hauptteil des Materals haben. [...] Laut Richtlinie 1.1 des Pressekodex' darf die "Unterrichtung der Öffentlichkeit über Vorgänge oder Ereignisse, die für die Meinungs- und Willensbildung wesentlich sind", "nicht durch Exklusivverträge mit den Informanten oder durch deren Abschirmung eingeschränkt oder verhindert werden". Denn damit schließe derjenige, der "ein Informationsmonopol anstrebt", "die übrige Presse von der Beschaffung von Nachrichten dieser Bedeutung aus und behindert damit die Informationsfreiheit."«*

Eine Entscheidung des Deutschen Presserats soll Ende März erfolgen.

Der Beitrag „(Alp-)Traum WikiLeaks" erschien in der Ausgabe 01-02/2011 des verdi-Magazins „M – Menschen machen Medien", der Beitrag „Datenberge und Nachhaltigkeit" in der „Berliner Gazette" vom 20.2.2011. Wir danken Christiane Schulzki-Haddouti für die Nachdruckgenehmigungen.

Christiane Schulzki-Haddouti

Anonyme Depots

Konkurrenz zu WikiLeaks formiert sich mit neuen Konzeptionen

In den letzten Wochen gingen eine Reihe von Internetplattformen und Verlagsdienstleistungen an den Start, die sich WikiLeaks zum Vorbild nehmen. Prominent kündigten etwa die WikiLeaks-Dissidenten Daniel Domscheit-Berg und Herbert Snorrason einen Nachfolgedienst mit einer neuen Konzeption an: Openleaks.org.

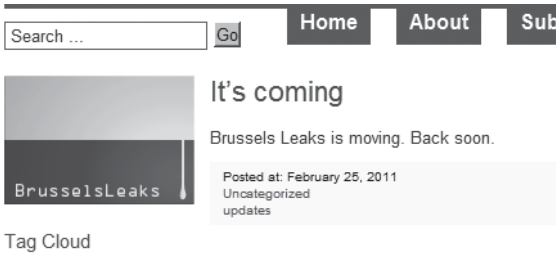
OpenLeaks soll Journalisten, Gewerkschaften und Menschenrechtsgruppen die technische Infrastruktur zur Verfügung stellen, damit Informanten ihre Informationen anonym deponieren können. Damit nehmen die Entwickler der Technik kein juristisches Risiko auf sich – es verbleibt traditionell bei denen, die die Materialien verwenden: Den Journalisten. Diskussionen darüber, ob eine solche Plattform „journalistisch" sei, erübrigen sich dann. Ebenso die Entscheidung, wie und wann die Dokumente veröffentlicht werden sollen. Die Technik soll kostenfrei zur Verfügung stehen. Medienorganisationen sollen jedoch eine „Infrastrukturspende" entrichten. Die Rede ist von monatlich zwischen 200 und 500 Euro, die die jährlichen Kosten von schätzungsweise 100.000 Euro decken sollen. Demnächst soll der Probebetrieb starten.

In Deutschland stellte Der Westen bereits einen Leserservice namens „Dateiupload" bereit, den Informanten anonym nutzen können, sowie eine anonyme E-Mail-Kontaktmöglichkeit. Beide

Funktionen werden über ein Webformular realisiert. In dem einen Fall kann man eine Datei hochladen, in dem anderen Fall eine Nachricht schicken. Dass so etwas auch für die Lokalpresse sinnvoll sein kann, hatte sich im August 2010 gezeigt, als auf WikiLeaks Dokumente zur Planung der Loveparade in Duisburg veröffentlicht worden waren. Seitdem WikiLeaks nur noch die US-Depeschen veröffentlicht, gibt es außer Cryptome keine bekannten Alternativen mehr für Informanten. Eine Veröffentlichung garantiert die WAZ allerdings nicht.

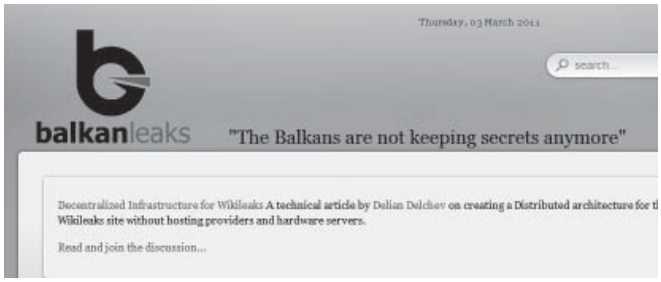
Die WAZ hat einige technische Vorkehrungen getroffen: „Unsere Datenleitungen sind elektronisch gesichert. Niemand wird Sie enttarnen können", verspricht Recherche-Leiter David Schraven. In der Tat nutzt die WAZ-Gruppe eine SSL-Verschlüsselung für ihre Verbindung. Auch sollen die Dateien mit GnuPG, einer Open-Source-Variante des berühmten und immer noch sicheren Kryptoprogramms „Pretty Good Privacy" verschlüsselt werden. Wirklich sicher ist das aber auch noch nicht: Jeder Besucher hinterlässt nämlich auf dem Server der Website mit seiner IP-Adresse eine Spur, die zur Identifizierung genutzt werden kann. Nutzer, die wirklich anonym bleiben wollen, sollten daher dafür sorgen, dass ihre IP-Adresse verschleiert wird, wenn sie die Website besuchen. Das geht über Dienste wie JAP: Die JAP-Rechner, die unter anderem vom schleswig-holsteinischen Landesdatenschutzzentrum betrieben werden, verschleiern über mehrere Stufen, welchen Internet-Zugangsserver ein Informant verwendet. Einen entsprechenden Hinweis darauf gibt es auf der Website des Westens aber nicht.

In Brüssel haben indessen Journalisten selbst das Heft in die Hand genommen und zusammen mit Aktivisten und Kommunikationsprofis „BrusselsLeaks.com" gegründet. Die Idee dahinter war, dass Journalisten zwar gute Kontakte zu möglichen Informanten in den Behörden und Lobbyvereinigungen in Brüssel pflegen. Da die Verbindungen jedoch in der Regel bekannt sind, ist es für diese riskant, die Informationen weiterzugeben. Anders wäre dies, so das Kalkül, wenn die Daten durch einen Trichter kommen und dann verteilt werden. Eine Art Datenwäsche sozusagen. Anonymität wird auf Wunsch versprochen. Das Ziel ist hochgesteckt: Aufgedeckt werden sollen „die vor Ort gesammelten Informationen, die die innere Funktionsweise der EU zentral abbilden".



https://brusselsleaks.com/ (Aufruf am 3.3.2011)

Zu Beginn bot BrusselsLeaks eine Datenübermittlung nur über ein gesichertes Webformular an, das auf Wordpress-Software beruht sowie E-Mail-Kontakt über den kanadischen Dienstleister Hushmail. com, der E-Mails verschlüsselt. Wie auch beim Westen gibt es keinen Hinweis darauf, dass die IP-Adressen der Besucher letztlich nicht geschützt sind. Welche Technik „Brussels Leaks" letztendlich einsetzen wird, ist noch ungewiss. Bislang gibt es nur eine Ankündigung, die ein großes Medienecho erfuhr. Bis auf Weiteres sind die Macher auf Tauchstation gegangen. Ähnliche Ankündigungen und Protoypen gibt es inzwischen auch für Indonesien in Form eines „Indoleaks", das einen E-Mail-Kontakt über Googlemail anbietet. In Bulgarien ging „Balkanleaks.eu" an den Start. Wikispooks.com wiederum basiert auf der Mediawiki-Software. Sie bietet PGP-verschlüsselten E-Mail-Kontakt sowie einen SSL-gesicherten anonymen Datei-Upload an. Dabei versichert sie, keine IP-Adressen zu protokollieren. Diese Website richtet sich an Mitarbeiter von Sicherheitsbehörden sowie Freunde von Verschwörungstheorien.



https://www.balkanleaks.eu/ (Aufruf am 3.3.2011)

https://wikispooks.com/ (Aufruf am 3.3.2011)

http://www.indoleaks.org/ (Aufruf am 3.3.2011)

Ob diese Plattformen und Dienstleistungen auf der Bugwelle von WikiLeaks für den Journalismus erfolgreich sein werden, ist ungewiss. Seit Jahren gibt es etwa die so genannte Privacybox der German Privacy Foundation, einer Art geschützten digitalen Briefkasten. 2.000 Personen aus Deutschland, Frankreich, Spanien und Russland nutzen zurzeit die etwa 3.000 sicheren Postfächer. Deutsche Medien haben dieses Angebot bislang nicht angenommen.

Dieser Beitrag erschien zuerst in der Ausgabe 01-02/2011 des verdi-Magazins „M – Menschen machen Medien. Wir danken Christiane Schulzki-Haddouti für die Nachdruckgenehmigung.

Appell gegen die Kriminalisierung von Wikileaks

Allgemeine Erklärung der Menschenrechte der Vereinten Nationen Artikel 19: „Jeder hat das Recht auf Meinungsfreiheit und freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, Meinungen ungehindert anzuhängen sowie über Medien jeder Art und ohne Rücksicht auf Grenzen Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten."
Die taz, die Frankfurter Rundschau, der Freitag, der Tagesspiegel, Perlentaucher.de, die Berliner Zeitung, netzpolitik.org und European Center For Constitutional and Human Rights (ECCHR) veröffentlichen diesen Appell gegen die Kriminalisierung von Wikileaks.

1. Die Angriffe auf Wikileaks sind unangebracht

Die Internet-Veröffentlichungsplattform Wikileaks steht seit der Veröffentlichung der geheimen Botschaftsdepeschen der USA unter großem Druck. In den USA werden die Wikileaks-Verantwortlichen als „Terroristen" bezeichnet, es wird sogar ihr Tod gefordert. Große internationale Unternehmen wie MasterCard, PayPal und Amazon beenden ihre Zusammenarbeit mit Wikileaks – ohne dass eine Anklage gegen die Organisation vorliegt, geschweige denn eine Verurteilung. Gleichzeitig wird die technische Infrastruktur von Wikileaks anonym über das Internet attackiert. Dies sind Angriffe auf ein journalistisches Medium als Reaktion auf seine Veröffentlichungen. Man kann diese Veröffentlichungen mit gutem Grund kritisieren, ebenso die mangelnde Transparenz, welche die Arbeit der Plattform kennzeichnet. Aber hier geht es um Grundsätzliches: die Zensur eines Mediums durch staatliche oder private Stellen. Und dagegen wenden wir uns. Wenn Internetunternehmen ihre Marktmacht nutzen, um ein Presseorgan zu behindern, käme das einem Sieg der ökonomischen Mittel über die Demokratie gleich. Diese Angriffe zeigen ein erschreckendes Verständnis von Demokratie, nach dem die Informationsfreiheit nur so lange gilt, wie sie niemandem weh tut.

2. Publikationsfreiheit gilt auch für Wikileaks

Die in der Allgemeinen Erklärung der Menschenrechte verbriefte Publikationsfreiheit ist eine Grundlage der demokratischen Gesellschaften. Sie gilt nicht nur für klassische Medien wie Zeitungen oder Fernsehanstalten. Das Internet ist eine neue Form der Informationsverbreitung. Es muss den gleichen Schutz genießen wie die klassischen Medien. Längst hätte es einen weltweiten Aufschrei gegeben, wenn die USA ein Spionage-Verfahren gegen die New York Times, einen finanziellen Kreuzzug gegen den Spiegel oder einen Angriff auf die Server des Guardian führen würden.

3. Recht auf Kontrolle des Staates

Die Kriminalisierung und Verfolgung von Wikileaks geht über den Einzelfall hinaus. Die Veröffentlichung als vertraulich eingestufter Informationen in solchen Mengen soll verhindert werden. Denn die Menge an Dokumenten liefert der Öffentlichkeit einen weit tieferen Einblick in staatliches Handeln als bisherige Veröffentlichungen in klasssischen Medien. Der Journalismus hat nicht nur das Recht, sondern die Aufgabe, den Staat zu kontrollieren und über die Mechanismen des Regierungshandelns aufzuklären. Er stellt Öffentlichkeit her. Ohne Öffentlichkeit gibt es keine Demokratie. Der Staat ist kein Selbstzweck und muss eine Konfrontation mit den eigenen Geheimnissen aushalten. Wir, die Initiatoren und Unterzeichner, fordern, die Verfolgung von Wikileaks, die dem Völkerrecht zuwiderläuft, zu stoppen. Wir fordern alle Staaten und auch alle Unternehmen auf, sich diesem Feldzug gegen die bürgerlichen Rechte zu widersetzen. Wir fordern alle Bürger, bekannt oder unbekannt, in politischen Positionen oder als Privatpersonen, auf, für die Einstellung der Kampagne gegen die Meinungs- und Informationsfreiheit aktiv zu werden. Wir laden alle ein, sich an dem Appell für die Medienfreiheit zu beteiligen.

Die Erstunterzeichner dieses Appells:

- taz
- Frankfurter Rundschau
- Der Freitag
- Tagesspiegel
- European Center For Constitutional and Human Rights (ECCHR)
- Perlentaucher.de

Jetzt mit dabei:

- Telepolis
- Berliner Zeitung
- netzpolitik.org
- AK Zensur
- Neues Deutschland
- Reporter ohne Grenzen
- Humanistische Union
- Blätter für deutsche und internationale Politik
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

und rund 16.000 weitere Unterzeichnerinnen und Unterzeichner (Stand: 6. März 2011).

Stefan Hügel

Wikileaks – soviel Transparenz wie möglich, soviel Geheimhaltung wie nötig

„Der erste ernsthafte Informationskrieg hat begonnen.
Das Schlachtfeld ist Wikileaks. Ihr seid die Truppen."
John Perry Barlow

Die Debatte zu Wikileaks hat durch die großen Veröffentlichungen des letzten Jahres – allen voran die Depeschen („Cables") der amerikanischen Botschaft – und nicht zuletzt durch die Verhaftung von Julian Assange große öffentliche Aufmerksamkeit auf sich gezogen. Vor allem Assanges Verhaftung, wegen eines Vorwurfs, der mit Wikileaks nichts zu tun hat, provoziert Mutmaßungen, die an Verschwörungstheorien denken lassen. Das wird befeuert durch eine Reihe von Verlautbarungen, insbesondere konservativer amerikanischer Politiker, die erhebliche Zweifel an deren demokratischer und rechtstaatlicher Gesinnung nähren.

Übersehen wird dabei häufig, dass Whistleblower-Plattformen kein neues Phänomen sind. Die Plattform Cryptome.org gibt es bereits seit 1996; ihr Betreiber war auch einer der Geburtshelfer für Wikileaks.

Die Diskussion hat eine Reihe von Aspekten, die gelegentlich vermischt zu werden scheinen. Gegen Wikileaks wird argumentiert:

- **Regierungen sind auf Geheimhaltung angewiesen – nicht nur in der Außenpolitik.** Sicherlich gibt es geheime Informationen, die nicht in die Öffentlichkeit dringen dürfen. Doch wo ist die Grenze zu ziehen? Soviel Geheimhaltung wie nötig – so viel Offenheit wie möglich: Was das konkret bedeutet, darüber gibt es keinen gesellschaftlichen Konsens – und damit eine breite Grauzone.

- **Die Veröffentlichungen verletzen Persönlichkeitsrechte und bringen Personen in Gefahr.** Dies ist zweifellos ein valides Argument. Veröffentlichungen müssen sorgfältig bereinigt werden, dass Rückschlüsse auf gefährdete Personen nicht mehr möglich sind. Dem Vernehmen nach geschieht das auch – Fehler lassen sich dabei aber sicher nicht immer vermeiden. Bisher sind keine konkreten Fälle solcher Gefährdungen bekannt geworden – dass musste auch der amerikanische Verteidigungsminister einräumen.

- **Die Veröffentlichungen sind doch nur Klatsch und Tratsch; sie führen zu keinen neuen Erkenntnissen.** Tatsächlich erweckten die ersten Veröffentlichungen diesen Eindruck: Einschätzungen der Qualifikation und des Charakters von Spitzenpolitikern, die zum Teil in ähnlicher Form bereits seit langem in der Öffentlichkeit diskutiert werden. Doch dies ist nur die oberflächliche Betrachtung. Verfolgt man die Veröffentlichungen weiter, so kommt man schnell zu ihrer Substanz. Tatsächlich ist aber die Debatte über Petitessen gelegentlich in den Vordergrund gerückt und hat die interessanten und wichtigen Aspekte der Veröffentlichungen überlagert.

- **Assange ist doch nur ein eitler Selbstdarsteller.** Das mag so sein oder nicht. Es hat mit dem Wert der veröffentlichten Informationen nichts zu tun.

Die zentrale Frage ergibt sich aus dem ersten der genannten Punkte: Wieviel Geheimhaltung ist nötig, wieviel Transparenz und Öffentlichkeit möglich. Damit ist die alte Frage der Informationsfreiheit berührt; Open-Government-Strategien hängen beispielsweise von der Antwort ab. Legitime Geheimhaltung betrifft vor allem sicherheitskritische Bereiche und Bereiche, in denen die Privatheit von Einzelpersonen gefährdet ist. Bei anderen Informationen ist der Grund für die Geheimhaltung fragwürdig: Gerade haben sich die Bürgerinnen und Bürger von Berlin in einem Volksentscheid die Veröffentlichung der Verträge für die Wasserversorgung erstritten; auf Wikileaks tauchten die Verträge über die Autobahngebühren mit dem Betreiber Toll Collect auf. Letztere offenbarten skandalöse Renditeversprechen. Verständlich, dass diese nicht an die Öffentlichkeit gelangen sollten – aber legitim?

Ein letzter Aspekt: die Sperrung von Konten durch Finanzdienstleister und von Serverkapazität durch IT-Dienstleister. Ob nun auf politischen Druck oder – wie behauptet – aufgrund der Verletzung von Nutzungsbedingungen: Vor allem letzteres müsste den einen oder anderen IT-Verantwortlichen aufmerksam werden lassen: Hat Wikileaks so auch nebenbei Probleme mit der Sicherheit und der Zuverlässigkeit von Cloud Computing aufgedeckt?

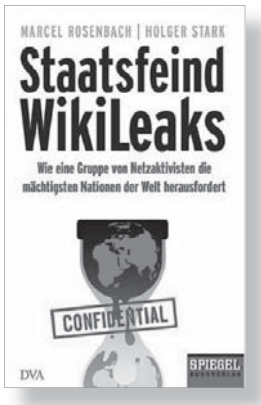
Die große öffentliche Aufmerksamkeit schlägt sich natürlich auch in einer Reihe von Publikationen nieder. Diese Veröffentlichungen behandeln unterschiedliche Aspekte: Zwei Bücher befassen sich mit der Geschichte von Wikileaks und Julian Assange aus einer jounalistischen Perspektive, der Bericht des früheren Wikileaks-Aktivisten Daniel Domscheit-Berg stellt die Sicht eines Insiders dar. Der letzte hier besprochene Band ist ein Sammelband, der Hintergründe und Konsequenzen von Wikileaks beleuchten will.

Was bei der Lektüre auffällt, aber auch nicht besonders überrascht: Viele Wertungen dessen, was passiert ist, hängen stark vom Blickwinkel des Erzählers ab. Während die ersten beiden Bände eine mehr neutrale Sicht bzw. die Sicht von Assange einnehmen – durchaus mit kritischen Untertönen – und Daniel Domscheit-Berg eher eine Randfigur darstellt, steht dieser in seinem eigenen Buch naturgemäß im Mittelpunkt. Es ist schwierig, die „richtige" Wertung allein aufgrund der Bücher zu treffen. Doch die Geschichte ist vielleicht überhaupt nicht das wichtigste: Wichtiger ist das, was in dem Sammelband von *Geiselberger (2011)* diskutiert wird: Was bedeutet der Enthüllungs- und Datenjournalismus, für den Wikileaks die Plattform bietet, für die künftige Politik? Der frühere Botschafter *John C. Kornblum* bringt es wohl sehr gut auf den auf den Punkt, wenn er schreibt:

Das langfristige Erbe der Wikileaks-Affäre wird wahrscheinlich nicht in der Offenlegung politischen Fehlverhaltens bestehen, sondern darin, der Öffentlichkeit dramatisch vor Augen geführt zu haben, wie radikal und mit welchen Folgen sich unser Umgang mit Informationen zu Beginn des 21. Jahrhunderts verändert. – Kornblum in Geiselberger (2011, Seite 175)

Dem gegenüber sollten die ebenfalls enthaltenen Berichte über gequälte Katzen, die der Boulevard gerne aufgreift, langfristig an Bedeutung verlieren.

Staatsfeind WikiLeaks: Wie eine Gruppe von Netzaktivisten die mächtigsten Nationen der Welt herausfordert



Das Nachrichtenmagazin *Der Spiegel* war einer der Medienpartner von Wikileaks bei den großen Veröffentlichungen des vergangenen Jahres. Spiegel-Redakteure *Marcel Rosenbach* und *Holger Stark* haben die Geschichte von Julian Assange und Wikileaks aufgeschrieben – von der unsteten Kindheit über die Hackerszene im Melbourne der späten 80er und frühen 90er Jahre bis heute. Dabei ist ein Kapitel der Vorgeschichte gewidmet, ein Kapitel erzählt die Anfänge von Wikileaks. Dem Jahr 2010 sind die weiteren Abschnitte gewidmet: Die Veröffentlichung des *„Collateral Murder"*-Videos, die Afghanistan-Feldberichte, die Krise von Wikileaks, die im Ausstieg mehrerer Aktiver gipfelte und die bisher umfangreichste Veröffentlichung: die amerikanischen Botschaftsdepeschen.

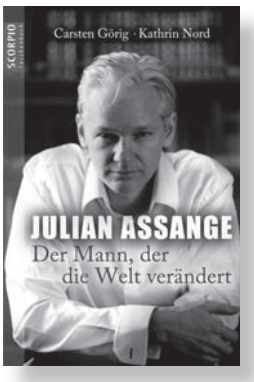
Danach kommen die Folgen der Veröffentlichung, die von Einigen als „Informationskrieg" bezeichnet werden. Zuerst die Verhaftung des mutmaßlichen Informanten *Bradley Manning*, der von den amerikanischen Behörden verdächtigt wird, Wikileaks umfangreiches Material zugespielt zu haben. Doch es geht weiter: DDOS-Attacken gegen die Wikileaks-Server, die Sperrung von Konten, Servern und DNS-Einträgen und die Verhaftung Assanges wegen des Vorwurfs sexueller Belästigung – nach einer weltweiten Suche durch Interpol. Gleichzeitig fordern hochrangige amerikanische Politiker, sowohl Manning als auch Assange hinzurichten. Ein Gegenschlag aus der Zivilgesellschaft erfolgt unter der Bezeichnung „Operation Payback": ebenfalls durch DDOS-Attacken werden die Server einiger Kreditkartenunternehmen und Anbieter von Serverkapazität zeitweise lahmgelegt.

Ein Fazit zieht der letzte Abschnitt: Wieviel Geheimhaltung ist für einen Staat notwendig, wieviel Transparenz sinnvoll. Wikileaks wurde auch und gerade aus Journalistenkreisen kritisiert: Zitiert wird beispielsweise der Chefredakteur der *Süddeutschen Zeitung*; er schreibt von einem „Weltbild von einer totalen, ins Totalitäre schwappenden Öffentlichkeit" und einer „umgekehrt orwellianischen Welt … nicht der Staat hat alle Kontrolle, sondern er verliert sie völlig." Die kritisierenden Journalisten ergriffen Partei für die Exekutive, weil sie um die Stabilität des Systems fürchteten. Dies entspreche aber nicht der Rolle der Medien in einem funktionierenden demokratischen System – Medien seien Moderatoren eines Reinigungsprozesses. „Sie machen idealtypisch politisches Handeln nachvollzieh- und diskutierbar, sie decken Fehlverhalten auf und führen so zu einer gesellschaftlichen Selbstheilung. Es ist eine für die Demokratie konstituierende Rolle."

Zusammenfassend bietet das Buch eine gut recherchierte Darstellung der Geschichte von Wikileaks, in der die großen Ereignisse des Jahres 2010 einen Schwerpunkt bilden. Im abschließenden Abschnitt werden aber auch die Konsequenzen für Journalismus, Medien und Politik beleuchtet – vielleicht der wichtigere Teil der Diskussion. Wenn man sich umfassend über die Geschichte von Wikileaks und seine Konsequenzen informieren will, von Autoren, die zumindest in der letzten Phase relativ nah an den Geschehnissen waren, sollte man von den hier besprochenen wohl am ehesten dieses Buch lesen.

Marcel Rosenbach, Holger Stark (2011): Staatsfeind Wikileaks: Wie eine Gruppe von Netzaktivisten die mächtigsten Nationen der Welt herausfordert. Spiegel-Buch, München: Deutsche-Verlags-Anstalt und Hamburg: Spiegel-Verlag, Preis €14,99

Julian Assange. Der Mann, der die Welt verändert



Einen im Vergleich deutlich knapperen biographischen Abriss des Lebens von Julian Assange enthält der Band von *Carsten Görig* und *Kathrin Nord*, wobei naturgemäß ebenfalls die Zeit von Wikileaks den Schwerpunkt des Bandes bildet.

Auch dieses Buch zeichnet die Anfänge bis zu den ersten großen Veröffentlichungen von Wikileaks nach: Erst die Zeit Assanges als Hacker in Australien, die Entwicklung zu juornalistischer Arbeit, die *Cypherpunks* und danach die Anfänge von Wikileaks und die ersten Enthüllungen.

Nach einem Exkurs in die Sicherheitstechnik werden die Entwicklungen von 2010 beschrieben: Das Video *„Collateral Murder"*, der mutmaßliche Informant Manning, die Zusammenarbeit mit den traditionellen Medien zunächst bei den Kriegsmeldungen aus Afghanistan. Darauf folgen drei Kapitel mit Hintergründen: Wikileaks als „One-Man-Show", der Ausstieg mehrerer Schlüsselpersonen im September 2010 und die Vergewaltigungsvorwürfe. Die bisher am meisten beachtete Veröffentlichung – die Botschaftsdepeschen – ist Thema des darauffolgenden Kapitels. Danach die Reaktionen: Der Versuch, die Enthüllungen zu kriminalisieren, die Versuche, Wikileaks durch technische Angriffe lahmzulegen und die Erwiderung des Netzes: die „Operation Payback".

In der abschließenden Behandlung der Konsequenzen stellt der Band die Frage nach möglichen Auswirkungen der Veröffentlichungen: Die Frage, ob sie künftige Kriege verhindern können, muss offen bleiben. Die Sichtweise der Kriege wird sich nach

Ansicht der Autoren aber ändern – man wird wegkommen vom eingebetteten Journalismus, bei dem nur das veröffentlicht wird, was den Journalisten vom Militär vorgeführt wird. Weitere Aspekte sind die Forderungen vieler Politiker nach mehr Kontrolle im Internet und die Frage von Geheimhaltung und Transparenz. Es fehlt nicht der Hinweis darauf, dass die von Assange propagierte Transparenz öffentlichen Handelns von ihm selbst und Wikileaks selbst nicht gelebt wird. „Julian Assange ist ein wandelnder Widerspruch. Jemand, der glaubt, dass totale Transparenz das Zusammenleben der Menschen erleichtert, dass das Enthüllen von Geheimnissen bessere Menschen hervorbringt. Jemand, der aber selbst ganz anders lebt, der nur seine eigenen Regeln beachtet. ... Julian Assange wäre nicht der erste Mensch, der etwas Wichtiges aufgebaut und die Welt in einem Teil geändert hat, um dann an seinem übergroßen Ego zu scheitern. Und er wäre vermutlich auch nicht der letzte."

Zusammengefasst ist der Band mit dem *Spiegel*-Buch vergleichbar; er ist aber kürzer und damit weniger detailliert. Er eignet sich damit vor allem für Leser, die sich schnell einen Überblick über die Geschichte von Assange und Wikileaks, und die Ereignisse des Jahres 2010 verschaffen wollen.

Carsten Görig, Kathrin Nord (2011): Julian Assange. Der Mann, der die Welt verändert. Berlin, München: Scorpio-Verlag, Preis €9,95

Inside Wikileaks: Meine Zeit bei der gefährlichsten Website der Welt

Mit Spannung wurde der Bericht eines der „Gesichter" von Wikileaks erwartet. *Daniel Domscheit-Berg* – der sich während seiner Zeit bei Wikileaks Daniel Schmitt nannte – stellt in *Inside Wikileaks* seine subjektiv gefärbte Sicht auf Assange und Wikileaks dar. Die Tatsache, dass er Wikileaks im Streit verlassen hat, lässt eine eher kritsche Perspektive insbesondere auf die die Person Julian Assange und die heutige Situation erwarten. In einer Reihe von Presseberichten und Interviews – beispielsweise bei *Zeit Online*, der Wirkungsstätte von Co-Autorin Tina Klopp – vermittelt der Autor den Eindruck, dass Wikileaks faktisch am Ende ist. Ein Eindruck, der jedoch nicht von allen geteilt wird.

Zum Inhalt: Domscheit-Berg berichtet über seine Zeit bei Wikileaks ab 2007, als er Assange kennenlernte. Die ersten großen Enthüllungen beim Schweizer Bankhaus *Julius Bär* und der *Scientology*-Sekte. Der Versuch des Bankhauses, Enthüllungen durch rechtliche Schritte zu verhindern, blieb erfolglos und zeigt, dass – entgegen anderslautender Ansichten – die Aktivitäten von Wikileaks durchaus durch das Recht gedeckt sind. Auch über erste Erfahrungen mit den Medien wird berichtet. Der Autor zieht den Schluss, dass aufwendige Dementis und Erläuterungen in der Regel nicht effektiv sind; besser sei es, auf die Vergesslichkeit der Öffentlichkeit zu vertrauen und Probleme einfach auszusitzen. Dies passierte dann auch, als erste Bedenken auftauchten, die Wikileaks-Plattform sei nicht so sicher wie dargestellt – Bedenken, die dem Autor nach durchaus einen wahren Kern enthielten.

Auch weiter orientiert sich der Rote Faden des Buchs am Ablauf der Geschehnisse – bis hin zum *„Collateral Murder"*-Video, den afghanischen Kriegstagebüchern und den amerikanischen Botschaftsdepeschen. Davor der Streit mit Assange und die Suspendierung. Breiteren Raum als in den anderen Veröffentlichungen erhalten die Planungen für OpenLeaks – hier kann Domscheit-Berg aus „erster Hand" berichten.

Eingebettet ist der Bericht über das persönliche Verhältnis des Autors zu Assange. Zunächst als Freundschaft, später mit wachsenden Spannungen, die letztlich mit der Suspendierung und dem darauffolgenden Abgang von Domscheit-Berg und von weiteren Aktiven eskalieren. Die Sicht auf Assange ist von Beginn an kritisch; Assange wird als exzentrische Persönlichkeit dargestellt. Gleichzeitig wird die organisatorische und technische Basis von Wikileaks kritisch beschrieben – die Darstellung nach außen sei meistens positiver gewesen, als die tatsächliche Situation. Deutliche technische Verbesserungen im Jahr 2010 seien beim Abgang der dafür verantwortlichen „Architekten" zurückgenommen worden; Wikileaks sei danach wieder auf dem technischen Stand von vorher gewesen.

Illustriert werden Darstellungen des persönlichen Verhältnisses mit Protokollen von Chats, die der Autor mit Assange geführt hat.

Inside Wikileaks bietet eine alternative Sichtweise zu den beiden vorher besprochenen Bänden. Es weist auf Unzulänglichkeiten von Wikileaks hin und zeichnet ein Porträt von Julian Assange abseits der Fernsehkameras – als einen genialen Menschen mit einer Vision, aber auch als einen Egozentriker, der gerne im Mittelpunkt steht. Das Bild ist notwendigerweise subjektiv – ob man den Einschätzungen von Domscheit-Berg folgen muss, oder ob es sich auch um eine Revanche für die Suspendierung handelt, ist für Außenstehende schwer zu beurteilen. Von manchen wird er in Kommentaren – beispielsweise bei *Zeit Online* – inzwischen scharf kritisiert: Domscheit-Berg habe mit seinen Äußerungen Wikileaks mehr geschadet, als es Geheimdienste je vermocht hätten. Um sich eine möglichst umfassende Meinung zu bilden, sollte seine Perspektive aber nicht übergangen werden.

Daniel Domscheit-Berg, Tina Klopp (2011): Inside Wikileaks: Meine Zeit bei der gefährlichsten Website der Welt. Berlin: Econ-Verlag, Preis €18,00

Wikileaks und die Folgen: Netz – Medien – Politik

Einen anderen Ansatz haben die Herausgeber dieses Sammelbandes gewählt. Die Geschichte von Wikileaks wird nur in einem einführenden Beitrag behandelt, dann wenden sich die Autoren den Konsequenzen zu: Gegliedert ist der Band in fünf Abschnitte, die unterschiedliche Aspekte von Wikileaks zum Thema haben:

- Hintergründe,
- Wikileaks und das Netz,
- Wikileaks und die Medien,
- Wikileaks und die Diplomatie,
- Wikileaks und die Demokratie.

Mit diesen Themen legt der Band über die Erzählung der reinen Geschehnisse hinaus den Schwerpunkt auf die Konsequenzen, die sich aus einer Form des Journalismus, wie sie durch Wikileaks gefördert wird, ergeben. Er bildet damit einen Ausgangspunkt für die wichtigen, weiterführenden Diskussionen: Welche Auswirkungen ergeben sich für Netz und weitere Medien, was bedeutet Wikileaks für die Zukunft der Diplomatie und was für die Entwicklung der Demokratie. Das ist immer mit der Frage verbunden, ob solche Enthüllungsplattformen vor allem eine Chance bieten oder ob sie in erster Linie schaden oder sogar eine Gefahr darstellen. Sicherlich wird die Antwort auf die Frage von der persönlichen Stellung des Autors und seinen Wertvorstellungen abhängen.

Zum Inhalt: Im Abschnitt *Hintergründe* wird zunächst die Geschichte zusammengefasst: Ausgehend von der Arbeit an dem Video, das später unter dem Titel „Collateral Murder" veröffentlicht werden sollte, gibt es im Beitrag *Keine Geheimnisse. Julian Assanges Mission der totalen Transparenz. Porträt eines Getriebenen.* von *Raffi Khatchadourian* eine Rückblende auf Vorgeschichte und persönliche Entwicklung. *Niklas Hoffmann* analysiert in seinem Beitrag *Der Gegenverschwörer* die Motive Assanges vor allem anhand seiner Einträge im Blog *iq.org*. *Die Wurzeln von Wikileaks* untersucht *Detlef Borchers*, ausgehend von der Veröffentlichung der *Pentagon Papers* in den frühen 70er Jahren hin zur *Cypherpunk*-Bewegung, deren Mitglied Assange war.

Den Abschnitt *Wikileaks und das Netz* leitet *Jaron Lanier* mit dem Beitrag *Nur Maschinen brauchen keine Geheimnisse* ein, in dem er sich kritisch mit dem Ansatz totaler Transparenz auseinandersetzt, der Wikileaks zu Grunde liegt. *Geert Lovink* und *Patrice Riemens* stellen in ihren *Zwölf Thesen zu Wikileaks* fest, dass es trotz mancher Unzulänglichkeiten eine wichtige Entwicklung darstellt. „Was denken Sie über Wikileaks? Ich glaube es wäre eine gute Idee", stellen sie einleitend frei nach *Mahatma Gandhi* fest und schließen: „Gäbe es Wikileaks nicht, dann müsste es dringend erfunden werden." Einen neuen *Strukturwandel der Öffentlichkeit*, der durch *„Super-empowered Individuals"* befördert wird, macht *Felix Stalder* in seinem Beitrag *Wikileaks und die neue Ökologie der Nachrichtenmedien* aus, der diesen Abschnitt abschließt.

Die beiden ersten Beiträge des nächsten Abschnitts *Wikileaks und die Medien* behandlen zwei Publikationen, die bei der Veröffentlichung von Material mit Wikileaks zusammengearbeitet haben: der *Spiegel* und der *Guardian*. Im Beitrag *Wir halten kritische Distanz* interviewt *Michael Hanfeld* die Spiegel-Redakteure *Mascolo* und *Müller von Blumencron*, die die Gründe für die Veröffentlichung durch den Spiegel, die redaktionelle Auswahl und den Informantenschutz eingehen. *Simon Rogers* beschreibt im Beitrag *Wikileaks und der investigativer Datenjournalismus. Wie wir beim Guardian mit den Wikileaks-Dateien umgehen*, wie der Guardian die vorhandenen Datenmengen ausgewertet und daraus neue Informationen generiert hat. *Michael Moorstedt* setzt sich im Beitrag *Der Skandal im Datenhaufen. Ein Selbstversuch* mit der Frage auseinander, wie aus der Menge an Daten und Informationen das Wichtige vom Unwichtigen getrennt werden kann und *Mercedes Bunz* beschreibt in *Das offene Geheimnis. Zur Politik der Wahrheit im Datenjournalismus*, wie Datenjournalismus als neue Form des Journalismus, der sich auf die Auswertung großer Datenmengen stützt, funktionieren kann.

Zwei der drei Autoren des Abschnitts *Wikileaks und die Diplomatie* waren selbst bereits Botschafter und argumentieren damit aus persönlicher Betroffenheit heraus. Vielleicht ist das ein Grund, warum sie, wie der dritte Autor eine kritische Haltung zu der bei Wikileaks vertretenen Transparenz einnehmen. *Wolfgang Ischinger*, heute Vorsitzender der Münchener Sicherheitskonferenz, erklärt im Beitrag *Das Wikileaks-Paradox: Weniger Transparenz, mehr Geheimdiplomatie*, die Veröffentlichung der Botschaftsdepeschen habe „das Potenzial, die Diplomatie selbst in ihren Grundfesten zu erschüttern" und nennt die vielfältigen Personenkreise, die die Konsequenzen der Veröffentlichung zu tragen haben. Er fürchtet, „die Leaks, die oberflächlich betrachtet mehr Transparenz bedeuten, werden zu weniger Offenheit … und zu mehr Geheimhaltung führen. Das angebliche Ziel einer transparenten Welt rückt damit in immer weitere Ferne."

Auch *Volker Perthes* sieht in seinem Beitrag *Wikileaks und warum Diskretion in der Außen- und Sicherheitspolitik wichtig ist* vor allem den diplomatischen Flurschaden und fürchtet, dass sich die Informationslage amerikanischer Diplomaten weiter verschlechtern wird. *John C. Kornblum* sieht in der Debatte in *Wikileaks und die Ära des radikalen Wandels* weniger eine Frage der konkret offengelegten Informationen als eine Frage des Umgangs damit im 21. Jahrhundert.

Der letzte Abschnitt behandelt *Wikileaks und die Demokratie*. Der Beitrag von *Christoph Möllers, Zur Dialektik der Aufklärung der Politik* behandelt die Zwiespältigkeit der Veröffentlichungen und stellt die Frage nach der politischen Agenda. *Das missbrauchte Staatsgeheimnis. Wikileaks und die Demokratie* von *Rahul Sagar* stellt die Frage nach der Legitimität der Geheimhaltungseinstufungen und hält es für möglich, dass Geheimhaltung auch verhindern soll, dass Fehlleistungen ans Licht der Öffentlichkeit gelangen. *Dirk Baecker* bezeifelt in *Falscher Alarm* abschließend die von einigen postulierten karastrophalen Auswirkungen auf das Tagesgeschäft der Politik und stellt die These auf, dass „der Wikileaks-Skandal dazu geeignet sein kann, den Blick auf dieses Tagesgeschäft zu lenken. Denn nur, wenn auch die Öffentlichkeit etwas von diesem Tagesgeschäft versteht, können wir damit beginnen, uns anzuschauen, ob die schiere Menge dieser Daten, die Schnelligkeit ihrer Bereitstellung und das elektronische Raffinement ihrer Verknüpfung an diesem Tagesgeschäft etwas ändern."

Der Band ist von den besprochenen derjenige, der am stärksten in die Zukunft weist. Er eröffnet die Debatte, wie wir künftig mit Plattformen wie Wikileaks, seinen Veröffentlichungen und Informationen insgesamt umgehen wollen. Wer an der Debatte teilnehmen will, sollte dieses Buch lesen.

Heinrich Geiselberger (Hg.) (2011): Wikileaks und die Folgen: Netz – Medien – Politik. edition suhrkamp, Berlin: Suhrkamp-Verlag, Preis €10,00

Gregor Koall

Wenn Unternehmen twittern

Betreff: Tweet #1 / Freitag, 10:01 Uhr

Lieber F., bezugnehmend auf unsere Besprechung von Montag letzter Woche, schicke ich dir nun den Tweet mit der Bitte um Veröffentlichung. Wir haben uns an die Zeichenzahl 140 gehalten.
Bei Rückfragen stehen wir dir gern zur Verfügung.
Viele Grüße H.

Re: Tweet #1 / Freitag, 10:15 Uhr

Lieber H., danke für deine Mail. Leider hast du den Tweet vergessen…
Gruß F.

Re Re: Tweet #1 / Freitag, 10:17 Uhr

Lieber F. oh sorry. Habe ich dir als Worddatei angehängt.
Viele Grüße H.

FW Re Re: Tweet#1 / Freitag, 10:30 Uhr

Hallo K, die Abteilung X will jetzt twittern. Schau mal drüber, das geht dann zur Freigabe an M.
Heute Mittagessen?
LG F.

Re: FW Re Re: Tweet#1 / Freitag, 11:30 Uhr

Hi F., tweet m.E. ok.
Essen gern. Um eins unten!
Gruß K.

FW: Re: FW: Re: Re: Tweet#1 / Freitag, 12:30 Uhr

Hallo H., aus Sicht des Pressesprechers gibt es gegen den Tweet keine Einwände. Ich schicke es jetzt an M. zur Freigabe. Der Tweet sollte dann spätestens heute Abend online sein.

Gruß F.

Twitter Abteilung X Freigabe, Tweet #1 / Freitag, 12:45 Uhr

Sehr geehrter Herr M.,
im Zuge der neuen Social Media Strategie unseren Unternehmens und als direkte Konsequenz unseres Workshops vom letzten Mai, hat sich die Abteilung X einen twitter-Account zugelegt und wird ab sofort twittern. Ich habe Ihnen den ersten tweet (siehe Worddokument) zur Freigabe geschickt. Herr K. hat aus Sicht der Pressestelle keine Bedenken.
Mit freundlichen Grüßen F.

Re: FW: Re: FW: Re: Re: Tweet#1 / Freitag, 14:30 Uhr

Lieber F. hast du schon ein Feedback aus der GL?
LG H.

Re: Re: FW: Re: FW: Re: Re: Tweet#1 / Freitag, 14:55 Uhr

Hallo H, die sitzen seit Mittag im Konferenzraum. Kann noch dauern.
Gruß F.

Re: Re: Re: FW: Re: FW: Re: Re: Tweet#1 / Freitag, 14:58 Uhr

Lieber F., ok, ist ja noch ein bisschen Zeit bis heute Abend…
LG H.

Re: Re: Re: Re: FW: Re: FW: Re: Re: Tweet#1 / Freitag, 18:05 Uhr

Lieber F. schon was von M. gehört? Ich müsste langsam Feierabend machen…
LG H.

Re: Twitter Abteilung X Freigabe, Tweet #1 / Freitag, 18:45 Uhr

wer oder was ist twitter?
M.
Diese Nachricht ist vertraulich. Sollten Sie nicht der vorgesehene Empfaenger sein, so bitten wir hoeflich um eine Mitteilung. Jede unbefugte Weiterleitung oder Fertigung einer Kopie ist unzulaessig. Diese Nachricht dient lediglich dem Austausch von Informationen und entfaltet keine rechtliche Bindungswirkung. Aufgrund der leichten Manipulierbarkeit von E-Mails koennen wir keine Haftung fuer den Inhalt uebernehmen.
This message is confidential and may be privileged. If you are not the intended recipient, we kindly ask you to please inform the sender. Any unauthorised dissemination or copying hereof is prohibited. This message serves for information purposes only and shall not have any legally binding effect. Given that e-mails can easily be subject to manipulation, we can not accept any liability for the content provided.

Re: Re: Twitter Abteilung X Freigabe, Tweet #1 / Freitag, 18:47 Uhr

Sehr geehrter Herr M.,
twitter ist ein Microbloggingdienst, der dem schnellen Austausch von Informationen dient. Wir hatten in unserem Workshop im Mai beschlossen, diesen Dienst als weiteren Kommunikationskanal zu nutzen. Abteilung X macht den Anfang.
Ich wünsche Ihnen ein sonniges Wochenende!

Mit freundlichen Grüßen F.
Von meinem iPhone gesendet.

Re: Re: Re: Re: Re: FW: Re: FW: Re: Re: Tweet#1 / Freitag, 19:00 Uhr

Lieber F. ich bin jetzt raus. Ich kann meine Mails aber auch zu Hause abrufen. ;-)
Schönes Wochenende!
LG H.

Re: Re: Re: Twitter Abteilung X Freigabe, Tweet #1 / Montag 07:15 Uhr

Freigegeben. Twitter müssen Sie mir aber noch mal erklären.
M.

Diese Nachricht ist vertraulich. Sollten Sie nicht der vorgesehene Empfaenger sein, so bitten wir hoeflich um eine Mitteilung. Jede unbefugte Weiterleitung oder Fertigung einer Kopie ist unzulaessig. Diese Nachricht dient lediglich dem Austausch von Informationen und entfaltet keine rechtliche Bindungswirkung. Aufgrund der leichten Manipulierbarkeit von E-Mails koennen wir keine Haftung fuer den Inhalt uebernehmen.

This message is confidential and may be privileged. If you are not the intended recipient, we kindly ask you to please inform the sender. Any unauthorised dissemination or copying hereof is prohibited. This message serves for information purposes only and shall not have any legally binding effect. Given that e-mails can easily be subject to manipulation, we can not accept any liability for the content provided.

Re:Re: Re: Re: Re: Re: FW: Re: FW: Re: Re: Tweet#1/ Montag, 10:05 Uhr

Hallo H. , der Tweet ist freigegeben. Ihr hattet noch Rechtschreibfehler (Groß- & und Kleinschreibung). Habe ich korrigiert. Anbei der korrigierte Tweet.
Viele Grüße F.

Re: Re:Re: Re: Re: Re: Re: FW: Re: FW: Re: Re: Tweet#1 / Montag, 12:30 Uhr

Hallo F., sorry war im Meeting. Danke für die Freigabe. Der Fehler ist kein Fehler. Wir wollten bewusst alles klein schreiben. Unsere Praktikantin findet, das sei normal im Internet.
LG H.

Re: Re: Re:Re: Re: Re: Re: Re: FW: Re: FW: Re: Re: Tweet#1 / Montag 13:00 Uhr

CC: K., M.
Hallo H., es interessiert hier nicht, was im Internet „normal" oder „nicht normal" ist. Wenn eure Abteilung über twitter Nachrichten verbreitet, dann macht sie das im Namen unseres Unternehmens. Das beinhaltet aber auch die korrekte Schreibweise. Bitte haltet euch an die von Herrn M. und K. freigegebene Version (siehe Mail von Montag, 10:05 Uhr).
Im Übrigen wäre es zu begrüßen, wenn ihr einen Kommunikationsplan für die tweets der kommenden 14 Tage erstellen könntet. Dann haben wir mehr Planungssicherheit.
Viele Grüße F.

Re:Re: Re: Re:Re: Re: Re: Re: Re: FW: Re: FW: Re: Re: Tweet#1 / Montag 13:40 Uhr

CC: K, M., P., D., L.
Hallo F., N. wird, gemeinsam mit unsereren neuen Praktikanten, ein paar Folien (Powerpoint) zusammenstellen und unsere Kommunikationsstrategie für twitter darlegen. Dazu werden wir Ende kommender Woche eine Besprechung einberufen. Ich denke es macht Sinn, das dann aus allen Abteilungen ein Entscheidungsträger anwesend ist.
Wir werden bis heute Abend eine Excel-Liste im Intranet veröffentlichen, die alle tweets der kommenden 14 Tage beinhaltet. Ich denke, das beschleunigt den Freigabeprozess.
Viele Grüße H.

beispielfirma Endlich Wochenende. Habt alle eine schöne Zeit.
less than 5 seconds ago from web

Gregor Koall

Gregor Koall betreibt den Blog Trendopfer (www.trendopfer.de), auf dem der Beitrag unter *http://www.trendopfer.de/wahrheit/2009/08/wenn-unternehmen-twittern/* am 17. August 2009 zuerst veröffentlicht wurde. Wir danken dem Autor für die freundliche Genehmigung zum Abdruck.

Ralf E. Streibl

Zivilitärische Informatik

Blick zurück nach vorne

In der Satzung des FIfF steht unter §2 „Zweck" u.a. zu lesen:

> *„Ein Schwerpunkt des Vereins liegt in der Friedensarbeit und -forschung im Sinne der Förderung der Völkerverständigung; seine vordringlichen Aufgaben sind:*
>
> 1. *die Bedeutung der Informationstechnik und der Arbeit der DV-Fachleute für militärtechnische Zwecke aufzuzeigen,*
> 2. *den militärischen Einfluß auf die Entwicklung der Informationstechnik und auf die Fachgebiete der Informations- und Kommunikationstechnik zu untersuchen,*
> 3. *die prinzipielle Fehlerhaftigkeit informationstechnischer Systeme, insbesondere komplexer Systeme im militärischen Bereich, und deren Implikationen aufzudecken,*
> 4. *die eigenen Fachkollegen, die politischen Entscheidungsträger und die Öffentlichkeit zu informieren und zur Diskussion zu ermuntern,*
> 5. *das Verantwortungsbewußtsein der im Bereich der Informationstechnik Tätigen zu schärfen,*
> 6. *gesellschaftlich verantwortbare und die internationale Zusammenarbeit fördernde Alternativen zur militärisch orientierten Forschung und Entwicklung im Bereich der Informationstechnik zu erarbeiten.*

Ein Thema, welches mich seit Beginn meiner Mitgliedschaft im FIfF gefesselt, erschreckt, interessiert und beschäftigt hat, ist die Ambivalenz von Informatik-Forschung und -Entwicklung im Spannungsfeld zwischen zivilen und militärischen Anwendungen. Den Begriff *Dual-Use* lernte ich Ende der 80er Jahre im FIfF-Zusammenhang kennen. Nicht zuletzt durch die Publikationen von Manfred Domke wurde mir deutlich, dass Dual-Use nicht nur Zufall oder unvermeidbar ist, sondern dahinter oft gezielte Planungen, fördernde Strukturen und die Absicht der Verschleierung stehen.

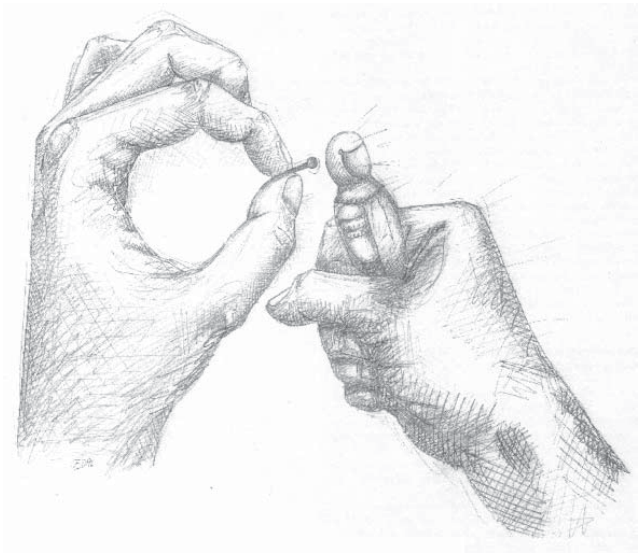
In diesem Sinne begann ich für mich, verschiedene Arten von Wechselwirkungen zu unterscheiden:

- zivile „Abfallprodukte" aus der Militärtechnik (oft als „Mehrwert" militärischer Forschung deklariert);
- militärische Verwendung bzw. Anpassung eigentlich ziviler Entwicklungen;
- offene militärische Interessen hinsichtlich „ziviler" Forschungsprojekte;
- verdeckte militärische Interessen an vordergründig „zivilen" Forschungsprojekten.

Anfang der 90er Jahre hatte das Thema auch interdisziplinär eine große Öffentlichkeit. So gab es beispielsweise im November 1992 in München eine von einem breiten Trägerkreis getragene Fachtagung unter dem Motto *Die Janusköpfigkeit von Forschung und Technik – Zum Problem der zivil-militärischen Ambivalenz*.[1]

Wenn ich mich heute umsehe, erscheint es mir wichtiger denn je, solche Fragen in den Blick zu nehmen. Vergleichsweise offenkundig stellt sich der Hintergrund mancher Wettbewerbe im Robotikbereich dar: Sei es die seit 2004 stattfindende *DARPA Grand Challenge* zur Entwicklung unbemannter Landfahrzeuge (*DARPA = Defense Advanced Research Projects Agency*, Behörde des amerikanischen Verteidigungsministeriums, die Gelder für Forschungsvorhaben verwaltet) oder seit 2006 *SAUC-E*, ein Wettbewerb des britischen und französischen Verteidigungsministeriums für autonome Unterwasserfahrzeuge. Das Akronym steht für *Student Autonomous Underwater Challenges – Europe* und macht deutlich, dass hier nicht nur eine Einflussnahme auf Forschungsprogramme zu verzeichnen ist, sondern gezielt auch Studierende involviert werden. Dual-Use im Kontext universitärer Lehre?

Zivil-militärische Kooperationen, Dual-Use, Militarisierung von



»Dual Use« – Zeichnung von Frank Drewes aus der FIfF-Kommunikation 3/96

Hochschulen – die Problematik hat an Aktualität nicht verloren, sondern womöglich noch gewonnen. Während an vielen Hochschulen und Forschungseinrichtungen olivgrün angehauchte Projekte mehr oder weniger offen beforscht werden, gab und gibt es andernorts Diskussionen[2] – auch in der Privatwirtschaft[3]. Die Problematik ist mehrschichtig: Kann man Dual-Use-Aspekte von Projekten an konkreten Aspekten fest machen?[4] Davon unabhängig – weil weitergehend – ist vor allem aber auch die Frage, wie der kritische Diskurs innerhalb und außerhalb der Disziplin – und dies heißt nicht zuletzt auch an den Hochschulen in den Studiengängen! – geführt und fundiert werden kann. Die Frage von Zivilklauseln in Bildungs- und Forschungseinrichtungen ist gerade jetzt wieder aktuell in die Aufmerksamkeit gerückt. In Wissenschaft und Frieden 3/2010 und 1/2011 finden sich lesenswerte Artikel hierzu.[5] Von aktuellen Diskussionen und Erörterungen an der Universität Bremen wird in einer kommenden Ausgabe der *FIfF-Kommunikation* ausführlicher die Rede sein.

Retrospektive

Für den 1991 von Ute Bernhardt und Ingo Ruhmann für das FIfF herausgegebenen Sammelband *Ein sauberer Tod – Informatik und Krieg* fasste Manfred Domke grundlegende Aspekte und kritische Überlegungen zu *Dual-Use* zusammen und illustrierte diese anhand konkreter Beispiele[6]. Wir haben diesen nun 20 Jahre alten Text vor dem Hintergrund der aktuellen Diskussionen als „Retrospektive" für diese Ausgabe der *FIfF-Kommunikation* ausgewählt, da hierdurch die Dauerhaftigkeit dieser Problematik deutlich wird. Zum anderen möge er als Beispiel und Anregung dienen, sich aus dem eigenen Fach- und Tätigkeitsgebiet heraus aktiv, fundiert und kritisch mit *Dual-Use*-Fragen zu beschäftigen und konkrete Projekte unter dieser Perspektive zu durchleuchten.

Anmerkungen

1 Liebert, W.; Rilling, R.; Scheffran, J. (Hrsg.) (1994): Die Janusköpfigkeit von Forschung und Technik. Zum Problem der zivil-militärischen Ambivalenz. Schriftenreihe Wissenschaft und Frieden (Band 19). Marburg: BdWi.

2 So beispielsweise auch bei der GMD (Gesellschaft für Mathematik und Datenverarbeitung) im Widerstand gegen eine Kooperation mit der Informations- und Medienzentrale der Bundeswehr sowie später in Zusammenhang mit der Eingliederung der GMD in die Fraunhofer-Gemeinschaft, vgl. z.B.:
Bernhardt, U. (1996): Information Warfare in der GMD? In: FIfF-Kommunikation, 13 (3), S.22.
Göhring, W. (2000): Forschung für den Markt. Zur Fusion von GMD und FhG. In: Wissenschaft und Frieden, 18 (3), S.49-52.
Borchers, D. (2009): Vor 10 Jahren: Innovation und Arbeitsplätze. In: iX, (11), S.156.

3 Vgl. hierzu als sehr interessante und ausführlich dokumentierte Debatte: Brössler, P.; Biskup, H.; Rauschmeyer, H. (1996): Damals hatte es ja keine Bedeutung. Ein Softwarehaus stellt sich der Gewissensfrage. In: FIfF-Kommunikation, 13 (3), S.28-34.

4 Hierzu lesenswert ein Beitrag, den Jürgen Friedrich im Nachgang zu einem Vortrag bei einer Veranstaltung der FIfF-Regionalgruppe Bremen verfasst hat:
Friedrich, J. (1996): Von einem, der auszog, die Software-Ergonomie zu verbreiten, und dabei zwischen die Fronten geriet. In: FIfF-Kommunikation, 13 (3), S.24-27.

5 Bisbis, N. (2010): Zivilklausel für alle Hochschulen. Handlungsbedarf gegen Militarisierung von Forschung und Lehre. In: Wissenschaft und Frieden, 28 (3), S.54-56.
Schulze, D. (2011): Zivilklausel international. Militarisierung der Hochschulen verhindern. In: Wissenschaft und Frieden, 29 (1), S.50-53.

6 Domke, M. (1991): DUAL-USE: Berücksichtigung militärischer Anforderungen bei der zivilen Entwicklung neuer Technologien. In: Bernhardt, U.; Ruhmann, I. (Hrsg.): Ein sauberer Tod. Informatik und Krieg. Schriftenreihe Wissenschaft und Frieden (Band 15). Bonn: BdWi/FIfF, S.172-191.

Retrospektive

Manfred Domke

DUAL-USE: Berücksichtigung militärischer Anforderungen bei der zivilen Entwicklung neuer Technologien

In der gegenwärtigen Abrüstungsphase werden zwar Soldaten und Waffensysteme wegverhandelt, Militärhaushalte gekürzt. Die Erforschung und Entwicklung (FuE) militärisch relevanter Technologien geht jedoch unvermindert weiter. Wenn künftig weniger Soldaten und weniger Waffensysteme die Verteidigungsbereitschaft sichern sollen, so müssen nach Meinung der Rüstungsstrategen Kommunikations-, Aufklärungs-, Führungs- und Waffen-Systeme intelligenter und wirksamer gemacht werden. Abrüstung im FuE-Bereich ist also nicht angesagt. FuE-Anstrengungen sollen eher verstärkt werden. Wie ist das bei reduzierten Haushalten zu schaffen? Eine Antwort auf diese Frage lautet: Noch mehr als bisher ist auf Dual-Use-Technologien zu setzen. Dahinter verbirgt sich eine zunehmende Integration militärischer und ziviler FuE-Prozesse sowie eine verstärkte zivile Nutzung neuer Technologien, die gewollt militärische Strukturelemente enthalten. Die Förderung von Dual-Use-Technologien bedeutet Förderung von Militarisierung ziviler Bereiche. Dieser Entwicklung kann nur entgegengetreten werden, wenn die Entstehungs- und Verwertungsbedingungen neuer Technologien analysiert, aufgedeckt und in Wissenschaft und Gesellschaft öffentlich debattiert werden.

Einführung

Das Militär stützt sich auf drei fundamental unterschiedliche Technologiearten:

a) Technologien, die auf militärische Anwendungen zugeschnitten sind, für die es schon aus Kostengründen keinen kommerziellen Markt gibt.
b) Technologien des zivilen Marktes, die auch militärisch genutzt werden.
c) Technologien, die im Interesse der Militärs und für das Militär zivil gefördert, zivil erforscht und entwickelt werden und aus Kostengründen auch zivil genutzt werden sollen.

Im folgenden werden nur die unter c) beschriebenen „Dual-Use-Technologien" betrachtet. Sie unterscheiden sich grundsätzlich von den unter b) genannten. Dual-Use-Technologien, die gemäß b) nur auf zivilen Bedarf zugeschnitten sind, aber dennoch vom Militär benutzt werden, sollen hier nicht weiter untersucht werden.

Die Bezeichnung „doppelt-verwendbare Technologien" gehört zu den Sprachregelungen, die bestehende Verhältnisse verschleiern. Mit „Dual-Use" wird abgelenkt von der Einflußnahme der Sicherheitspolitik auf die Forschungs-, Technologie- und Wirtschaftspolitik sowie vom Einsatz ziviler Ressourcen bei der Entwicklung von Technologien für das Militär. „Dual-Use" sugge-

Dieser Artikel erschien 1991 in dem von Ute Bernhardt und Ingo Ruhmann herausgegebenen Buch „Ein sauberer Tod. Informatik und Krieg“ als Band 15 Schriftenreihe Wissenschaft und Frieden (S.172-191). Herausgeber jener Schriftenreihe waren der Bund demokratischer Wissenschaftlerinnen und Wissenschaftler (BdWi), das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., die Informationsstelle Wissenschaft und Frieden sowie die Naturwissenschaftler-Initiative Verantwortung für den Frieden.

Wir danken Manfred Domke für seine Genehmigung zum Nachdruck dieses Beitrags als Retrospektive in dieser FIfF-Kommunikation.

Die Redaktion

riert Neutralität, Wert- und Zweckfreiheit von Wissenschaft und Technologie. Dem Steuerzahler wird darüberhinaus das Gefühl vermittelt, daß seine Steuern selbst in der Rüstung gut angelegt sind. Der verdeckte Gebrauch ziviler Ressourcen für die Entwicklung neuer Informationstechnologien (IT) für das Militär und die damit einhergehende Deformierung des IT-Sektors können nur dann reduziert bzw. verhindert werden, wenn die Entstehungs- und Verwertungsbedingungen neuer IT analysiert, aufgedeckt und auch in den Bereichen von Wissenschaft und Gesellschaft öffentlich debattiert werden, die nicht am Entwicklungsprozeß beteiligt sind. Zentraler Untersuchungsgegenstand wäre also nicht die doppelte Verwendbarkeit neuer IT, sondern

- die Einflußnahme der Sicherheitspolitik auf die Forschungs-, Technologie- und Wirtschafts-Politik,
- die Unterschiede ziviler und militärischer Anforderungen an die IT,
- die Zusammenhänge zwischen den unterschiedlichen Anforderungen und den entsprechenden Forschungs-, Entwicklungs-, Produktions- und Vermarktungs-Prozessen,
- die Vorteile für Gesellschaft, Wissenschaft, Wirtschaft und Industrie bei Aufgabe der „Dual-Use-Politik“.

Militärische und zivile Geschäftsbereiche unterscheiden sich erheblich. Deutlich wird dies bei Anforderungen, Fertigungsprozessen, Erfolgsfaktoren und Spielregeln. Die Zusammenarbeit beider Geschäftsbereiche in Industrieunternehmen zielt darauf ab, maßgeschneiderte militärische IT-Produkte mit zivilen Geldern zu finanzieren. So konnte der Siemens-Bereich „Sicherungstechnik“, der sich im wesentlichen mit Verteidigungselektronik befaßt, in der Vergangenheit durch Nutzung von Synergien ca. zwei Drittel der Entwicklungskosten unter dem Titel „bezahlt“ buchen.

„Dual-Use-IT“ und sozialverträgliche IT stehen im Widerspruch (z.B. Reduzierung der menschlichen Rolle auf die Funktionstüchtigkeit vs. menschliche Entwicklungsfähigkeit). Ein Abgehen von der „Dual-Use-Politik“ im Bereich IT wäre ein Beitrag zur Entflechtung militärischer und ziviler Forschung und Entwicklung, zur dringend notwendigen „Abrüstung in der FuE“ von IT und damit zur strukturellen Abrüstung.

Dual-Use-Politik

Während über die Reduzierung von Raketen, sonstigen Waffensystemen und Kampftruppen verhandelt wird, soll die „Aufrüstung im FuE-Bereich“ eher noch verstärkt werden. Wegverhandelte militärische Geräte und Soldaten sollen durch den Einsatz sehr teurer supermoderner Technik ausgeglichen werden. Die militärische Überlegenheit bleibt untrennbar mit der Überlegenheit auf dem IT-Gebiet verbunden. Selbst wenn die Rüstungshaushalte sinken sollten, werden die FuE-Aufwendungen vermutlich weiter steigen (vgl. dazu auch den Beitrag „Informationstechnik im Forschungs- und Verteidigungsetat“ in diesem Band[1]). Im ressortübergreifenden Zukunftskonzept Informationstechnik (ZKI) der Bundesregierung[2] wird die wachsende Rolle der Informationstechnik für das Militär beschrieben:

Die Verbesserung der Verteidigungsfähigkeit der Bundeswehr durch effektive Nutzung moderner Technologien sei politisch wünschenswert und als Ziel eine große Herausforderung für Forschung und Industrie. Der Informationstechnik komme dabei eine Schlüsselrolle zu. Ihr Anteil an den Entwicklungs-, Produktions- und Nutzungskosten würde steigen. Die Bundeswehr versuche, sich weitgehend auf Entwicklungen für den zivilen Bereich abzustützen. Dies gelte insbesondere für Führungs- und Informationssysteme und Mikroelektronik.

> *„In Zukunft wird auch verstärkt darauf hinzuwirken sein, sogenannte Dual-Use-Technologien intensiver zu nutzen, d.h. zu versuchen, militärische Forderungen bei zivilen Entwicklungen frühzeitig mitberücksichtigen zu lassen, beziehungsweise auf derartige Dual-Use-Technologien in Form von Add-On-Programmen aufzusetzen, um den militärischen Bedarf zu decken.“* [3]

Im Gegensatz zu den USA werden in der Bundesrepublik die Grundlagenarbeiten für Mikroelektronik und Informationstechnik nicht vom Bundesminister für Verteidigung (BMVg) gefördert. Diese Aufgabe liegt beim Bundesminister für Forschung und Technologie (BMFT)[4].

Bei der Vorstellung des Forschungs- und Technologie-Programms der Bundeswehr[5] wurde darauf hingewiesen, daß es trotz der Abhängigkeit der Verteidigungstechnik von der Mikroelektronik kein BMVg-Programm für militärische Mikroelektronik geben würde.

Absprachen zwischen dem BMVg, dem BMFT und anderen Ressorts sorgen dafür, daß die militärischen Anforderungen in der Forschungspolitik und den FuE-Programmen Berücksichtigung finden.

„Zwischen dem BMFT und dem BMVg bestehen vielfältige, enge Verbindungen auf allen Ebenen. So werden beispielsweise zwischen den Staatssekretären die Grundsatzfragen zur Forschung und Zukunftstechnologie laufend abgestimmt. Dies gilt aber nicht nur für die ‚große Linie': In enger Zusammenarbeit der Fachleute beider Ressorts wird auch – und das ist notwendig – das Vorgehen im Detail koordiniert."[6]

Dual-Use-Interessen

Die Anforderungen an die IT werden vom Militär, der Atomenergie- und der Luft- und Raumfahrtindustrie ständig erhöht. Diese Schubkraft des militärisch-industriellen Komplexes bietet der kommerzielle Markt nicht. Militärische und zivile Anforderungen unterscheiden sich erheblich.

Im Interesse der nationalen Sicherheit und einer gewissen Unabhängigkeit bei der Produktion von Militärtechnik greift der Staat in das Marktgeschehen ein und fördert zugleich Kooperation und Wettbewerb, die sich ergänzen. Der strategische Wert einer engen Kooperation bei der Entwicklung militärisch relevanter Technologien wiegt eventuelle Wettbewerbsnachteile im kommerziellen Bereich auf. Wettbewerb wird als treibende Kraft für ausgezeichnete Leistungen angesehen.

„Despite the commercial competition between Japan and the United States, many U.S. and Japanese experts believe that the strategic value of closer cooperation in defense and economics outweigh the drawbacks of competition."[7]

„E. Wong (OSTP)" (Office of Science and Technology Policy, The White House) „presented the U.S. government view. He explained that the U.S. government officials at this meeting came as observers, not participants, and were attracted by the prominence of international cooperation on the agenda. He recognized many theoretical advantages of cooperation, such as economy in the use of R&D funds that could be used for other means of promoting economic growth in a time of world-wide capital shortage. But he pointed out that the excellence is driven by competition, that Japan has learned better than the U.S. that cooperation and competition can coexist, and praised MITI for fostering both successfully."[8]

Durch staatliche nationale und internationale FuE-Förderprogramme und erhöhten Wettbewerbsdruck soll die Leistungsfähigkeit von Industrie, Hochschulen und FuE-Einrichtungen erhöht werden. Nur so können nach Meinung von Regierung und Industrie die FuE- und Produkt-Märkte den militärischen Bedarf bei ständig steigenden Anforderungen decken. Bezahlbar ist die permanente hochtechnische Sicherheit jedoch nur dann, wenn militärisch unmittelbar relevante Technologien auch zivil vermarktet werden.

Eine offizielle Formulierung der dargestellten Zusammenhänge am Beispiel Luftfahrttechnologie (z.B Hyperschallflugzeuge) liest sich wie folgt:

„Die Luftfahrttechnologie ist durch einen außergewöhnlich raschen Fortschritt gekennzeichnet. Dieser Fortschritt wird nicht nur durch direkte Wettbewerbsanstöße seitens der weltgrößten Firmen und der regionalen Regierungen, sondern ebenso durch die gewaltigen staatlichen Investitionen in Forschung und Technologie beeinflußt. Dies trifft besonders auf die USA zu im Bereich Verteidigung, was wiederum einen beträchtlichen Nutzen durch »Dual Use« für Entwurf und Fertigung ziviler Produkte nach sich zieht."[9]

Der doppelte Nutzen der Förderung militärisch relevanter Technologien ist in der Vergangenheit recht einseitig der militärischen Seite zugute gekommen. Daß dies auch so gewollt ist und auch so bleiben soll, zeigen jüngste Äußerungen aus der US-Rüstungslobby. Als die Reagan-Administration begann, die Rüstungshaushalte massiv zu erhöhen, empfahl Gansler, die Rüstungsindustrie durch Integration militärischer und ziviler Produktionsmittel sowie durch verstärkten Wettbewerb wiederzubeleben. In der Zeit reduzierter Rüstungshaushalte sollen vor allem militärisch orientierte FuE-Kapazitäten durch Dual-Use eine zivile Tarnkappe erhalten. Heute schlagen Gansler und Heilmeier (Texas Instruments Inc.) wieder die Integration des militärischen und zivilen Sektors vor, diesmal allerdings in der entgegengesetzten Richtung, um dem Department of Defense (DoD) Kosten zu sparen:

„The emphasis will be on mobility – that is, lighter equipment –, sustainability, strategic defense, special operations capability, intelligence capability, extended-range weapons, and strong R&D. (...) Pursue commercial diversification, he says, with dual-use technology. (...) The

Manfred Domke

Manfred Domke
Zu Ausbildung und Beruf:
1961-1968 Mathematik-Studium in München,
1968-1970 Zentrallabor für Nachrichtentechnik, Siemens München.
1971-1973 Zentralstelle für das Chiffrierwesen, Bonn
1973-2001 GMD-Forschungszentrum Informationstechnik, Sankt Augustin
2001-2004 Fraunhofer Institut AIS, Sankt Augustin

idea of looking at civilian markets is strongly backed by Jacques S. Gansler, president of Analytic Sciences Corp. of Arlington, Va. »Competitiveness could be improved by a conscious DoD effort to integrate the military and commercial sector,« he says. »For the DoD, this would mean lower costs, increased competition, and a way to gain surge capability. For the commercial sector, it would mean government dollars and increased R&D skills.«

To accomplish such a marriage, says Gansler, defense would have to be »less different«. The defense department would have to move toward the civilian sector in three areas:

- *The government should sponsor dual-use technology, not just fallout.*
- *Plants should be integrated.*
- *The government should use commercial specifications and standards, as well as buying practices."*[10]

„There needs to be much closer harmony and integration between the defense and commercial industrial bases. The DoD can no longer afford to maintain its own separate technology base. It must depend on, and leverage, the commercial industrial base more heavily than at any time in the past 50 years. The barrier to closer integration is not technology, it is DoD's business practices. These have fostered striking contrasts between the currently separate domains. Engineers and companies wishing to participate successfully in the more integrated environment that is inevitable must recognize and adapt to the differences between today's defense and commercial worlds. (...) There are other contrasts – in the basic infrastructures and approaches to systems design and production – that also call for adaption."[11]

In der Bundesrepublik und in der Europäischen Gemeinschaft (EG) wurden von Anfang an militärisch relevante Technologien mit zivilen Geldern gefördert (z.B. BMFT und IT-Förderprogramm ESPRIT der EG).

Obwohl EUREKA eine politisch griffige Alternative zu SDI sein sollte, wurde in der politischen Diskussion über die Aufgabenstellung sehr schnell das Dilemma zwischen ziviltechnologischer und militärischer Nutzung dieser europäischen Technologieinitiative deutlich. Auch in der Bundesrepublik waren einzelne Regierungsstellen sowie starke Gruppen in der CDU/CSU daran interessiert, das Verteidigungsmotiv zur Stärkung der Eureka-Initiative einzusetzen. „Ja, sie wollen den Eureka-Mantel auch zur Finanzierung neuer konventioneller Rüstungstechnologie für eine europäische Verteidigung nutzen." Die Betonung der zivilen Aufgabenstellung war nicht zuletzt deshalb wichtig, weil damit gleichzeitig der verbreiteten öffentlichen Ablehnung des Weltraumrüstens und dem Wunsch Rechnung getragen werden sollte, „daß öffentliche Forschungsmittel direkt zur Förderung wirtschaftlich nutzbarer Technologie eingesetzt werden." Diese Zitate stammen aus einer Lagenotiz[12] der international hochangesehenen Stiftung für Wissenschaft und Politik in Ebenhausen, die vor allem dem Kanzleramt, Auswärtigem Amt und Verteidigungsministerium zuarbeitet, mit dem Privileg, auch Geheimdokumente auswerten zu dürfen.

Militärisch unmittelbar relevante Technologien, die über kommerzielle Märkte allein nicht finanzierbar sind, bringen den Unternehmen auch über den Export hohe Gewinne. Das ist selbst für Länder wie Japan interessant, in denen ein generelles Waffenexportverbot existiert. Durch den Verkauf von Dual-Use-Technologien kann ein Exportverbot umgangen werden. (Das generelle Waffenexportverbot Japans aus dem Jahr 1976 wurde 1983 durch eine Vereinbarung zwischen den USA und Japan eingeschränkt. Seitdem ist der Transfer von militärischem Know-How Japans ausschließlich in die USA gestattet.)

„Yielding in part to U.S. pressure and in part to its own feeling that it would be better off depending less on the United States, Japan has increased its military budget by 5-6 percent annually during the past decade to nurture domestic weapon systems and subsystems. (...) Another charge is that Japanese companies may be eyeing the export market in military weapons. But government reversal of the current ban on arms export is unlikely to happen in the near future because the issue is politically sensitive and the Liberal Democratic Party is already weak, Nishihara said. What might happen, however, is circumvention of the export ban by selling dual-use subsystems, he said. (...) In contrast to the U.S. technology, Japanese technology emphasizes commercial applications but even so has military applications of interest to the United States. R&D conducted at universities and industry is generally not carried out specifically with eventual military applications in mind, but may be dual-use in nature."[13]

Dual-Use-Beispiele

Im ZKI[14] heißt es, daß Mikroelektronik, Bildverarbeitung, Computer Aided Engineering, Software-Engineering, Rechnerstrukturen, Kommunikationstechnik und Künstliche Intelligenz notwendige Grundlagen für die Bundeswehr definieren, „auf denen, aufbauend auf bestehenden zivilen Ergebnissen, ressortspezifische Ausprägungen notwendig sind." Es sei daran erinnert, daß diese zivilen Ergebnisse als Dual-Use-Technologien bereits bestimmte militärische Anforderungen erfüllen.

Die FuE-Schwerpunkte in der BRD, der EG, den USA und Japan unterscheiden sich nicht wesentlich. Es überrascht nicht, wenn die oben genannten Dual-Use-Technologien in der Liste der kritischen Technologien des DoD (1989) wieder zu finden sind, die langfristig die Überlegenheit der US-Waffensysteme sichern sollen. Dazu gehören u.a. auch Supraleiter, Antriebssysteme oder Biotechnologie.

Anhand von Beispielen soll im folgenden gezeigt werden, daß

- qualitative Anforderungen der Militärs durch technologiepolitische Initiativen der US-Militärs als allgemein verbindliche Standards durchgesetzt werden sollen,
- es gravierende Unterschiede zwischen militärischen und zivilen Technologie-Anforderungen gibt,
- die frühzeitige Berücksichtigung militärischer Anforderungen im Rahmen ziviler FuE sehr aufwendig sein kann, weil dazu spezifische Methoden und Fertigungstechniken erforderlich sind.

Defense Critical Technologies

1	Semiconductor Materials & Microelectronic Circuits	The production and development of ultra-small integrated electronic devices for high-speed computers, sensitive receivers, automatic control, etc.
2	Software Engineering	The generation, maintenance, and enhancement of affordable and reliable software in a timely fashion.
3	High Performance Computing	High performance computing systems having 10^3 fold improvements in computation capability and 10^2 fold improvements in communication capability by 1996.
4	Machine Intelligence & Robotics	Incorporation of aspects of human "intelligence" into computational devices which enable intelligent function of mechanical devices.
5	Simulation & Modeling	Visualization of complex processes and the testing of concepts and designs without building physical replicas.
6	Photonics	Includes ultra-low-loss fibers and optical components such as switches, couplers, and multiplexers for communications, navigation, etc.
7	Sensitive Radar	Radar sensors capable of detecting low-observable targets, or capable of non-cooperative target classification, recognition, and/or identification.
8	Passive Sensors	Sensors not needing to emit signals to detect targets, monitor the environment, or determine the status or condition of equipment.
9	Signal & Image Processing	Combination of computer architecture, algorithms, and microelectronic signal processing devices for near real-time automation of detection, classification, and tracking of targets.
10	Signature Control	The ability to control the target signature (radar, acoustic, optical, or other) and thereby enhance the survivability of vehicles and weapon systems.
11	Weapon System Environment	A detailed understanding of the natural environment (both data and models) and its influence on weapons system design and performance.
12	Data Fusion	The machine integration and/or interpretation of data and its presentation in convenient form to the human operator.
13	Computational Fluid Dynamics	The modeling of complex fluid flow to make dependable predictions by computing, thus saving time and money previously required for expensive facilities and experiments.
14	Air Breathing Propulsion	Light-weight, fuel efficient engines using atmospheric oxygen to support combustion.
15	Pulsed Power	The generation of repetitive, short-duration, high-peak power pulses with relatively light-weight, low-volume devices for weapons and sensors.
16	Hypervelocity Projectiles & Propulsion	The ability to propel projectiles to greater-than conventional velocities (over 2.0 km/sec), as well as understanding the behavior of projectiles and targets at such velocities.
17	High Energy Density Materials	Compositions of high-energy ingredients used as explosives, propellants, or pyrotechnics.
18	Composite Materials	Two or more constituent materials that are combined together in such a manner to produce a substance possessing selected properties superior to those of its individual components.
19	Superconductivity	Makes use of the zero resistance property and other unique and remarkable properties of superconductors for creation of high-performance sensors, electronic devices and subsystems, and supermagnet based systems.
20	Biotechnology	The systematic application of biology for an end use in military engineering or medicine.
21	Flexible Manufacturing	The integration of production process elements aimed at efficient, low cost operation for small, as well as high, volume part number variations, with rapidly changing requirements for end product attributes.

Aus Platzgründen verzichten wir in diesem Heft auf den Nachdruck der im Orignaltext an dieser Stelle folgenden Beispiele. Diese sind im Originalartikel nachzulesen unter

www.fiff.de/alias/domke1991

Zusammenfassung

Technischer Fortschritt, orientiert am alten Prinzip, daß der Krieg der Vater aller Dinge sei, dominiert weiterhin den sozialen und menschlichen Fortschritt. Die Entstehungsprozesse neuer Technologien werden in ihrer politischen, wirtschaftlichen, wissenschaftlichen und technischen Dimension nicht transparent gemacht. Die dahinterliegenden Interessen- und Machtstrukturen, die allenfalls exemplarisch erkennbar sind, müssen aufgedeckt werden. Deshalb sollten alternative Projekte vorrangig die Zusammenhänge zwischen Sicherheits-, Forschungs-, Technologie- und Wirtschaftspolitik einerseits und den Forschungs- und Entwicklungsprozessen andererseits zum Untersuchungsgegenstand machen. Dabei sind insbesondere die Beziehungen zwischen militärischen und zivilen Anforderungen an die IT und den Fertigungsmethoden, Fertigungstechniken und Fertigungsprozessen zu untersuchen. Dringend erforderlich sind Analysen zur Dimensionierung der neuen IT. Es ist zu fragen, ob und inwieweit die Mega- und Giga-Dimensionen im Chipbereich oder die Teraflop-Dimension im Supercomputerbereich zur Lösung der drängenden gesellschaftlichen Probleme, wie z.B. Klima, Luft, Wasser, Boden, Nahrung, Abfall, Drogen, Arbeitslosigkeit, Grundrechte und Demokratie, beitragen. Umfassende Anforderungsanalysen an eine IT, die orientiert ist an der Wiederherstellung, am Erhalt und an der Verbesserung menschlicher Lebensgrundlagen, müssen erarbeitet werden. Vom Dual-Use-Konzept ist radikal Abschied zu nehmen. Ziel muss es sein, über eine Abrüstung im FuE-Bereich zu einer Richtungsänderung in der Forschungs- und Technologiepolitik zu gelangen. Statt IT, die militärisch sehr relevant ist, muß eine sozialförderliche IT erforscht und entwickelt werden. Ohne eine in der Öffentlichkeit geführte Diskussion wird dieses Ziel nicht erreicht werden können. Die Technologiedebatte muß über den Kreis technikorientierter Experten hinausgehen.

Anmerkungen

1 Anmerkung der Redaktion: Karlheinz Hug (1991): Informationstechnik im Forschungs- und Verteidigungsetat. Ein Vergleich. In: U. Bernhardt & I. Ruhmann (Hrsg.): Ein sauberer Tod. Informatik und Krieg. Schriftenreihe Wissenschaft und Frieden (Band15). Bonn: BdWi/FIfF, S.234-249.
2 ZKI, BMFT und BMWi, 1989, S. 120 ff
3 ebd., S. 122
4 Protokoll, 1983
5 Forndran, 1985
6 Rüstungsstaatssekretär Timmermann in Sadlowski (1984)
7 Chen, 1989, S. 29
8 Kahaner, 1990, S. 10
9 EG, 1988, S.3
10 Wolff, 1990
11 Rosenblatt, 1990, S. 39-40
12 Deubner, 1985, S. 21
13 K.T. Chen, 1989, S. 28, 32
14 ZKI, S. 123

Literatur

Adam, J.A. (1990): Toward smaller, more deployable forces, as lethal as can be, in: Special Report DEFENSE: How much is enough?, IEEE Spectrum, November, S. 30-41.

BMFT-Joumal (1987): Durchbruch bei der Supraleitung, Nr.4 / August, S. 8.

Cates, R. (1990): Gallium arsenide finds a new niche, IEEE Spectrum, April, S. 25-28.

Chen, K.T. (1989): The State of Japan's military art, IEEE Spectrum, September, S. 28-33.

Dahlem, P. (1990): Aufträge in den Stemen, high-Tech 4/90, S. 106-109.

Deubner, C. (1985): Kritische Überlegungen zu Eureka, Stiftung Wissenschaft und Politik, Ebenhausen, SWP-LN 2446, August.

DOD (1989): The Department of Defense Critical Technologies Plan for the Committees on Armed Services United States Congress, 15 March.

Domke, M. (1988): Einflußnahme von Politik, Militär und Industrie auf die Informatik am Beispiel Supercomputer, in: Rudolf Kitzing u.a. (Hrsg.) Schöne neue Computerwelt, Zur gesellschaftlichen Verantwortung der Informatiker, Verlag für Ausbildung und Studium in der Elefantenpress Berlin, S. 136-163.

Domke, M. (1990): Janusgesicht der zivilen Forschung (JESSI und Dual-Use), die computer zeitung, 11. Juli, S. 21-22.

Domke, M. (1990): JESSI und Dual-Use, Beispiel für Großindustrie-Subventionen und verdeckte Rüstungs-Haushalte, Informatik Forum, 4. Jahrgang, Heft 3, September, S. 147-151.

EG (1988): Strategisches Forschungs- und Technologieprogramm im Bereich Luftfahrt, Mitteilung der Kommission an den Rat und an das Europäische Parlament, Technologie-Nachrichten, Programm-Informationen, Nr. 434-2. November, S. 1-16.

Forndran, D. (1985): Das Forschungs- und Technologiekonzept der Bundeswehr, 58. Arbeitstagung der Deutschen Gesellschaft für Wehrtechnik e.V., 24.-25. April, Bonn-Bad Godesberg.

Gansler, J.S. (1982): Can the Defense Industry Respond to the Reagan Initiatives? International Security, Spring, Vol. 6, No. 4, S. 102-121.

Gilmore, H.L. (1984): R&M Implications of the DoD Acquisition Improvement Program, IEEE Transactions on Reliability, Vol. R-33, No.2, June, S. 138-144.

Kahaner, D.K. (1990): New Information Processing Technology (NIPT) Workshop, held in Hakone I Japan, 1-2 December, e-mail report 26 Dec, gmd-news vom 15.1.1991.

Lathrop, R.H. et al. (1990): „Functional abstraction" anticipates timing glitches, IEEE Spectrum, April, S. 41-42.

Naegele, T. (1989): Hard times in Rad-Hard, Electronics/May, S. 82-87.

OTA (1988): Commercializing High-Temperature Superconductivity, Congress of the United States, Office of Technology Assessment, OTA-ITE-388, Washington, U.S. Printing Office, June.

Protokoll (1983): Über ein Gespräch von BMFT und BMVg mit Vertretem aus Wissenschaft und Industrie über verteidigungsrelevante Informationstechnik am 17./18. November 1983, Bonn, BMFT/413, 1. Dezember.

Riesenhuber, H. (1990): Zum Stand der Durchführungsphase des Eureka-Programms für Mikroelektronik JESSI (Joint European Submicron Silicon), Pressemitteilung Nr.43/90, BMFT-Pressereferat Bonn, 19. April.

Rosenblatt, A. (1990): Expert observers: defining national technology options, IEEE· Spectrum, Volume 27, Number 11, November, S. 37-41.

Sadlowski, M. (1984): Innovationsfreundliche Beschaffungspolitik, wt-Gespräch mit dem Rüstungsstaatssekretär, wt 11/84, S. 14-16.

Sanders, J. and Mitchel, A. (1990): Dateline 1995!, Parallelogram, November, S. 8-9.

Santo, B. and Wollard, K. (1988): The world of silicon: it's dog eat dog, IEEE Spectrum, September, S. 30-39.

US Air Force (1987): The US Air Force R&M 2000 Initiative, IEEE Transactions on Reliability, Vol. R-36, No.3, August, S. 277-381.
Voelcker, J. (1988): Flex in specs: A license to innovate?, IEEE Spectrum, Volume 25, Number 12, November, S. 55-60.
Waller, L. (1987): VHSIC finally builds a head of steam, Electronics, April 16, S. 84-86.
Wolfe, A. (1986): DoD seeks a standard 32-bit instruction set, Electronics, February 24, p.24.
Wolff, H. (1990): As defense costs face the ax, the scenarios fly thick and fast, How to get by in hard times, letter from the Pentagon, Electronics June, S. 8-13.
ZKI (1989): Zukunftskonzept Informationstechnik, BMFT und BMWi, Bonn, August.

Jens Rinne

AC11 – der AKtiVCongreZ

Der AKtiVCongreZ (AC11) – die ungewohnte Schreibweise kommt daher, dass im Namen die drei Organisationen AK-Vorrat, CCC und AK Zensur verewigt sind – wurde Mitte Februar 2011 zum zweiten Mal veranstaltet. Unterstützt wurde der Kongress vom DGB-Bildungswerk und der Bundeszentrale für politische Bildung.

Wie im Vorjahr, beim AC10, gab es erfreulicherweise erneut eine Förderung durch die Bundeszentrale für politische Bildung; diese hatte auf dem dort einen Beobachter, und im Nachgang wurden infolge seines Berichtes die Förderbedingungen für die Ausrichtung von Aktiventreffen angepasst. Somit können Versammlungen von Aktiven seither direkter und einfacher gefördert werden.

Im Januar wurde vom FoeBuD leider recht kurzfristig zum AC11 eingeladen. Dadurch wurden leider nicht alle möglichen 50 Plätze ausgeschöpft. Es ist jedoch verständlich, das der FoeBuD eigenen Terminkollisionen mit der für im April anstehenden Big-BrotherAwards-Verleihung vermeiden wollte und den AKtiV-CongreZ daher kurzfristig nach vorne verlegte. An die Aktiven und Interessierten geht der Appell, sich den Termin fürs kommende Jahr schon mal vorzumerken und freizuhalten.

Wie im letzten Jahr wurde inhaltlich auf dem AKtiVCongreZ viel und intensiv gearbeitet. Von Freitagabend ab 19:00 Uhr bis Sonntag um 12:00 Uhr standen insgesamt 41 Zeitstunden zur Verfügung. Im Plenum bzw. in parallel stattfindenden Arbeitsgruppen wurden davon alleine 17 Stunden gearbeitet – ohne Pausen. Beim Bier, in der im Tagungshaus befindlichen Sauna, beim Pausentee und -kaffee, sowie zu den Essenszeiten wurde nicht minder intensiv diskutiert, und vor allem dort wurden persönliche Bekanntschaften geknüpft, weswegen sich die Ruhezeit mitunter auf die wenigen Schlafstunden reduzierte.

Die professionelle Moderation, die uns das Wochenende begleitete, hat den vorherrschenden Aktivitätsdrang der Anwesenden sehr gut geordnet und ihn in konstruktive Bahnen gelenkt. Sie hat dadurch deutlich zum Gelingen des AC11 beigetragen. Die TeilnehmerInnen haben sich ihrerseits darauf eingelassen, sich motivieren zu lassen und konstruktiv mitzuarbeiten.

So haben wir unter anderem das Greenpeace-Kampagnenmodell auf unsere abstrakte Datenschutz- und Bürgerrechtsthematik übertragen; dies lieferte gute Herangehensweisen.

Lange Diskussionen und Überlegungen zur diesjährigen „Freiheit-statt-Angst"_Demonstration bereiteten einen Vorschlag vor, der auf die Mailingliste des AK-Vorrat getragen wird, um dort gemeinsam auch mit den nicht anwesenden Aktiven zu einer realisierbaren Entscheidung zu kommen, die von allen getragen und durch mehrere Personen umgesetzt werden kann.

Darüber hinaus lässt sich das Wochenende inhaltlich nur schwer beschreiben – es passierte so viel Gleichzeitiges und alle wichtigen Themen wurden angesprochen oder sogar vertieft bearbeitet. Eine Auflistung kann hier nur unvollständig sein.

Interessant war für mich persönlich – neben dem Kennenlernen von vielen Personen –, die einvernehmliche Verständigung der Anwesenden, miteinander eingeschränkt öffentlich zu kommunizieren und geschützte Kommunikationsräume zuzulassen. Wir haben uns darauf verständigt, nicht alle Beiträge sofort öffentlich werden zu lassen, sondern Ergebnisse zunächst zu konsolidieren. Nach viel zerbrochenem Geschirr im AK Vorrat in den letzten Jahren und persönlichen Erlebnissen bei Diskussionen bzgl. einer eingeschränkt öffentlichen Kommunikation im AK Zensus (ei-

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.

nem Arbeitskreis des AK Vorrat), beginnt offensichtlich im persönlichen Kontakt sich wieder ein Grundvertrauen auszubreiten und die Zusammenarbeit im Vordergrund zu stehen.

Die Bewegung wird erwachsen und braucht genau diese Gelegenheiten, sich mit sich selbst auseinander zu setzten und wieder neu zu positionieren. Von einer Stockung oder Erlahmung kann bei den anwesenden verschiedenen Meinungen nicht die Rede sein. Dennoch bestehen innerhalb der Bewegung verschiedene Auffassungen der weiteren Ausrichtung, dies muss aber nicht zu einer Spaltung, sondern kann konstruktiv angegangen zu einer Belebung werden. Die vorhandenen persönlichen Animositäten und strukturellen Widersprüche in der Zusammenarbeit wurden an dem Wochenende ebenso angesprochen und für die Anwesenden durchaus befriedigend geklärt.

Die TeilnehmerInnen werden sich jeweils wie bisher persönlich dafür einsetzen und dafür sorgen, die Bewegung weiter in Bewegung zu halten, damit es zu grundsätzlichen Veränderungen im Lande kommt. Dies war die positive Grundstimmung aller, als am Sonntagmittag viele nach Hause aufbrachen und etliche noch zum Weiterarbeiten blieben.

Persönliche Treffen sind eine unverzichtbare Ergänzung für Mailinglisten, auf denen Menschen zusammenarbeiten will. Ob dies beim AKtiVCongreZ erfolgt oder im Rahmen einer Großdemo ist zweitrangig, die Möglichkeit miteinander ins Gespräch zu kommen und sich kennenzulernen ist immanent wichtig.

Das DBG-Bildungszentrum in Hamburg-Sasel ist absolut erhaltenswert. Leider gibt es beim DGB Überlegungen, sie zu schließen. Ich hoffe, sie steht auch für den nächsten AKtiVCongreZ wieder zur Verfügung – in unserem Interesse und vor allem in dem der dort beschäftigten.

Also dann bis zum nächsten Mal (bei der FIfF-Jahrestagung im November in München, bei den BigBrotherAwards oder dem nächsten AKtiVCongreZ, dem AC12.

Ralf E. Streibl

Ein exemplarischer Fall

Anmerkungen zur Causa Guttenberg aus der Perspektive von Informatik und Gesellschaft

Karl Theodor Maria Nikolaus Johann Jacob Philipp Franz Joseph Sylvester Freiherr von und zu Guttenberg[1] (im weiteren Verlauf abgekürzt KTzuG) geriet ab Mitte Februar 2011 ob seiner Dissertation in einen Strudel von Ereignissen, die innerhalb von knapp zwei Wochen zur Aberkennung des ihm von der Universität Bayreuth verliehenen Doktorgrades als auch zu seinem Rücktritt von seinen politischen Ämtern führten. Es scheint mir spannend, die »Causa Guttenberg« im Nachgang aus der Perspektive des Fachgebiets »Informatik und Gesellschaft« zu betrachten, da es hier vielfältige Bezüge gibt. Für eine ausführliche und detaillierte Analyse der Affäre war – angesichts des bereits weit überschrittenen Redaktionsschlusses dieser FIfF Kommunikation (an dieser Stelle vielen Dank für die hierdurch arg strapazierte Geduld des Layouters!) – nicht wirklich Zeit. Insofern sind die folgenden Anmerkungen vor allem als Anregung zu begreifen, der ein oder anderen Frage vertieft nachzugehen, dabei aber das Ganze nicht aus dem Blick zu verlieren.

Urheberrecht und Plagiate

Am Anfang war das Wort. Im konkreten Fall waren es mehrere, ja sogar recht viele Worte. Und diese stammten nicht von dem Autor, der für das Gesamtwerk verantwortlich zeichnete. Betrachten wir daher zum Einstieg – quasi als Hintergrund der Affäre – einige Paragraphen des Urheberrechtsgesetzes[2],

> *„§1 Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe dieses Gesetzes."*
>
> *„§11 Das Urheberrecht schützt den Urheber in seinen geistigen und persönlichen Beziehungen zum Werk und in der Nutzung des Werkes."*

Das Zitieren regelt §51, darauf Bezug nehmend ist in §63 „stets" die deutliche Angabe der Quelle gefordert. Leinveber führte hierzu bereits 1966 aus:

> *„Zweck der Quellenangabe ist es, unbeschadet der freien Werkbenutzung das Urheberpersönlichkeitsrecht auch in diesem Punkt im Hinblick auf die Urheberehre*

> *zu wahren, ferner aber auch, eine Nachprüfung der Richtigkeit der Entlehnung zu ermöglichen und zugleich den Ursprung des angeführten Gedankens nachzuweisen und dadurch das benutzte Werk dem Interesse des Lesers näherzubringen, so dass in diesem Werbemoment ein gewisser Ausgleich für die entschädigungslose Wiedergabe des benutzten Werkes liegt. Hiergegen wird in der Praxis nicht selten verstoßen. Das Gebot des literarischen Anstands erfordert aber, dass gerade in diesem Punkt peinlich korrekt verfahren wird. Dazu gehört, dass bei jeder Entlehnung die Quelle genau nach der Fundstelle bezeichnet wird, also unter Verfasser- und Titelangabe, Auflage und Seitenzahl oder Abschnitt mit Anmerkungsziffer usw."*[3]

Andreas Fischer-Lescano, Professor für Völkerrecht an der Universität Bremen, berichtet in einem Interview, wie es zu der Entdeckung kam: Im Zusammenhang mit der Vorbereitung einer Lehrveranstaltung sowie einer Rezension für die Zeitschrift *Kritische Justiz* befasste er sich mit KTzuGs Dissertation als einschlägige Arbeit eines konservativen Rechtspolitikers. Inhalt und Qualität dieses Werkes überzeugten ihn nicht wirklich. Die Frage, ob er gezielt nach Plagiaten gesucht habe, verneint er und erläutert:

> *„Aber mir fiel auf, dass das Niveau dieser Arbeit – sowohl sprachlich als auch argumentativ – sehr uneinheitlich war. Besonders schwach fand ich die Passage, in der es um den fehlenden Gottesbezug in der EU-Verfassung geht. (...) Ich habe diese Passage gegoogelt, weil ich vermutete, dass zu Guttenberg teilweise seine eigenen politischen Reden verwendet haben könnte. Das ist zwar zulässig, aber ich hätte in meiner Rezension kritisiert, dass es sich inhaltlich rächt, wenn man politische Reden als Versatzstücke für eine Patchwork-Dissertation benutzt. Prompt fand ich einen Link ...“*[4]

Dieser Link – und auch diverse weitere, die später gefunden wurden – führte bekanntlich jedoch nicht zu eigenem Material KTzuGs, sondern zu verschiedenen Presse- und Fachartikeln, und auch bei Materialien des wissenschaftlichen Dienstes des Bundestags hat sich der Autor bedient. Nach Absprache mit der Redaktion der *Kritischen Justiz* informierte Fischer-Lescano zunächst die Gutachter an der Universität Bayreuth. Am 16.02.2011 titelte dann die *Süddeutsche Zeitung*:

> *„Plagiatsvorwurf gegen Verteidigungsminister. Guttenberg soll bei Doktorarbeit abgeschrieben haben“*[5]

Zur Etymologie der Aneignung fremden geistigen Eigentums:

Das Wort *Plagiat* als Ausdruck für den »Diebstahl geistigen Eigentums« geht – so berichtet das Duden Herkunftswörterbuch (Duden Bd. 7, 3. Aufl. 2001) – auf das lateinische Wort *plagium* zurück, welches übersetzt »Menschenraub, Seelenverkauf« bedeutet. *Plagiator* – im heutigen Sprachgebrauch »jemand, der ein Plagiat begeht; Abschreiber« – bedeutete danach im Lateinischen »Menschenräuber«.

KTzuG äußerte sich am 16.2.2011 zu den Vorwürfen zunächst folgendermaßen:

> *„Der Vorwurf, meine Doktorarbeit sei ein Plagiat, ist abstrus. Ich bin gerne bereit zu prüfen, ob bei über 1.200 Fußnoten und 475 Seiten vereinzelt Fußnoten nicht oder nicht korrekt gesetzt sein sollten und würde dies bei einer Neuauflage berücksichtigen.“*[6]

Was bedeutet ein Plagiatsvorwurf genau? Loewenheim schreibt im Handbuch des Urheberrechts über »Plagiate«:

> *„Plagiat ist diejenige Urheberrechtsverletzung, bei der sich jemand fremde Urheberschaft bewusst anmaßt. Es geht also um den Vorwurf des geistigen Diebstahls, der bewussten Aneignung fremden Geistesguts: Jemand gibt sich als Urheber eines von einem anderen geschaffenen Werkes aus. (...) Auch das Zitat ohne Quellenangabe stellt ein Plagiat dar, wenn der Eindruck erweckt wird, das Zitierte stamme vom Zitierenden. Der Begriff des Plagiats geht auf die Antike zurück. Das Urheberrechtsgesetz verwendet ihn nicht. Wird der Vorwurf des Plagiats erhoben, so kommt es rechtlich darauf an, ob ein Tatbestand der Urheberrechtsverletzung erfüllt ist.“*[7]

KTzuG am 18.2.2011:

> *„Meine von mir verfasste Dissertation ist kein Plagiat, und den Vorwurf weise ich mit allem Nachdruck von mir. Sie ist über etwa sieben Jahre neben meiner Berufsabgeordnetentätigkeit als junger Familienvater in mühevollster Kleinarbeit entstanden und sie enthält fraglos Fehler. (...) Es wurde allerdings zu keinem Zeitpunkt bewusst getäuscht oder bewusst die Urheberschaft nicht kenntlich gemacht.“*

KTzuG argumentierte angesichts immer deutlicher und umfangreicher werdender Vorwürfe hinsichtlich Plagiaten in seiner Dissertation stets, er „habe nicht bewusst getäuscht“ – möglicherweise als Rettungsanker, sich auf »Kryptomnesie« herauszureden. Dies ist ein Begriff dafür, dass der zweite Urheber Dinge oder Formulierungen für eigene Schöpfung hält, die er zuvor als verborgene Erinnerung in sein Unbewusstes aufgenommen hat. In diesem Fall wäre dann der Vorsatz zu verneinen, weshalb dieser Einwand in Urheberrechtsprozessen oft als Schutzbehauptung herhalten muss.[8] Und so erklärte KTzuG am 21.2.2011 auf einer Parteiveranstaltung, auf der er ankündigt, den Doktortitel dauerhaft nicht mehr führen zu wollen, nochmals:

> *„Und nach dieser Beschäftigung habe ich auch festgestellt, wie richtig es war, dass ich am Freitag gesagt habe, dass ich den Doktortitel nicht führen werde. Ich sage das ganz bewusst, weil ich am Wochenende, auch nachdem ich diese Arbeit mir intensiv noch einmal angesehen habe, feststellen musste, dass ich gravierende Fehler gemacht habe. Gravierende Fehler, die den wissenschaftlichen Kodex, den man so ansetzt, nicht erfüllen. Ich habe diese Fehler nicht bewusst gemacht.“*

Informatik und Bildung

Plagiate im Bereich der Bildung sind keineswegs ein neues Phänomen. Im Zeitalter riesiger Datenbestände in einem globalen Netz ist es jedoch für Suchende sehr viel einfacher geworden, Material zu einem spezifischen Thema zu finden. Stefan Weber formuliert dies in seinem Buch *Das Google-Copy-Paste-Syndrom* ebenso plakativ wie einleuchtend (vgl. Kasten).

Natürlich blieb die durch die Leichtigkeit des Quellenzugangs angeregte Zunahme an Plagiaten nicht verborgen. Für diejenigen, die die Arbeiten korrigieren, sind die verwendeten Textbausteine schließlich ebenso leicht zugreifbar – das hätte KTzuG wissen können wie jeder Schüler. Erfolgreiches (quid?!) Plagiieren erfordert einen beträchtlichen Aufwand, um zum einen an nicht ganz offensichtliche bzw. leicht zugängliche Textquellen heranzukommen, zum anderen um die übernommenen Texte

„In den vergangenen Jahren, so die allgemeine These, sind womöglich tausende und abertausende akademische Arbeiten entstanden, bei denen die »Autoren« so gut wie kein eigenes Hirnschmalz investieren mussten. Die Schüler und Studenten von heute texten zunehmend nicht mehr selbst. Sie lesen tendenziell nicht, schon gar nicht genau, und schreiben auch ungern selbst verfasste Sätze. Texte sind vielmehr immer öfter das Ergebnis eines dreistufigen Prozesses:

1) *Ergoogelung des Themas: Das Eintippen eines Worts oder einer Wortkette wie etwa »Medienrezeption +Kindheit« in die Suchmaschine Google. Dann das meist eher oberflächliche Navigieren durch die Ergebnisse; die Wikipedia oder Börsen wie hausarbeiten.de sind oft ganz vorne dabei.*

2) *Aneignung von prägnanten, »wohlklingenden« Textbausteinen durch Copy/Paste, genauer: Markieren im Web, dann Steuerung + C, dann Steuerung + V in Word.*

3) *Textbearbeitung: Montage/Collagieren dieser Textsegmente; eventuell sprachliche Adaption, Vereinheitlichung von Schreibweisen von Fachbegriffen, schließlich ansprechendes Layout. Denn in der (akademischen) Textkultur des Als-Ob zählt primär die Form und nicht der Inhalt.*

Wichtig ist, dass am Ende ein Produkt herauskommt, das seinen Fake-Charakter auf den ersten Blick verschleiert. Und Studierende wissen: Selten geht es noch um mehr als um diesen ersten flüchtigen Blick."

aus: Weber, S. (2009): Das Google-Copy-Paste-Syndrom. Wie Netzplagiate Ausbildung und Wissen gefährden. 2. Aufl. Hannover: Heise, S.7.

so zu kaschieren, dass die Übernahme nicht sofort auffällt bzw. entdeckt werden kann. Man kann feststellen, dass in den letzten Jahren die Zahl der Veröffentlichungen zum Thema Plagiate in Schule und Studium deutlich angestiegen ist. Das Problem ist zum Thema geworden.[9] Neben praktischen Ratgebern zum Aufdecken von Plagiaten werden z.B. auch die unterschiedlichen Sichten von Studierenden und Lehrenden verglichen[10]. Immer häufiger wird dabei auch die Frage aufgeworfen, ob die sorglose Bedienung am geistigen Eigentum anderer auch Ausdruck eines kulturellen Zeitwandels sein könnte.

Das Spektrum möglicher Konsequenzen für ertappte Plagiatoren ist potenziell recht groß. Allgemeingültige Verfahren und Regelungen gibt es nicht – insbesondere hängt die Beurteilung auch von der Schwere des Vorfalls ab. Naheliegend ist jedoch, dass Plagiate in einer Dissertation, der zentralen Qualifikationsarbeit in der Wissenschaft, deutlich dramatischer zu beurteilen sind als das Abschreiben in einem Schulaufsatz. Insofern richteten sich schnell die Blicke Richtung Bayreuth, wo die Universität dann am 23.02.2011 auch die Entscheidung verkündete, KTzuG den Doktorgad abzuerkennen.[11]

Sozialisation mit digitalen Medien

Ohne an dieser Stelle ins Detail gehen zu können, sei hier darauf verwiesen, dass sich die Gesellschaft in den letzten Jahren durch Digitalisierung und globale Vernetzung stark verändert hat: War früher das private Kopieren der Langspielplatte eines Freundes oder einer Freundin auf eine Compact Cassette ein zeitintensiver und mit Klangverlust behafteter Akt, so ist im Zeitalter digitaler Kopien und Flatrates qualitativ verlustfreies und schnelles Kopieren urheberrechtlich geschützter Werke mit einer Reichweite deutlich jenseits des persönlichen Umfeldes tagtägliche Praxis geworden. In mancherlei Hinsicht mag die Einfachheit auch eine Mentalität befördert haben, die eher durch Sammeln gekennzeichnet ist, also durch Wertschätzung und Anerkennung des geistigen Eigentums anderer. Die Selbstverständlichkeit der ubiquitären medialen Zugänglichkeit lässt Fragen nach der Rechtmäßigkeit der Nutzung in den Hintergrund rücken. Fragen nach dem gesellschaftlichen Verständnis von Original und Kopie bringt Buggert in seinem Editorial zu einer Schwerpunktausgabe »Raubkopien« der Online-Zeitschrift *archimæra* in folgenden Sätzen zum Ausdruck:

> *„Oftmals begnügen wir uns mit Kopien, seien es die geklauten CDs aus dem Internet, das Remake eines berühmten Filmes oder die Revival-Band, die gute alte Zeiten wieder aufleben lässt. Es stellt sich nun die Frage, wie die Bedeutung des Originals in Zukunft verstanden wird. Hat uns die digitale Welt von der Verpflichtung zum Original befreit? Welchen Einfluss haben die virtuellen Welten auf unser Verständnis von Realität und wieviel Weltflucht können wir uns erlauben? Welche Formen des Umgangs mit Originalen gelten und welche Erkenntnisse sind in der Auseinandersetzung mit ihnen zu gewinnen? Welches Repertoire liegt unseren heutigen Bemühungen, Originelles zu schaffen, zu Grunde, und stellt dieses Repertoire eine Verbindlichkeit dar? Wann ist ein Zitat eine Kopie und wann eine Kopie eine Raubkopie, ein Plagiat?"*[12]

Der Zugang zu Informationen verändert sich – man kann mehr und mehr den Eindruck gewinnen, dass für viele (und dazu gehören nicht nur Kinder und Jugendliche, die mit diesen Angeboten aufgewachsen sind) die Welt der Recherche bei *google* und *Wikipedia* beginnt und gleich darauf wieder endet. Mediale Querverweise, Wiederholungen, Variationen und selbstdarstellerische Kommentierungen überbieten einander im Kampf um die karge Aufmerksamkeit. Das gefundene Material scheint zur freien Verfügung zu stehen. Der einstige Traum der Informationsgesellschaft – jeder kann selbst Sender sein – hat sich zumindest teilweise erfüllt, im Guten wie im Schlechten.

Virtuelle Gemeinschaften

Am 17. Februar 2011 wurde das *GuttenPlag Wiki*[13] gegründet, nach eigenem Verständnis eine *„Kollaborative Dokumentation von Plagiaten in der Dissertation »Verfassung und Verfassungsvertrag: Konstitutionelle Entwicklungsstufen in den USA und der EU« von Karl-Theodor Freiherr zu Guttenberg. (...) Die gefundenen Plagiate erlauben es der akademischen und allgemeinen Öffentlichkeit, sich selbst ein Bild des Falls zu machen."*

Binnen kürzester Zeit erhielt diese Plattform einen hohen Bekanntheitsgrad und wurde ihrerseits zur Recherchequelle vieler Journalisten. Das Prinzip: Einzelnen Textpassagen der Dissertation, die jemand als Plagiat erkannt zu haben glaubte, können auf der Plattform zusammen mit dem als Ausgangsquelle vermuteten Textabschnitt in Form von Zitaten mit Quellenangaben eingestellt werden, so dass jede und jeder den Vorwurf prüfen und kommentieren kann. Zum Zeitpunkt der Drucklegung des vorliegenden Artikels wird an einem Abschlussbericht gearbeitet.

Aus der Perspektive von Informatik und Gesellschaft ist *GuttenPlag* als ein spannendes Beispiel für die Eigendynamik des Web 2.0 anzusehen. Eine zuvor nicht existierende Gruppe formierte sich aus einem aktuellen Anlass zu einem bestimmten Zweck – nicht formal konstituiert, sondern über ein digitales Medium kommunikativ organisiert. Ähnlich wie bei anderen Wikis und Datenbanken sowie bei *open source Projekten* wird kritischen Einwänden hinsichtlich der Glaubwürdigkeit mit dem Argument sozialer Qualitätssicherung begegnet. Im *Guttenplag FAQ* heißt es dazu:

> *„Das Wiki bemüht sich um korrekte Ergebnisse, nicht um Zuverlässigkeit. Das heißt: Änderungen der Ergebnisse, insbesondere Korrekturen aufgrund zutreffender Kritik. (...) Das mittlerweile sehr gut organisierte Wiki dokumentiert jeden Plagiat einzeln und wortgenau, woraufhin diese Dokumentationen von Administratoren und vielen Lesern geprüft werden."*[14]

Schutz von Persönlichkeitsrechten

Wenn an verschiedenen Stellen im Netz und in den Medien der Fokus in solch starker Weise auf eine Person gerichtet wird und alle schauen hin – kommen hier nicht möglicherweise Aspekte von »Cybermobbing« oder medialen Feindbildern zum Tragen? Wie sieht es mit dem Schutz der Persönlichkeitsrechte des Betroffenen aus?

Wurde also mit *GuttenPlag* ein »digitaler Pranger« im Netz errichtet, einzig mit dem Ziel der Karriere und Person eines Politikers zu schaden? Auch innerhalb des Kreises der *GuttenPlag*-Nutzerinnen und Nutzer wurde dies bereits sehr früh angesprochen und im Forum z.B. über eine allgemeinere »PlagiPedia« nachgedacht.

Die Frage der Rechtmäßigkeit einer detaillierten Berichterstattung über persönliche Aspekte einzelner Menschen (insb. sogenannter »Personen des öffentlichen Lebens«) ist grundsätzlich schwierig – auch die reguläre Presse hat hier öfters Klärungsprobleme, die von Fall zu Fall (nachträglich) vor Gericht geklärt werden. Im konkreten Fall KTzuG ist das Medium *GuttenPlag* wohl eher als eine harmlose Variante anzusehen, da die Einträge auf den Wiki-Seiten jeweils aus zitierten und mit nachvollziehbaren Quellenverweisen versehenen Ausschnitten der veröffentlichten Dissertation KTzuGs sowie anderer Veröffentlichungen bestehen. Fragen von Anprangerung oder persönlichen Angriffen stellten sich im Laufe der Affäre somit wohl eher in anderen Kontexten. Ein Beispiel sind die harschen Dialoge am 23.02.2011 im Deutschen Bundestag.[15] Das Ansinnen der CDU/CSU, dort KTzuG zugedachte Bezeichnungen wie „Betrüger", „Lügner" oder „Hochstapler" rügen zu lassen, wurde vom Ältestenrat jedoch abgelehnt.

Informationsfreiheit

Im Falle einer Veröffentlichung – wie z.B. einer Dissertation – hat die Öffentlichkeit prinzipiell Zugang zu dem Medium, um sich eine eigene Meinung zu bilden und Sachverhalte zu überprüfen. Dies ist längst nicht bei allen Dokumenten der Fall. Daher sollte offensiv daran gearbeitet werden, die Anzahl öffentlicher Quellen weiter zu erhöhen, auch wenn nicht unbedingt davon auszugehen ist, dass jegliches Dokument ein vergleichbar hohes Interesse hervorrufen wird wie diese Dissertation.

Online-Kommunikation

Im Nachgang zu der der Aktuellen Stunde im Deutschen Bundestag wandten sich einige Doktorandinnen und Doktoranden in einem offenen Brief an die Bundeskanzlerin, um ihren Unmut und ihr Unverständnis hinsichtlich des politischen Umgangs mit der Plagiatsaffäre von KTzuG zum Ausdruck zu bringen. Neben den bis dahin bekannten Fakten bezogen sich die Unterzeichnerinnen und Unterzeichner des Briefes auch auf die Bedeutung der Affäre für ihre eigene Situation:

> *„(...) Herr zu Guttenberg hat am 23. Februar 2011 in der Aktuellen Stunde im Deutschen Bundestag darauf verwiesen, er wolle nur nach seiner Tätigkeit als Verteidigungsminister beurteilt werden. Er hat dabei auf eine Formulierung von Ihnen angespielt, wonach Sie ihn nicht als »wissenschaftlichen Assistenten« eingestellt hätten.*
>
> *Dies ist eine Verhöhnung aller wissenschaftlichen Hilfskräfte sowie aller Doktorandinnen und Doktoranden, die auf ehrliche Art und Weise versuchen, ihren Teil zum wissenschaftlichen Fortschritt beizutragen. Sie legt darüber hinaus nahe, dass es sich beim Erschleichen eines Doktortitels um ein Kavaliersdelikt handele und dass das »akademische Ehrenwort« im wirklichen Leben belanglos sei. (...)*
>
> *Möglicherweise aber halten Sie unseren Beitrag zur Gesellschaft schlicht für vernachlässigenswert. Dann möchten wir Sie aber bitten, in Zukunft nicht mehr von der von Ihnen selbst ausgerufenen „Bildungsrepublik Deutschland" zu sprechen. (...)"*[16]

Der Brief fand über diverse Mailinglisten, Online-Plattformen, Foren und andere elektronische Wege in Windeseile seinen Weg durch die akademische Welt der Republik und wurde innerhalb vier Tagen von Zehntausenden junger Wissenschaftlerinnen und Wissenschaftler mit unterzeichnet.

Informatik und Politik

Die Schnelligkeit digitaler Kommunikation und die Möglichkeit, ortsunabhängig binnen kurzer Zeit Unterstützerinnen und

Unterstützer für Projekte zu erhalten, zeigt das politische Potenzial dieser Medien. Dennoch stellt sich die Frage, warum nicht jedes Thema gleichermaßen solche Resonanz auslöst wie der Fall KTzuGs. Vermutlich sind hier mehrere Faktoren zusammengekommen. Zum einen seine – wie er in seiner Rücktrittserklärung auch ansatzweise selbstkritisch durchklingen ließ – eigene Funktionalisierung der Massenmedien zu Gunsten seiner Themen und persönlichen Popularität, zum anderen aber auch das überaus schlechte Krisenmanagement im Kontext der Plagiatsaffäre. Es scheint, als habe KTzuG zu Beginn völlig unterschätzt, dass diesem Thema in Teilen der Bevölkerung ein hohes Interesse entgegengebracht wurde und jeder Versuch, Zeit zu gewinnen oder den Sachverhalt herunterzuspielen oder in seiner Bedeutung zu relativieren gerade gegenteilige Wirkung entwickelte: Das Fehlen von Transparenz sowie der Eindruck, dass hier „etwas unter den Teppich gekehrt" werden solle oder mit zweierlei Maß gemessen werde, aktivierte weite Kreise, sich stärker mit dem Thema auseinanderzusetzen bzw. sogar selbst aktiv nachzuforschen.

> *„Politiker werden gern an moralischen Maßstäben gemessen – ganz im Kontrast zur gleichzeitig weitverbreiteten Überzeugung vom »schmutzigen Geschäft« der Politik mit ihren Sachzwängen, die Politiker scheinbar zu Opfern und nicht zu Tätern machen."*[17]

Preiser arbeitet in seinem lesenswerten Beitrag von 1989 die Rolle der Medien bei politischen Skandalen heraus, so z.B. dass Medien latente Skandale in manifeste Skandale transformieren und dass es ohne Medien kein politisches Skandalbewusstsein gäbe. Es wird interessant, diese Überlegungen vor dem Hintergrund der seither gewachsenen Online-Medien sowie der netzbasierten Recherche- und Kommunikationsmöglichkeiten weiter zu diskutieren. Preiser spricht über den hohen Aufmerksamkeitswert von Skandalen, aber auch das kurzlebige öffentliche Interesse. Auch hier mag die leichte Recherchierbarkeit der Vergangenheit im Netz möglicherweise Veränderungen bringen. Es ist für einzelne Bürgerinnen und Bürger heute viel leichter als früher möglich, sich selbst ein Bild davon zu machen, was beispielsweise Politiker vor einigen Monaten oder Jahren gesagt haben und wie sie sich zu einem späteren Zeitpunkt diesbezüglich verhalten haben.

Digitale Kunst und Satire

Über allen jene Debatten und Diskurse darf aber auch nicht vergessen werden, dass KTzuG in seiner Plagiatsaffäre vielfältige Anregungen für künstlerische und satirische Aufarbeitungen bot. Oft beziehen sich diese direkt auf Computer-Aspekte – erwähnt seien hier exemplarisch die vielfältigen bei eBay und andernorts feilgebotenen Guttenberg-Tastaturen mit reduziertem Tastenlayout sowie die »Copy-Paste« für die Haare oder die Star-Trek-Hommage »Wir sind Guttenborg!!! Ihr Text wird unserer Doktorarbeit hinzugefügt – Widerstand ist zwecklos!«.[18]

Virtuelle Gemeinschaften – Nachschlag

Nicht nur KTzuGs Kritiker nutzen das Netz. Es gibt bekanntlich Facebookseiten pro KTzuG, deren Unterstützerzahlen weit in die Hunderttausende gehen.[19] Die Erwartung oder Hoffnung mancher Befürworter, dass aus diesen virtuellen Unterstützerzahlen auch eine Massenbewegung auf den Straßen werden würde, hat sich bei den geplanten Demonstrationen am 5.3.2011 jedoch nicht bestätigt. Der Nordbayerische Kurier berichtete diesbezüglich:

> *„Zu den Sympathiekundgebungen in insgesamt acht Städten hatte die Facebook-Gruppe »Wir wollen Guttenberg zurück« aufgerufen. Die Initiatoren sprechen sich auf der Internet-Plattform Facebook trotz der Plagiatsaffäre für ein politisches Comeback des 39-Jährigen aus. Bis Samstagmorgen wurde der Link »Gefällt mir« dort 570.000 Mal angeklickt. Inwieweit es sich um echte »Unterstützer« handelt, ist aber offen."*[20]

Anstelle von tausenden Befürwortern kamen an den meisten Orten nur wenige oder gar keine Pro-KTzuG-Demonstrierende. Und mancherorts lockte der Demo-Aufruf auch die Spötter und Gegner auf die Straße.

Leben in der Informationsgesellschaft

Das Internet als größte Bibliothek und umfassendes Wissensreservoir der Welt – dies war ein Wunschtraum, der beim Ausbau der »Datenautobahnen« und bei der Vernetzung zum »globalen Dorf« immer wieder beschworen wurde. Und in der Tat: Wie der Fall KTzuG zeigt, lässt sich im Netz durchaus vieles finden.

Bislang ist vielen Menschen wohl noch nicht handlungsleitend bewusst geworden, dass »das Netz« nicht so leicht vergisst. Ob Peinlichkeiten, Privates oder unangemessene Äußerungen und Dialoge – vieles was einmal netzöffentlich war, ist weltweit zugreifbar, bleibt erhalten und suchbar und ist oft schwer bis gar nicht aus dem Netz zu entfernen. Für die oder den Einzelnen mag dies dann durchaus unangenehme Folgen haben.

In Bezug auf seine Plagiatsaffäre muss KTzuG aber wohl damit leben, dass er als Person des öffentlichen Lebens und der Zeitgeschichte im Fokus medialer Aufmerksamkeit stand. Auch die Plagiatsaffäre mit allen Vorwürfen, Dementis, Fakten und Reaktionen bleibt somit dauerhaft Teil seiner virtuellen Vita.

Im Online-Katalog der Universität Bremen steht übrigens inzwischen beim Katalogeintrag von KTzuGs Dissertation als Bemerkung:

> *„Zugl.: Bayreuth, Univ., Diss., 2006 (02/2011: Doktorgrad aberkannt)"*

Verantwortung

KTzuG betonte bei vielen Erklärungen im Zusammenhang mit seiner Plagiatsaffäre, dass er Verantwortung übernommen habe (und auf die Führung des Doktertitels vorübergehend / dauerhaft verzichte / die Universität bitte, die Verleihung des Doktortitels zurückzunehmen), ebenso in seiner Rücktrittserklärung am 1.3.2011:

> *„(...) Und ich gehe nicht alleine wegen meiner so fehlerhaften Doktorarbeit, wiewohl ich verstehe, dass dies für*

große Teile der Wissenschaft ein Anlass wäre. Der Grund liegt im Besonderen in der Frage, ob ich den höchsten Ansprüchen, die ich selbst an meine Verantwortung anlege, noch nachkommen kann. (...).“

Nur langsam, Stück für Stück – immer wenn die vorherigen Aussagen und Behauptungen gar nicht mehr zu halten waren, und in dem Maße, in dem immer weitere Kreise sein Verhalten kritisch beäugten – kamen von KTzuG weitergehende Aussagen. Aus „abstrusen“ Vorwürfen wurden „vereinzelt nicht korrekt gesetzte Fußnoten“, „fraglos Fehler“, „gravierende Fehler“ und es gab noch eine abstrakte Entschuldigung bei all jenen, „die ich aufgrund meiner Fehler und Versäumnisse verletzt habe“.

Befürworter seiner Person sowie politische Freunde sahen nach KTzuGs Erklärungen jeweils die Angelegenheit als erledigt an. Er habe Fehler eingestanden / sich entschuldigt – und außerdem habe das Ganze ohnehin nichts mit seinem politischen Amt zu tun. Diese Rechnung ging jedoch nicht auf. Zu viele Menschen sahen Zusammenhänge zwischen persönlichem Verhalten und Amt, und sie wollten – zumindest nicht nahtlos – einen Menschen, dessen persönliche Glaubwürdigkeit so massiv gelitten hatte, in solch verantwortungsvoller Position sehen. Auch im Wissenschaftsbetrieb wäre wohl kaum vermittelbar gewesen, wie KTzuG vor dem Hintergrund der Faktenlage gleichzeitig noch qua Amt für die Bundeswehr-Hochschulen hätte zuständig sein können.

Verantwortung zu übernehmen heißt nicht nur, darüber zu sprechen. Diese Lektion musste KTzuG offenkundig lernen.

Fazit

Ein abschließender Ausblick vor dem Hintergrund meiner eigenen Lehrtätigkeit:

Vielerorts wurde im Reflex auf den Fall KTzuG gefordert, dass Prüfungsarbeiten umfassend durchleuchtet und am besten vollständig mit Plagiatsprüfungssoftware gecheckt werden solle. Einmal davon abgesehen, dass entsprechende Softwareprodukte in ihrer Zuverlässigkeit und ihrer Funktion kritisch zu diskutieren sind, greift diese Forderung m.E. aus prinzipiellen Gründen völlig daneben:

Genauso, wie ich keine Vorratsdatenspeicherung aller Telekommunikationsdaten haben möchte (obwohl so vielleicht einmal ein Terrorist entdeckt werden könnte), möchte ich auch keine verdachtsunabhängige Vollkontrolle, um Plagiatsünder aufzuspüren. Beides drückt ein grundsätzliches Misstrauen gegenüber allen Menschen aus – ein Misstrauen, welches ich weder habe, noch haben möchte. Selbstverständlich – und das wissen auch die Studierenden – mache ich vereinzelt Stichproben und natürlich gehe ich immer dann auf die Suche, wenn ich konkreten Anlass zu der Vermutung habe, dass Textpassagen nicht von den Studierenden stammen, die sie in ihrer Arbeit abgegeben haben.

Für die nächsten Jahrgänge von Studierenden freue ich mich darauf, dass dank KTzuG hinsichtlich des Themas Plagiate eine gewisse Grundaufmerksamkeit vorhanden sein dürfte. Die in *GuttenPlag* dokumentierten Stellen bieten für Kurse im »Wissenschaftlichen Arbeiten« eine Fülle guter Beispiele, um über die Problematik und Abgrenzbarkeit von Plagiaten konkret zu diskutieren.

Aus der Perspektive von »Informatik und Gesellschaft« – dies hat hoffentlich dieser Beitrag zeigen können – gibt es ebenfalls viele Anknüpfungspunkte, den Fall (und hier meine ich ihn nun wirklich in doppelter Wortbedeutung als Causa und den daraus resultierenden Absturz) des KTzuG vielschichtig zu analysieren und zu diskutieren.

Friedrich Dürrenmatt schrieb in den 21 Punkten zu seiner Komödie *Die Physiker*:

„(4) Die schlimmstmögliche Wendung ist nicht vorhersehbar. Sie tritt durch Zufall ein.

(9) Planmäßig vorgehende Menschen wollen ein bestimmtes Ziel erreichen. Der Zufall trifft sie dann am schlimmsten, wenn sie durch ihn das Gegenteil ihres Ziels erreichen: Das, was sie befürchteten, was sie zu vermeiden suchten (...).“[21]

Anmerkungen

1 Im vorliegenden Beitrag spielt auch die Leichtigkeit eine Rolle, mit der in der sogenannten Informationsgesellschaft auf Daten zugegriffen werden kann, hier symbolisiert durch die aus Wikipedia (Stichwort »Karl-Theodor zu Guttenberg«, 5.3.2011) in den Artikel hineinkopierte Langfassung des Namens. Auch für die weiteren Recherchen zu diesem Beitrag waren diverse Suchmaschinen und Datenbanken im Internet ausgesprochen hilfreich. Die bei der Abfassung des Textes verwendeten Quellen werden übrigens angegeben.

Ralf E. Streibl

- **Ralf E. Streibl** ist Diplom-Psychologe
- Mitglied im FIfF-Vorstand und in der Redaktion der FIfF-Kommunikation
- hauptberuflich tätig an der Universität Bremen im Studienzentrum Informatik
- Schwerpunkte in der Lehre: »Informatik und Gesellschaft« sowie »Wissenschaftliches Arbeiten«

2 Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG). Bonn: Bundesministerium der Justiz. http://bundesrecht.juris.de/bundesrecht/urhg/gesamt.pdf

3 Leinveber, G. (1966): Rechtsprobleme um das sog. „große und kleine Zitat" zu wissenschaftlichen Zwecken. In: Gewerblicher Rechtsschutz und Urheberrecht, 68 (9), S. 479-482.

4 „Ich wollte es nicht glauben" – Ein Gespräch mit dem Juristen Andreas Fischer-Lescano, der zu Guttenberg entlarvte. In: DIE ZEIT, 24.2.2011, (9), S.40.
Die Rezension von Fischer-Leskano für die Zeitschrift „Kritische Justiz" wurde vorab im Internet veröffentlicht:
Fischer-Lescano, A. (2011): Rezension zu „Karl-Theodor Frhr. zu Guttenberg, Verfassung und Verfassungsvertrag. Konstitutionelle Entwicklungsstufen in den USA und der EU, Berlin (Duncker & Humblot) 2009". In: Kritische Justiz, 44 (1) (im Druck), S.112-119. http://www.kj.nomos.de/fileadmin/kj/doc/zu_guttenberg.pdf

5 Preuß, R.; Schultz, T. (2011): Plagiatsvorwurf gegen Verteidigungsminister. Guttenberg soll bei Doktorarbeit abgeschrieben haben. In: Süddeutsche Zeitung, 16.02.2011, http://www.sueddeutsche.de/politik/1.1060774

6 Dieses Zitat sowie die weiteren im Text wiedergegebenen wörtlichen Aussagen von KTzG habe ich der Tagesschau-Chronologie „Von »abstrusen Vorwürfen« zur Rücktrittserklärung" entnommen. http://www.tagesschau.de/inland/guttenberg770.html

7 Loewenheim, U. (2010): Handbuch des Urheberrechts. 2. Auflage. München: Beck. §8, Rn. 24

8 vgl. Zimmer, T. (2003): Die psychologische Dimension des Urheberrechts. In: Zeitschrift für Urheber- und Medienrecht, 47 (3), S.474f.

9 Vgl. z.B.:
Rieble, V. (2008): Das Wissenschaftplagiat. Frankfurt/M.: Klostermann.
Roberts, T.S. (ed.) (2008): Student plagiarism in an online world: problems and solutions. Hershey: Information Science Reference.

10 vgl. z.B. Sutherland-Smith, W. (2008): Plagiarism, the Internet and student learning: improving academic integrity. New York: Routledge.

11 Medienmitteilung Nr. 037/2011 der Universität Bayreuth vom 23. Februar 2011: Universität Bayreuth erkennt zu Guttenberg den Doktorgrad ab. http://www.uni-bayreuth.de/presse/info/2011/040-037-gutten.pdf

12 Buggert, D. (2009): Raubkopie (Editorial). In: archimæra, (2), S.3-4. http://www.archimaera.de/download/archimaera_raubkopie.pdf

13 http://de.guttenplag.wikia.com/wiki/GuttenPlag_Wiki

14 http://de.guttenplag.wikia.com/wiki/FAQ

15 Fragestunde „Plagiatsvorwürfe im Zusammenhang mit der Dissertation des Bundesministers der Verteidigung" sowie später am gleichen Tag eine Aktuelle Stunde „auf Verlangen der Fraktionen SPD und BÜNDNIS 90/ DIE GRÜNEN: Die Stellungnahme des Bundesministers der Verteidigung Dr. Karl-Theodor Freiherr zu Guttenberg und mögliche Textübernahmen aus Ausarbeitungen des Wissenschaftlichen Dienstes des Deutschen Bundestages sowie angebliche Textübernahmefunde nach »GuttenPlag Wiki« auf 270 Seiten der Dissertation des Bundesministers der Verteidigung", dokumentiert im Plenarprotokoll 17/92 des Deutschen Bundestages, http://www.bundestag.de/dokumente/protokolle/plenarprotokolle/17092.pdf

16 http://offenerbrief.posterous.com/causa-guttenberg-offener-brief-von-doktorande, vgl. auch:
"Ich bin begeistert von der Kraft des Internets" – Interview mit Tobias Bunde. Spiegel online, 01.03.2011, http://www.spiegel.de/unispiegel/studium/0,1518,748251,00.html

17 Preiser, S. (1989): Ganz normale menschliche Reaktionen. Skandalverarbeitung im Spannungsfeld politischer Erfahrungen, Werte und Einstellungen. In: Moser, H. (Hrsg.): L'Eclat c'est moi. Zur Faszination unserer Skandale. Weinheim: Deutscher Studien Verlag, S.98-117.

18 http://www.fastbacklink.de/blog/wp-content/uploads/guttenberg-tastatur.png
http://www.stupidedia.org/images/2/27/Copypaste.jpg
http://twitpic.com/43cbx6

19 z.B. http://www.facebook.com/ProGuttenberg

20 http://www.nordbayerischer-kurier.de/nachrichten/1299561/details_8.htm

21 Dürrenmatt, F. (1980): 21 Punkte zu den Physikern [geschrieben für den Sammelband Komödien II, 1962]. In: Die Physiker. Zürich: Diogenes.

(Abrufdatum aller Links 6.3.2011)

Bild aus dem Burgenbuch der Staatsbibliothek Bamberg, Staatsbibliothek Bamberg, RB.H.bell.f.1 Original von 1523, Druckvorlage des Babenberg Verlag mit Genehmigung der BibliothekUrheber, PD

Lesen –
Neues für den Bücherwurm

Ralf E. Streibl

„Die Hoffnung stirbt zuletzt“

Memorabilien, Recherchen und Schlussfolgerungen eines De-Plagiators

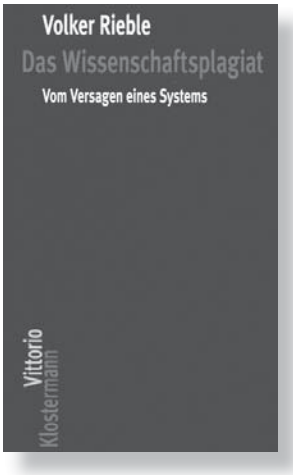
Das Buch ist lesenswert – soviel kann ich direkt sagen. Den Grund hierfür oder die Wirkung der Lektüre auf mich zu beschreiben ist viel schwieriger. Volker Rieble, Inhaber des Lehrstuhls für Arbeitsrecht und Bürgerliches Recht der Ludwig-Maximilians-Universität München, legte mit „Das Wissenschaftsplagiat“ ein in Form und Inhalt stark juristisch geprägtes kleines Büchlein vor, welches dennoch leicht lesbar und in Teilen fast anekdotisch unterhaltsam einher kommt. Und doch: im Kern stimmt es nachdenklich, macht wütend und die Lektüre hinterlässt auch eine gewisse Hilflosigkeit. Erschienen vor dem Guttenberg-Dissertations-Desaster erhält das 120-seitige Büchlein plötzlich intensive Aufmerksamkeit. Es ist beileibe nicht die einzige Publikation, die sich diesem Thema widmet. Aber es gibt zwei wesentliche Unterschiede:

Zum einen diskutiert Rieble sowohl die Entstehung von Plagiaten, als auch die seiner Ansicht nach mangelnde Aufdeckung und Sanktionierung nicht nur als persönliche Verfehlung. Es sieht diese im Grundsatz auch systembedingt – befördert durch wissenschaftlichen Konkurrenz- und Publikationsdruck ebenso wie durch Abhängigkeitsverhältnisse im Wissenschaftsbereich (was z.B. die Verwertung von Arbeiten Studierender oder von Mitarbeiterinnen und Mitarbeitern angeht).

Zum anderen benennt Rieble eine ganze Reihe seiner Meinung nach identifizierte Plagiatoren namentlich. Der Autor vertritt die Position, es sei geboten und notwendig, Plagiatoren öffentlich zu benennen – als Sanktion, aber vor allem auch zum Schutz und Rettung der Autorenehre für die geschädigten Urheberinnen und Urheber, deren Textpassagen unter dem Namen des Plagiators als scheinbar dessen geistige Schöpfung beliebig zitiert und weiterverbreitet würden.

Natürlich erhält das Buch durch die detaillierten und konkreten Beispiele einen ganz anderen Authentizitätscharakter. Oder ist es nur ein skandallüsterner Hinschaufaktor, vergleichbar der Schaulust mittelalterlichen Publikums angesichts am Pranger stehender Delinquenten? „Das geschieht den Plagiatoren recht!“, mag das aufrechte Wissenschaftlerherz konstatieren. Doch welches sind die Kriterien? Da es sich bei den von ihm benannten Personen nicht immer um rechtskräftig verurteilte Plagiatoren handelt, sondern teilweise um Riedels eigenen Interpretationen wissenschaftlichen Fehlverhaltens, hat ihm und dem Verlag die Namensnennung erwartungsgemäß schon Rechtsstreitigkeiten eingebracht. Einzelne Betroffene haben inzwischen eine einstweilige Anordnung erwirkt: Das Buch darf in dieser Form nicht nachgedruckt werden, allerdings kann die bereits vorhandene Auflage noch verkauft werden.

Manche Schilderungen, Gedanken und Forderungen Riebels zum Wissenschaftssystem und seinen Rahmenbedingungen sind gut nachvollziehbar und recht anregend, selbst weiterzudenken. Andere Überlegungen des Autors kommen jedoch weniger plausibel einher, so scheinen mir beispielsweise seine Kenntnisse, sein Verständnis und seine Auseinandersetzung mit *Open Access* und *Creative Commons* recht verkürzt zu sein. Sollte es eine überarbeitete zweite Auflage geben, wäre hier auf jeden Fall Nachbesserungsbedarf.



Erfrischend deutlich bleibt Rieble hingegen in seiner Forderung, dass Wissenschaft und Gesellschaft derartiges Fehlverhalten nicht dulden dürfen. Für sich zieht er den Schluss, dass Wissenschaftsethik und Selbstregulation nicht ausreichen, demzufolge brauche es – hier spricht der Jurist – klarer gesetzlicher Regelungen und rechtlicher Sanktionen.

Am Ende seiner Arbeit resümiert Rieble mit Blick auf „Abschreiber“:

> *„Das ist der Preis, den der Wissenschaftsautor mit dem Schritt an die Öffentlichkeit zahlt: dass nämlich sein Werk in jeder Hinsicht diskutiert wird – auch mit Blick auf dessen Herkunft. Wissenschaft ist gefährlich“ (S.110).*

Ex-Doktor und Ex-Minister zu Guttenberg wird ihm diesbezüglich wohl recht geben.

Volker Rieble (2010): Das Wissenschaftsplagiat. Vom Versagen eines Systems. Frankfurt/M.: 2010. 120 S., 14,80 €.

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
Kontoverbindung: 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
- **Ralf E. Streibl** – Bremen
- **Joerg Zeltner** – Köln

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	Carsten Büttemeier, Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Jens-Holger Streck, Ralf E. Streibl (Koordination)
Schwerpunktredaktion	Stefan Hügel und Ralf E. Streibl
V.i.S.d.P.	Ralf E. Streibl
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 *sj@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *res@fiff.de*
Layout	Berthold Schroeder
Titelbild	Eine Wordle-Verarbeitung von »213.251.145.96/About.html« / R. E. Streibl
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*)

Verleihung der BigBrotherAwards
1.4.2011 in Bielefeld
www.bigbrotherawards.de

!!! Stichtag der Volkszählung 2011 !!!
9.5.2011 – siehe auch *www.zensus11.de*

FIfF-Studienpreis 2011
31.5.2011 Ende der Einreichungsfrist (vgl. Seite 20)

FIfF-Jahrestagung 2011
„Dialektik der Informationssicherheit – Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit"
11. – 13.11.2011 in München

FIfF-Vorstandssitzung

Juni 2011 in Bremen (genauer Termin noch offen)
September 2011 in Köln (genauer Termin noch offen)
13. November 2011 in München (im Rahmen der Jahrestagung)

FIfF-Kommunikation

2/2011 »transparenz.arbeit.kontrolle«
Stefan Hügel, Ralf E. Streibl u.a.
(Redaktionsschluss: 30.4.2011)

3/2011 »IT in Europa«
Stefan Hügel u.a.
(Redaktionsschluss: 05.8.2011)

W&F – Wissenschaft & Frieden:

1/11 – Moderne Kriegführung

2/11 – Kosten des Krieges

DANA – Datenschutz-Nachrichten:

1/11 – transparenz.arbeit.kontrolle

2/11 – Datenschutzprobleme moderner Technik

3/11 – Online-Spiele

4/11 – Datenschutz im Bildungswesen

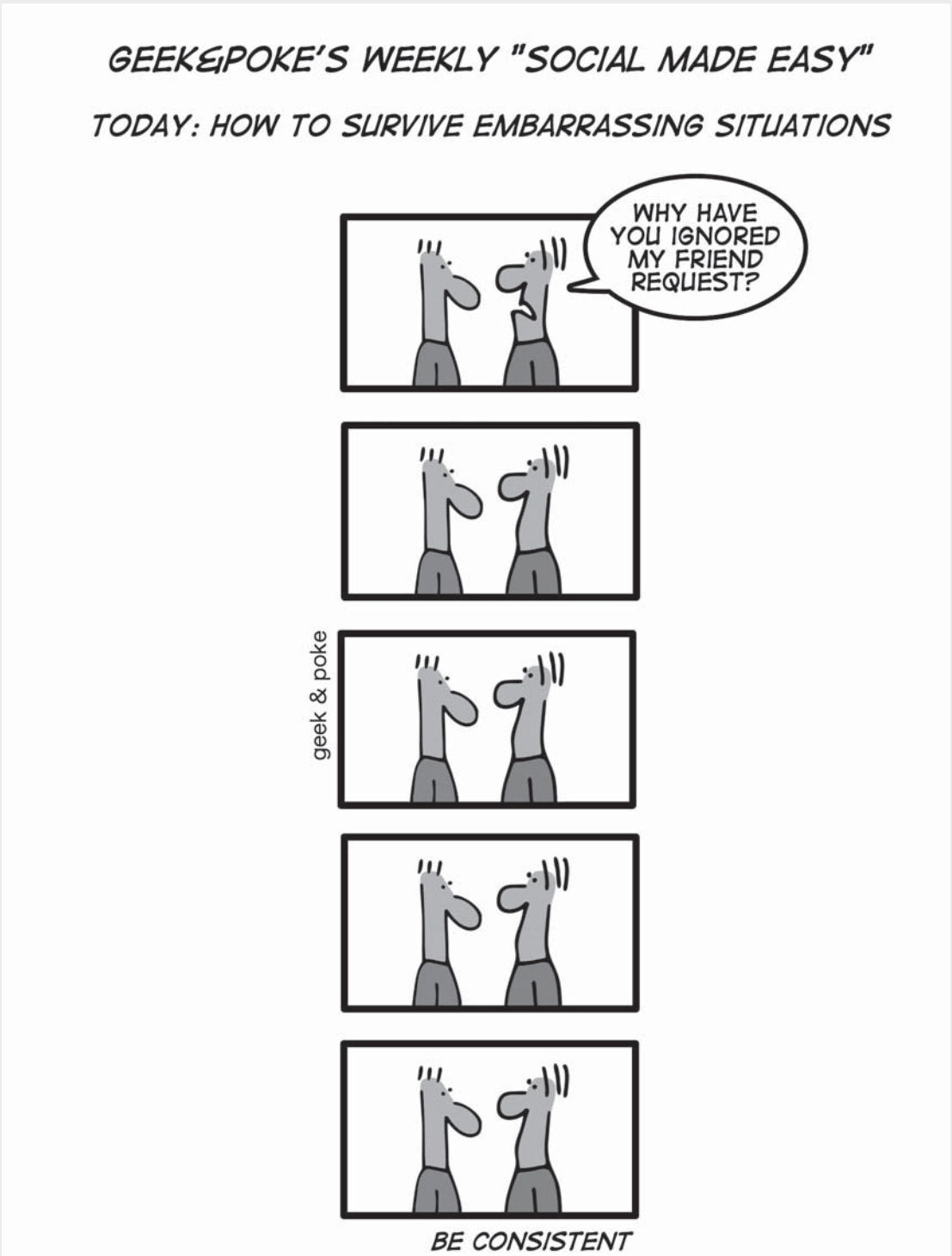
Das FIfF-Büro

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



Cartoon von Oliver Widder
Website: http://www.geekandpoke.com

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