H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

31. Jahrgang 2014 Einzelpreis: 7 EUR

2/2014 – Juni 2014

ISSN 0938-3476

• Schwerpunkte: Überwachung – Videoüberwachung – BigBrotherAwards 2014 •

FIfF Kommunikation

Titelbild: Fotomontage zur Überwachung/Videoüberwachung
Bildnachweis Seite 65

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Inhalt

Ausgabe 2/2014

inhaltt

Editorial

Das Thema *Überwachung* lässt uns nicht los. Diese Ausgabe enthält dazu gleich einen dreiteiligen Schwerpunkt: Zuerst befassen wir uns mit der *alltäglichen Überwachung vor allem der Kommunikation* durch Nachrichtendienste und staatliche Behörden. Ein zweiter Abschnitt hat die *Videoüberwachung* zum Thema, die sich in unserer Umgebung weiterhin ausbreitet, und im dritten Abschnitt des Schwerpunkts berichten wir von den *BigBrotherAwards*, die wie jedes Jahr in Bielefeld verliehen wurden.

Obwohl die Debatte um die Ausspähung – begonnen durch Berichte des *Guardian* aufgrund der Dokumente von Edward Snowden – nun gut ein Jahr andauert, sind wenig ernsthafte politische Konsequenzen sichtbar. Selbst der inzwischen gebildete NSA-Untersuchungsausschuss lässt nicht gerade Anzeichen eines unbändigen Aufklärungswillens erkennen – lieber streitet man sich über die Anhörung wesentlicher Zeugen. Die Bundesregierung scheint durch die Angst gelähmt, einen wichtigen Bündnispartner zu verprellen. Doch die Affäre muss Konsequenzen haben. *Werner Koep-Kerstin* und *Stefan Hügel* haben einen Katalog von *Forderungen zur Ausspähaffäre* zusammengestellt, die nach den Enthüllungen an Politik und Justiz zu richten sind.

Wenn auch unser Blick vor allem auf die Situation in Deutschland gerichtet ist, dürfen wir die Ausspähung in anderen Ländern und Regionen nicht vergessen. *Maria Xynou* berichtet von der Situation in Indien: *Surveillance in the world's largest democracy*. Sie fragt, wie demokratisch die größte Demokratie der Welt angesichts dieser Überwachung tatsächlich ist.

Nichts als Hilflosigkeit verspüren *Jens Crueger* und *Thomas Krämer-Badoni* angesichts der von ihnen konstatierten Unumkehrbarkeit der Überwachung digitalisierter Datenströme. Der eigentliche Kampf müsse zukünftig um die Frage geführt werden, wer die Erkenntnisse der Überwachung nutzen und was er damit machen darf. Sie erwarten einen langen Kampf mit vielen Rückschlägen.

John Perry Barlow erklärte in den neunziger Jahren die Unabhängigkeit der Netzbürger im Cyberspace. Für *Albrecht Funk* erscheint dies in seinem Beitrag *Nationale Sicherheit im Cyberspace?* wie ein letzter, trotziger Aufschrei aus dem letzten Jahrhundert. Die USA hätten durch ihre Sicherheitsapparate die absolute Vorherrschaft erlangt. Versuche, die sich daraus für die Bürger der Bundesrepublik ergebenden Probleme anzugehen, seien gescheitert. „Die widersprüchlichen Reaktionen speist eine symbolische Politik, die nationale Souveränität suggeriert, wo Hilflosigkeit herrscht", so Funk. „Die Versuche, mit einer nationalen Strategie die Informationssicherheit der Bundesbürger zu schützen – oder sei es auch nur die der Bundesregierung – münden in einer Sackgasse. Sie reduzieren in offenen Netzen, die keiner zentralen Kontrollinstanz unterworfen sind und global genutzt werden, die Informationssicherheit aller Nutzer."

Einen besonderen Aspekt der Überwachung, den Versuch, durch Data-Mining in großem Ausmaß und durch computergestützte Simulation das Verhalten komplexer sozialer Systeme vorherzusagen, behandelt der Beitrag von *Helge Peters*: *Biopolitische Si-*

Weltweiter Protest-Tag – The day we fight back
Photo Credit: alecperkins, CC BY

mulationen. Die dem Beitrag zugrundeliegende Arbeit wurde beim letztjährigen FIfF-Studienpreis ausgezeichnet. „Was also mit der Geste der Objektivität gleichsam der zu beherrschenden Natur zugeschlagen wird, verlässt den Raum demokratischer Willensbildung als Aushandlung differenter Interessen und Wissensbestände und wird stattdessen zur Domäne des technischen Managements unbestreitbarer Fakten", stellt er in seinem Beitrag fest. Dies stelle die Frage nach den Grenzen und den politischen Folgen des Objektivitätsanspruchs eines technowissenschaftlichen Zugriffs auf soziale Tatbestände.

Der zweite Abschnitt des Schwerpunkts setzt sich in mehreren Beiträgen mit der Videoüberwachung auseinander. Dieser Schwerpunkt wurde von *Peter Bittner* zusammengestellt, der in einem eigenen Schwerpunkteditorial in das Thema einführt. In fünf Beiträgen von ebenso vielen Autoren wird die Thematik umrissen – von Automatisierungs- und rechtlichen Fragen bis hin zur konkreten Situation der Videoüberwachung in der Großstadt Frankfurt am Main.

Der dritte Schwerpunkt, die *BigBrotherAwards*, wird durch einen Bericht von der diesjährigen Gala eingeleitet. Darauf folgen vier Laudationes: *Rolf Gössner* hielt die Laudatio auf das Bundeskanzleramt, das den BigBrotherAward in der Kategorie *Politik* für sein passives Verhalten in der Ausspähaffäre zugesprochen bekam. Den Preis in der Kategorie *Neusprech* gab es für den Begriff *Metadaten*, der die flächendeckende Überwachung verschleiert, den neuen Positivpreis *Julia-und-Winston-Award* erhielt *Edward Snowden*, auf den der Leiter des Innenressorts der Süddeutschen Zeitung, *Heribert Prantl*, eine engagierte Laudatio hielt, und die Laudatio von *Frank Rosengart* auf die Preisträger der Kategorie *Technik*, für die Spione im Auto.

Rubriken und aktuelle Beiträge ergänzen die Schwerpunkte. Eine neue Rubrik wird es ab dieser Ausgabe in Form einer Kolumne geben: *Betrifft: Cyberpeace* soll analog zu unserer bekannten Kolumne *Betrifft: Faire Computer* – die es natürlich auch dieses Mal gibt – aktuelle Entwicklungen der Cyberwarfare kommentieren.

Women in International Security (WIIS) ist eine Organisation, die Frauen in der Außen- und Sicherheitspolitik vernetzen und in Führungspositionen bringen will. Die Ziele dieser Organisa-

tion dürften in einigen Punkten von den Zielen des FIfF abweichen; dennoch ist es wichtig, dass auch wir uns mit den unterschiedlichen Aspekten der Sicherheitspolitik auseinandersetzen. Die Münchener Gruppe von WIIS, so *Dagmar Boedicker* in ihrem Beitrag, ist eine sehr heterogene Organisation mit einem vielfältigen Meinungsspektrum. Sie schlägt vor, in einen Meinungsaustausch einzutreten.

Die *Initiative Zivile Uni Bonn* lehnt die geplante *Henry-Kissinger-Professur* für Internationale Beziehungen und Völkerrechtsordnung an der Universität Bonn ab, das FIfF hat sich der Erklärung angeschlossen. Die Finanzierung dieses Lehrstuhls durch das Verteidigungsministerium lässt indirekte und direkte Einflussnahme befürchten; der Name *Henry Kissingers* ist angesichts der von ihm in den 60er- und 70er-Jahren betriebenen Außenpolitik für eine Professur für Völkerrecht untragbar.

Ein subjektiver Bericht über den Erstbesuch des *LinuxTages* von *Werner Hülsmann* und das *Log 2/2014* von *Sara Stadler* runden die Ausgabe ab. Passend zum Schwerpunkt hat *Dietrich Meyer-Ebrecht* den Band *Der NSA-Komplex* rezensiert.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Stefan Hügel
für die Redaktion

Brief an das FIfF

Boooom!

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

> *„Die 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 ist ungültig."*

So urteilte lapidar der Europäische Gerichtshof (EuGH) zur seit langem schwelenden Debatte um die anlasslose, verdachtsunabhängige Speicherung von Kommunikationsdaten sämtlicher Kommunikationsvorgänge.

Ein schwerer Schlag, so müsste man meinen, für die innenpolitischen Scharfmacher, die seit langem, ungeachtet juristischer und menschenrechtlicher Argumente – und ungeachtet des Urteils des Bundesverfassungsgerichts von 2010 –, die Forderung nach der Einführung der Vorratsdatenspeicherung ständig wiederholen. In der Tat lassen die Urteile die Möglichkeit offen, eine „verfassungskonforme" Vorratsdatenspeicherung einzuführen. Doch darf der Maßstab der Gesetzgebung immer das gerade noch verfassungsrechtlich Erlaubte sein? Gehört es nicht zu einem stabilen, lebendigen Rechtsstaat, dass ein freiheitlicher Geist die Gesetzgebung bestimmt?

„Wir werden die EU-Richtlinie über den Abruf und die Nutzung von Telekommunikationsverbindungsdaten umsetzen. Dadurch vermeiden wir die Verhängung von Zwangsgeldern durch den EuGH", so heißt es im Koalitionsvertrag der Regierungskoalition zwischen CDU/CSU und SPD. Dieser Grund fällt nun also weg. Aktuell scheint die Vorratsdatenspeicherung trotz massiver Forderungen vor allem von konservativer Seite auf Eis gelegt – warten wir ab, wann die Pläne wieder aus den Schubladen geholt werden.

Auch wenn Innenpolitiker die übelsten Folgen einer fehlenden Vorratsdatenspeicherung an die Wand malen – wobei sie es mit den Fakten nicht immer allzu genau nehmen –, den Nachweis eines Nutzens für die Strafverfolgung sind sie bisher schuldig geblieben. Und eins sollten wir festhalten: Sollen Grundrechtseingriffe einer solchen Tragweite wie bei der Vorratsdatenspeicherung vorgenommen werden, sind diejenigen in der Beweispflicht, die die verfassungsgemäßen Grundrechte einschränken, und nicht die, die sie verteidigen wollen.

Zu Recht können wir allerdings fragen, welche Rolle diese Debatte überhaupt noch im Gesamtkontext spielt. Seit nun gut einem Jahr wissen wir von der Ausspähung unserer gesamten Kommunikation durch Nachrichtendienste – verkürzend als *NSA-Skandal* bezeichnet – gegen die sich die Vorratsdatenspeicherung als harmlose Petitesse ausnimmt. Der NSA-Untersuchungsausschuss scheint sich durch kleinliches Hickhack um die Befragung Edward Snowdens selbst zu neutralisieren; die Bundesregierung hat bereits angekündigt, für die Untersuchung notwendige Unterlagen nicht freizugeben. Ausschussmitgliedern wird mit einem Gutachten gedroht, demzufolge sie sich möglicherweise allein durch die Mitgliedschaft im Untersuchungsausschuss strafbar gemacht haben sollen – ein beispielloser Versuch der Einschüchterung eines Verfassungsorgans.

Bemerkenswert dagegen die Gutachten dreier renommierter Verfassungsrechtler – darunter zwei ehemalige Verfassungsrichter – die nicht nur eine Schutzpflicht des Staates vor der Ausspähung betonen, bei deren Erfüllung er offenkundig versagt, sondern auch die Rechtmäßigkeit eines erheblichen Teils der Aktivitäten deutscher Nachrichtendienste in Zweifel ziehen.

Den Whistleblower Edward Snowden wird gleichzeitig durch eine Reihe bürgerrechtlicher Preise – unter anderen der *Whistleblower-Preis* von *IALANA*, der *Fritz-Bauer-Preis* der *Humanistischen Union*, der Positivpreis *Julia-und-Winston-Award* im Rahmen der *BigBrotherAwards* – die Solidarität der Zivilgesellschaft zuteil. Viele fordern, ihm in Deutschland Asyl zu gewähren. In seiner Laudatio zum Julia-und-Winston-Award stellt Heribert Prantl zur Diskussion um Snowdens Vernehmung im Untersuchungsausschuss fest: „*Der Mann habe doch schon alles gesagt, was er wisse, heißt es; man brauche ihn doch daher gar nicht mehr zu vernehmen. Das ist vorweggenommene Beweiswürdigung. Die ist im gesamten Recht verboten; im Deutschen Bundestag auch.*" Es fällt schwer, an einen echten Aufklärungswillen des Untersuchungsausschusses zu glauben.

Wir dürfen aber auch nicht in den Fehler verfallen, die Ereignisse um Edward Snowden als Agentenstory in James-Bond-Manier zu trivialisieren. Dem Vernehmen nach soll nun bereits ein Film über ihn gedreht werden, mehrere Bücher sind bereits auf dem Markt. Wichtig ist, dass er nach seinem zeitlich begrenzten Asyl in Russland einen stabilen Aufenthaltstitel in einem rechtstaatlichen Land erhält. Das darf aber nicht den Blick darauf verstellen, worum es eigentlich geht: Um die Ausspähung der Menschen in weltweitem Ausmaß und damit um den Bruch ihres Menschenrechts auf Privatheit – und um die Konsequenzen, die sich aus dieser Ausspähung ergeben. Es sei hier nur an die Nutzung der Daten für tödliche Drohnenangriffe erinnert – und an die potenzielle Kompromittierung der gesamten Informationsinfrastruktur.

Welche Gefährdungen daraus erwachsen können, zeigt vielleicht der *Heartbleed-Bug*, der in der Open-Source-Bibliothek *OpenSSL* gefunden wurde und den der Sicherheitsexperte Bruce Schneier als katastrophal bezeichnet hat. Presseberichte, nach denen dieser Fehler bei der NSA lange bekannt war und von ihr genutzt wurde, wurden umgehend dementiert. Wie auch immer – dieser Fall kann durchaus eine Blaupause für andere Fälle, auch in der Zukunft, sein, in der Risiken für die Allgemeinheit in Kauf genommen werden, um die Ausspähung zu betreiben und fortzusetzen.

Durch eine weitere Entscheidung hat der Europäische Gerichtshof in diesen Tagen das Recht der Internet-Nutzer auf Vergessenwerden gestärkt. Suchmaschinenbetreiber werden verpflichtet, personenbezogene Daten auf Wunsch aus dem Index zu entfernen. Das ist eine Stärkung der Verbraucherrechte – mit Nebenwirkungen. Denn damit können auch unliebsame Informationen verschwinden, die durchaus von öffentlichem Interesse sind. Wir müssen beobachten, wie sich diese Entscheidung langfristig auswirken wird.

Mit FIfFigen Grüßen

Stefan Hügel

bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken

FIfF-Jahrestagung 2014

Der Fall des Geheimen – Blick unter den eigenen Teppich

7. bis 9. November 2014 in Berlin (Mitte)

Wir wollen die Rolle Deutschlands und insbesondere der deutschen Geheimdienste im Kontext der neueren Erkenntnisse (Snowden, Foschepoth) bearbeiten.

Wie kommt es, dass Deutschland oft als *Datenschutzmekka* und *Demokratievorzeigestaat* bezeichnet wird, obwohl sich gerade hier einer der Dreh- und Angelpunkte von Folterflügen, Drohnenmordkoordination, Kriegslogistik und Infrastruktur für flächendeckende Überwachung innerhalb Europas zu befinden scheint.

Inwiefern ist die Rolle Deutschlands keine widerwillig helfende, ja fast opferhafte, sondern ganz im Gegenteil eine rege, aktive, tragende Säule des sich immer weiter offenbarenden antidemokratischen Zustands der Welt? Dabei mutet es fast schon als eine Plattitüde an, wenn gesagt wird, dass dieser Zustand auf das Werk einer Techniker-Gemeinde zurückführbar ist – aber wie sind diese Systeme gebaut und nach welchen normativen Weltauffassungen wurden sie konzipiert?

Dazu wollen wir das Thema in drei Dimensionen beleuchten:

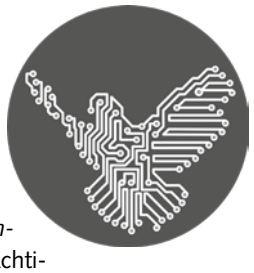
1. mit historischem Blick auf die deutschen Geheimdienste und ihre technisch-organisatorische Entwicklung,

2. mit aktuellen Analysen der gegenwärtigen Lage der Geheimdienste, ihres technischen Apparats und ihrer rechtlichen Einhegung; gerade die Verflechtungen zwischen den Geheimdiensten, Telkos und der Techniker-Gemeinde bedürfen einer besonderen Aufmerksamkeit;

3. mit Erfahrungsberichten direkt Betroffener oder gar Erzählungen von Whistleblowern (wenn wir welche kriegen).

Kurzum: Vor allem den selten beleuchteten technischen Aspekten soll in der Debatte um die deutschen Geheimdienste Rechnung getragen werden, aber für ein Verständnis der Lage ist natürlich mehr nötig, daher wollen wir auch Vortragende aus anderen Bereichen einladen und uns dabei von Verschwörungstheorien abgrenzen.

Dietrich Meyer-Ebrecht, Hans-Jörg Kreowski, Stefan Hügel



Betrifft: Cyberpeace

Der NSA-Skandal hat uns für die Kompromittierbarkeit unserer Privatsphäre sensibilisiert, nicht jedoch für die militärische Dimension der Ausspähung. Der umfassende Missbrauch der Informatik und Informationstechnologie für den *Cyberwarfare*, die Kernkomponente der heute maßgebenden Kriegsführungsdoktrin, wird kaum wahrgenommen. Die Methoden beginnen mit Ausspähung und Spionage und reichen von Informationsmanipulation über Sabotage und Destabilisierung lebenswichtiger Infrastrukturen bis hin zu vernetzten kriegerischen Operationen. Der Kreis schließt sich, wenn die Ausspähung des Mobilfunks dazu dient, Ziele für völkerrechtswidrige Drohnenoperationen zu ermitteln. Weltweit wird derzeit mit *Cyberwaffen* aufgerüstet. Die Gefahren für den inneren und äußeren Frieden, für die Zivilgesellschaft und für jeden Einzelnen sind unabsehbar. Sie werden jedoch von Öffentlichkeit, Politik und Wirtschaft ignoriert oder verschwiegen. Die Zivilgesellschaft muss wieder zum politischen Handeln mobilisiert werden: gegen Ausspähung der Privatsphäre, zum informationellen Selbstschutz, zur Einforderung sicherer und unkompromittierbarer IT-Produkte und -Infrastrukturen. Sie soll die Achtung der Menschenrechte im virtuellen Raum einfordern und ihr Schutzbedürfnis durch die Politik artikulieren.

Nahezu alle Lebensbereiche unserer Zivilgesellschaft sind von digitaler Informationstechnologie tief durchwoben. Dies setzt uns neuen Risiken und Gefahren aus. Steht der Komfort, den Internet, Mobiltelefonie, Informationsdienste im Alltag bieten, oder der wirtschaftliche Nutzen, den eine Vernetzung von Produktions-, Logistik- und Verwaltungsprozessen ermöglicht, zur Disposition, schauen wir lieber nicht so genau auf Risiken. Das Wegsehen wird erleichtert durch die abstrakte Natur der Informations- und Kommunikationsprozesse, und es wird unterstützt durch absichtsvolles Ignorieren und Verschweigen realer Gefahren. Zwar hat der NSA-Skandal den virtuellen Raum als ein Ausspähinstrument bisher nicht gekannten Ausmaßes enttarnt, zeigt damit aber nur die Spitze des Eisbergs: Der virtuelle Raum ist zentral für die aktuellen militärischen Szenarien – als Ort für die Spionagetätigkeit der Geheimdienste und Militärs und als Operationsraum für Cyberwaffen. Auch Industriespionage hat im Hinblick auf die technologische Hochrüstung militärstrategische Bedeutung. Gängige Cyberwarfare-Szenarien reichen von Destabilisierung durch Meinungsmanipulation über Sabotage bis zu Tod und Zerstörung verursachenden Eingriffen in digitale Infrastrukturen. Dass diese hoch geheim gehaltenen Operationen gleichsam in den zivilen Informationsströmen mitschwimmen, stellt ein Fundamentalrisiko für die Zivilgesellschaft dar. Die Öffnung des virtuellen Raums für Cyberwarfare setzt die Aushebelung von Grundrechten wie auch von IT-Sicherheitsfunktionen zwingend voraus. Schon heute bedroht dies nicht nur unsere informationelle Privatsphäre. Es setzt die Zivilgesellschaft und uns Einzelne unkalkulierbaren Risiken aus – toleriert von Politik und Wirtschaft. In seiner Unfassbarkeit und Unkontrollierbarkeit stellt Cyberwarfare eine verschwiegene, aber höchst reale latente Gefahr für den Frieden dar.

Neben dem *Cyberwarfare* „im eigentlichen Sinne", d. h. die Ausspähung, die Kompromittierung und Zerstörung von IT-Infrastrukturen mit programmiertechnischen Mitteln, nimmt der *Cyberwarfare* durch *Kampfroboter* – autonom oder ferngesteuert – konkrete Form an. Heute vor allem in Form von ferngesteuerten *Drohnen*, durch die die gezielte Tötung Terrorverdächtiger und weiterer Opfer, die sogenannten *Kollateralschäden*, zur alltäglichen Form der Kriegführung geworden ist. Zynisch mutet da die bis heute nicht umgesetzte Ankündigung des US-Präsidenten Barack Obama an, das Gefangenenlager in Guantánamo zu schließen – heute werden keine Gefangenen mehr gemacht. Es fällt unter diesen Gesichtspunkten schwer, daran zu glauben, dass wir wirklich noch in einer Wertegemeinschaft leben – auch und gerade angesichts der nicht geringen Akzeptanz für solche Angriffe in der Bevölkerung – übrigens auch hierzulande.

Ohnehin steht Deutschland offenbar im Mittelpunkt (nicht nur) der drohnengestützten Kampfführung. Wie zahlreiche Publikationen berichten, ist der US-Stützpunkt *Ramstein* in Rheinland-Pfalz zum Zentrum des drohnengesteuerten Todes geworden. „Ohne diese Basis in Deutschland würde das alles nicht funktionieren", so der ehemalige Drohnenpilot der US-Luftwaffe *Brandon Bryant*, der aus Gewissensgründen den Dienst quittierte, nachdem er offenbar an 1.626 gezielten Tötungen beteiligt war. Vielleicht werden wir seinen Namen einmal in einem Atemzug mit den Namen von *Edward Snowden* und *Chelsea Manning* nennen müssen.

„Von deutschem Boden soll nie wieder Krieg ausgehen", so lautete die Maxime nach den Millionen Toten zweier Weltkriege. Doch beim *Krieg gegen den Terror* kann man offenbar auf solche hehren Ideale keine Rücksicht mehr nehmen. Aber die Bundesregierung hat – wie so häufig – „keine Erkenntnisse" über die Beteiligung deutscher US-Stützpunkte am Drohnenkrieg. Es mutet merkwürdig an, dass man ein Land wie die Bundesrepublik regieren kann, wenn man in so vielen Fällen keine Erkenntnisse von wesentlichen Vorkommnissen auf deutschem Boden hat. Gleichzeitig soll auch die Bundeswehr mit Drohnen ausgerüstet werden – dies scheiterte bei der Drohne *Eurohawk* zunächst noch an Fehlleistungen bei der Beschaffung.

Doch die ferngesteuerten Drohnen sind nur eine Form der Kampfroboter – die nächste Stufe ist erreicht, wenn autonome Roboter menschliche Mitwirkung beim Töten überflüssig machen. Im Rahmen der 78. Jahrestagung der Deutschen Physikalischen Gesellschaft an der Humboldt-Universität zu Berlin hat die Arbeitsgruppe *Physik und Abrüstung* (AGA) vom 19. bis 21. März 2014 dazu einen Workshop veranstaltet. Hans-Jörg Kreowski hatte die Ehre und das seltene Vergnügen, eingeladen worden zu sein mit einem Vortrag über *Entwicklung autonomer Roboter – Stand der Technik, Perspektiven und das besondere Problem der Kampfroboter*. Der Veranstaltungsort war das Hauptgebäude, von dem mit einer gewissen Ehrfurcht gesagt wurde, dass dort auch schon Einstein und Heisenberg gelehrt haben. Sein Vortrag war mit rund 250 Zuhörerinnen und Zuhörern überraschend gut besucht. Die hohe Zahl hat allerdings eine plausible Erklärung: Die WE-Heraeus-Stiftung hat die Tagung unterstützt, indem sie die Tagungskosten von einer großen Zahl junger Physikerinnen und Physiker – insbesondere Studierender – bezuschusst hat, so dass trotz vieler paralleler Veranstaltungen die Räume nicht leer

blieben. Solch eine Stiftung wäre für die Informatik auch nicht schlecht. Neben dem Vortrag gab es in diesem Workshop noch über 20 weitere Präsentationen, die sich überwiegend mit Fragen der nuklearen Abrüstung und ihrer Verifikation sowie einer Reihe weiterer Waffensysteme beschäftigt haben, wobei es meist um Wirkungsweise, Proliferation und Verifikation ging. Besonders interessant waren Ausführungen von Tatsujiro Suzuki über *Nuclear Energy Policy Issues after the 3.11 Fukushima Nuclear Accident* und von Rob Goldston über *Fusion Energy and Nuclear Non-Proliferation*. Direkt auf autonome Kampfroboter war auch der Vortrag von Jürgen Altmann bezogen, der die Frage des Verbots solcher Waffensysteme diskutiert hat.

Am Donnerstagvormittag hat die AGA zusammen mit dem *Forschungsverbund Naturwissenschaften, Abrüstung und internationale Sicherheit* (FONAS) parallel zum Workshop noch ein Fachgespräch organisiert – es war bereits das 22. – zum Thema *Autonome Waffensysteme – Trends, Gefahren und vorbeugende Begrenzungen*. Durch die knapp 30 Teilnehmenden waren das Auswärtige Amt und das Verteidigungsministerium, einige Büros von Mitgliedern des Bundestages sowie einige Stiftungen, Vereine und Kampagnen wie Friedrich-Ebert-Stiftung, Rosa-Luxemburg-Stiftung, Stiftung Wissenschaft und Politik, Hessische Stiftung Friedens- und Konfliktforschung, Facing Finances, International Committee for Robot Arms Control (ICRAC), Deutsche Sektion der internationale Ärzte für die Verhütung des Atomkriegs (IPPNW) und urgewald e. V. vertreten. In dieser illustren Runde haben Jürgen Altmann und Hans-Jörg Kreowski ihre Vorträge verkürzt und politisch etwas zugespitzt wiederholt. Außerdem hat Thomas Göbel aus dem Referat 241 *Konventionelle Rüstungskontrolle* des Auswärtigen Amts den Stand der Diskussion über autonome Waffensysteme im internationalen Bereich erläutert, und Thomas Küchenmeister von *Facing Finance* hat die internationale *Campaign to Stop Killer Robots* vorgestellt.

Als Quintessenz wäre festzuhalten, dass es auch im Rahmen der Gesellschaft für Informatik überlegenswert wäre, eine Arbeitsgruppe *Informatik und Rüstung* zu schaffen, und ein regelmäßiges Fachgespräch zu Informatik und Rüstung mit Vertreterinnen und Vertretern aus Politik und Gesellschaft wäre eine feine Sache.

Für die, die noch mehr über den Vortrag erfahren möchten, folgt eine Kurzfassung und ein Link auf die Vortragsfolien:

> *Seit einigen Jahren wird mit erheblichem Aufwand an der Entwicklung autonomer Roboter (und anderer autonomer Systeme) gearbeitet, wobei mit Autonomie gemeint ist, dass spezifische Aufgaben in einer sich ändernden und nicht vollständig bekannten Umgebung selbstständig und ohne Fremdsteuerung erledigt werden. Solche Roboter müssen so programmiert werden, dass sie ihre Umgebung erfassen und interpretieren und entscheiden können, welche Aktivitäten unter den jeweils gegebenen Umständen am ehesten zum Ziel führen. Trotz erheblicher Fortschritte sind noch eine Reihe technischer Hindernisse zu überwinden, da weder für die Umgebungsinterpretation noch für die Entscheidungsfindung zufriedenstellende Lösungen existieren. Eine Hauptschwierigkeit liegt darin, dass bekannte Lösungen nicht exakt genug sind oder zu viel Zeit brauchen. Bei autonomen Kampfrobotern kommen noch ethische Probleme hinzu. Sie müssen das Kriegsvölkerrecht einhalten, wofür aber völlig unklar ist, ob und wie sich ein solches Verhalten programmieren lässt.*
> *(http://www.informatik.uni-bremen.de/theorie/aga2014/AGA190314.pdf)*

Der Cyberwar als Ausspähung, Kompromittierung oder Zerstörung von Infrastrukturen mit programmiertechnischen Mitteln, Kampfroboter und Drohnen – ob autonom oder ferngesteuert –, all dies steckt den Rahmen ab, den wir künftig mit unserer neuen Kolumne *Betrifft: Cyberpeace* füllen wollen. Wechselnde Autorinnen und Autoren werden über Entwicklungen berichten und sie kommentieren, die aktuellen Bezug haben, aber über den Tag hinausweisen. Durch die Kommentierung der Entwicklungen wollen wir einen kleinen Beitrag dazu leisten, dass *Cyberpeace* statt *Cyberwar* Realität werden kann.

Initiative Zivile Uni Bonn

Erklärung zur geplanten Henry-Kissinger-Professur in Bonn

Die Initiative *Zivile Uni Bonn* lehnt die geplante *Henry-Kissinger-Professur für Internationale Beziehungen und Völkerrechtsordnung* an der Universität Bonn ab. Henry Kissinger war als Nationaler Sicherheitsberater (1969 – 1975) und Außenminister (1973 – 1977) maßgeblich für die Außenpolitik der Vereinigten Staaten verantwortlich. Bei den von Kissinger geplanten und überwachten Bombardements in Vietnam, Kambodscha und Laos starben Hunderttausende Menschen, die ökologischen Folgen des massiven Bomben- und Gifteinsatzes führen bis heute zu Fehlbildungen bei Neugeborenen. Während des von ihm nachdrücklich unterstützten Putsches 1973 in Chile gegen eine demokratisch gewählte Regierung wurden 3000 Menschen ermordet und Tausende gefoltert oder ins Exil getrieben. Kissinger befürwortete den „Schmutzigen Krieg" in Argentinien, während dem 30.000 Menschen spurlos verschwanden. Kissinger gab der indonesischen Führung sein Einverständnis im Namen der USA für einen Angriffskrieg gegen Osttimor, der mindestens 100.000 Timoresen das Leben kostete (bei einer Gesamtbevölkerung von 800.000).

Initiative Zivile Uni Bonn

Nach dem Statut des Internationalen Strafgerichtshofs könnten einige seiner Handlungen als Kriegsverbrechen und Verbrechen gegen die Menschlichkeit angesehen werden.

Henry Kissinger äußerte sich einmal zu seinem Verhältnis zum Recht in den internationalen Beziehungen:

„The illegal we do immediately. The unconstitutional takes a little longer."
(„Das Illegale machen wir sofort. Das Verfassungswidrige dauert etwas länger.")

Der Name Henry Kissingers für eine Professur für Völkerrecht ist untragbar.

Die überwiegende Finanzierung des geplanten Kissinger-Lehrstuhls durch das Verteidigungsministerium lässt direkte und indirekte Einflussnahme befürchten und gefährdet die universitäre Autonomie. Wir sprechen uns klar dagegen aus, dass Lehrstühle durch das Bundesministerium der Verteidigung oder die Bundeswehr finanziert werden. Forschung, Lehre und Studium an der Universität sollen zivilen und friedlichen Zwecken dienen. Wir fordern eine ausreichende Grundfinanzierung der Universitäten, um sie als Institutionen zu stärken und in die Lage zu versetzen, Angebote abzulehnen, welche nicht mit ihrer gesellschaftlichen Verantwortung in Einklang stehen.

Initiatoren: Lukas Mengelkamp; Carlos Echegoyen; Albert Flock; René El Saman; Marvin Mendyka; Konrad Hentze; Daniela Kulla

Unterzeichner: *AStA der Universität Bonn; Komitee für Grundrechte und Demokratie e.V.; ila – Informationsstelle Lateinamerika e.V.; ver.di-Bezirk NRW-Süd; Deutsche Friedensgesellschaft – Vereinigte KriegsdienstgegnerInnen (DFG-VK) e.V., Gruppe Bonn-Rhein-Sieg; Lateinamerika Nachrichten e.V.; SprecherInnenkreis der Evangelischen Studierendengemeinde Bonn; Bonner Friedensbündnis; Matthew Robson, Former Minister for Disarmament and Arms Control, New Zealand; European Center for Constitutional and Human Rights e.V. (ECCHR); Forschungs- und Dokumentationszentrum Chile-Lateinamerika e.V. (FDCL); Stiftung Asienhaus, Köln; Bundesausschuss Friedensratschlag; Bonner Friedensbündnis; Philippinenbüro e.V, Köln; AG Friedensforschung, Kassel; Forschungs- und Dokumentationszentrum Chile-Lateinamerika e.V. (FDCL); Informationsstelle Militarisierung e.V. (IMI); IPPNW e.V. – Internationale Ärzte und Ärztinnen für die Verhütung des Atomkriegs, Ärzte in sozialer Verantwortung, deutsche Sektion; Bundesvorstand der Vereinigung Demokrati- sche Juristinnen und Juristen e.V.; INKOTA-netzwerk e.V.; Frauennetzwerk für Frieden e.V.; Solidaritätsdienst International e.V. (SODI); Bonner Jugendbewegung (BJB); Netzwerk Friedenskooperative; AK Zivilklausel Köln; Bund demokratischer Wissenschaftlerinnen und Wissenschafler – BdWi; Aachener Friedenspreis e.V.; AK Zivilklausel Konstanz; AStA der Universität Paderborn; AStA der Hochschule Darmstadt; AK Zivilklausel der Uni Frankfurt/M; FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.; Förderkreis Oscar Romero Haus Bonn e.V.; Barbara Lochbihler, MEP; Raja Bernard, Mitglied des Senats der Universität Bonn; Prof. Dr. Michael Klundt, Hochschule Magdeburg-Stendal; Bernhard „Felix" von Grünberg, MdL (NRW); Christel Müller, Mitglied des Personalrates der Universität Bonn; Prof. Dr. Klaus Meschkat, Hannover; Rolf Beu, MdL (NRW); Renate Koppe, Mitglied des Personalrates der Universität Bonn; Horst Lüdtke, Geschäftsführer GEW Bonn; Andrej Hunko, MdB; Ingeborg Breines, Co- President International Peace Bureau; Rainer Braun, Geschäftsführer IALANA; Prof. Dr. Andreas Buro, Frankfurt; Prof. Ph.D. Lawrence Wittner, New York; Hein van der Kroon, President of Museum for Peace and Non Violence NL; Prof. Dr. Christof Butterwegge, Köln; Prof. Ph.D. Kazuyo Yamane, Kyoto; Colin Archer, Secretary-General International Peace Bureau, Switzerland; Dr. Peter van den Dungen, Peace Studies, University of Bradford, UK; Dr. Susanne Jalka, Wien; Bruce Kent, Vice President Movement for the Abolition of War, UK; Prof. Dr. Günter Giesenfeld, Marburg; Jakob Horneber, Senator der Universität Bonn; Dr. Antonio Sáez-Arance, Iberische und Lateinamerikanische Abteilung, Historisches Institut, Universität zu Köln*

und ca. 1.600 weitere individuelle Unterzeichner. Der Auftruf kann unter *http://www.zivile-uni-bonn.de* mitgezeichnet werden (Stand: 2. Mai 2014).

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in Faire Fußbälle.

Die vermutlich wichtigste Entwicklung gleich zu Beginn: In China gibt es viel Bewegung in der Arbeiterschaft. Ein ungewöhnlich großer und langer Streik betraf zwar die Weltturnschuhproduktion, aber auch bei der IT-Industrie gab es mehrtägige Proteste, im vergangenen Quartal bei einem von Lenovo aufgekauften IBM-Werk und einem Samsung-Zulieferer. Die junge Generation der Wanderarbeiter lässt sich nicht mehr alles gefallen. Die Hunde bellen, die Karawane zieht weiter: Dass Samsung in Vietnam Fabriken aufbaut, berichteten wir schon in der vorherigen Kolumne. Foxconn nun, der aus Taiwan stammende größte IT-Fertiger der Welt mit Werken vor allem in China, investiert in Indonesien.

Foxconns Hauptkunde Apple punktet auf sichererem Terrain: Greenpeace hat Apple gelobt für die vollständige Umstellung ihrer Cloud auf erneuerbare Energien. Für seine Strategie musste sich Chef Cook sogar gegen Investoren wehren: „If you want me to do things only for ROI reasons, you should get out of this stock." Was an Green-IT allerdings so absurd ist: Man kümmert sich vor allem um den Stromverbrauch beim Betrieb der Geräte, dabei kann man im Gebrauch gar nicht mehr so viel einsparen um all das auszugleichen, was man beim Bau schon verbraucht hat.

Das ist bei Fair-IT anders: Nichtkaufen ist nicht die Lösung, und der Herstellungsprozess steht im Fokus. Dass giftige Chemikalien nicht nur in den Kopfhörern, Computermäusen und ähnlichem stecken, wie die c't jüngst aufdeckte, sondern auch beim Herstellungsprozess die Gesundheit der Arbeiterinnen und Arbeiter gefährdet ist, wurde im März durch den beeindruckenden Kurzfilm *Who Pays the Price? The Human Cost of Electronics* in Erinnerung gerufen.

Zumindest in Südkorea gibt es speziell zu den bekannten Krebsfällen in der Halbleiterherstellung bei Samsung gleich zwei Neuerscheinungen im Kino, den Spielfilm *Another Promise* und die Dokumentation *The Empire of Shame*. Ob die Filme in Europa zu sehen sein werden, ist unklar, englische Untertitelung soll es aber geben. Die Fälle sind in Südkorea Teil der Innenpolitik geworden. Samsung hat sich nun entschuldigt und Zahlungen angekündigt, lehnt einen Zusammenhang mit den Arbeitsbedingungen aber weiterhin ab. Komisch auch, dass es ihnen nicht einmal eine Pressemeldung Wert war.

Dem oben genannten Kurzfilm soll im Laufe des Jahres ebenfalls eine Langversion folgen. Er hat eine neue US-basierte Kampagne *Bad Apple* (so nannte sich übrigens schon 2006 eine Initiative gegen iPod-Elektroschrott) inspiriert, die den Einsatz von Benzol und n-Hexan in der Produktion der iPhones u. a. kritisiert, zudem größere Transparenz, die Übernahme von Behandlungskosten und ungefährlichere Substitute fordert. Diese einzusetzen würde vermutlich nur 1$ pro Gerät kosten. Apple tut es trotzdem nicht, da braucht es wohl auch keinen Investorendruck. Interessant ist die Begründung, warum gerade Apple als Kampagnenziel gewählt wurde: Apple sei *leader in corporate social responsibility*, eben wegen oben genannter klimafreundlicher Strategie und auch wegen des Versprechens, keine Konfliktmineralien mehr einsetzen zu wollen. Letzteres hatten sie allerdings schon 2011 in ihrem Zuliefererbericht versprochen.

Womit wir beim zweiten großen Thema des vergangenen Quartals wären. Ein US-Gericht hat nun aufgrund einer Klage von Industrieverbänden gesprochen: Eine Firma darf nicht gezwungen werden, öffentlich bekannt zu machen, dass sie möglicherweise Konfliktrohstoffe in ihren Produkten hat. Die Folgen sind unklar. Berichte über die Sorgfalt im Einkauf von Konfliktrohstoffen wird es trotzdem geben, vielleicht werden sie aber nicht mehr vollständig öffentlich sein.

Ein solches Gerichtsurteil kann der EU nicht passieren, bei der es neben neuen öko-fairen Vergaberichtlinien und Regelungen zur Offenlegung nicht-finanzieller Informationen von Firmen inzwischen auch einen Kommissionsentwurf für die Kontrolle des Handels mit bestimmten Rohstoffen (wie in den USA lediglich Tantal, Zinn, Wolfram und Gold) aus Konfliktgebieten (anders als in den USA nicht nur D.R. Kongo) gibt. Allerdings sollen das die Firmen (gemeint sind nur Schmelzhütten, nicht alle Hersteller wie in den USA) freiwillig machen dürfen, ja, sie sollen sich sogar freiwillig selbst zertifizieren dürfen, also öffentlich darlegen, wie sie dafür gesorgt haben, dass beim Einkauf keine bewaffnete Partei Geld verdient hat. Ob sie das wohl machen werden? Eine große Gruppe von NGOs, der auch das FIfF angehört, zeigte sich ob der Freiwilligkeit enttäuscht. Das Öko-Institut sieht in seiner Kritik des Entwurfs zu wenig Anreize, es zu tun, befürchtet zudem, dass wie in den USA einfach nicht mehr in kritischen Gebieten eingekauft wird, und somit der Bevölkerung eine Einnahmequelle genommen wird, statt aktiv verantwortungsvollen Bergbau zu fördern.

Das zu verhindern, ist bekanntermaßen die Absicht von Fairphone, die andeuteten, 2015 in ihrem nächsten Modell fair gehandeltes Gold einzusetzen. Zunächst aber wird im Sommer eine neue Charge des schon vorhandenen, gar nicht so fairen, Modells neu aufgelegt. Nager-IT gibt derweil ihr Wissen über faire Beschaffung von Bauteilen an andere Firmengründer und an Bastler weiter. Eine Art *Fair-Maker-Szene* ist im Entstehen.

Es ist wichtig, sich den einzelnen Elektro-Komponenten zuzuwenden, also nicht nur den Lebensumständen in den Rohstoffminen oder den Arbeitsbedingungen beim Zusammenbau der Geräte, sondern auch, wie die Teile hergestellt werden. An dieser Stelle kann man im Einzelnen das faire vom nicht-so-fairen trennen.

Sebastian Jekutsch ist aktiv im *AK Faire Computer* des FIfF und *AK Faire Elektronik* in Hamburg. Wer sich für die Quellen der Nachrichten oder das Thema überhaupt interessiert sollte Kontakt aufnehmen über fairit@fiff.de.

Dagmar Boedicker

Women in International Security?

... nie gehört ...

Sollte frau aber!
WIIS hat weltweit 7000 (natürlich vorwiegend weibliche) Mitglieder in 47 Ländern, allein in Deutschland sind es schon fast 300. 2013 hat die deutsche Gruppe ihr zehnjähriges Jubiläum gefeiert, und wenn das nicht jede/r bemerkt hat, gibt es dafür einen ziemlich einfachen Grund.

Vorbilder? Fehlanzeige

Die Außen- und Sicherheitspolitik ist in Deutschland nicht eben eine Frauendomäne. Frau von der Leyen war eine höchst überraschende Wahl, *Vorzeigedamen* wie Madeleine Albright oder Hillary Clinton in den USA fehlen bei uns. Deshalb hat sich WIIS e. V. zum Ziel gesetzt, Frauen zu vernetzen, und will sie in Führungspositionen sehen, auch in Forschung und Wissenschaft. Das erzählt mir Carina Schmidt, Doktorandin in Sicherheitspolitik an der Universität der Bundeswehr, seit zwei Jahren bei WIIS und Regionalgruppenleiterin der Münchner Gruppe. Sie findet, dass Frauen auch auf diesem Politikfeld entsprechend ihrem Anteil in der Gesellschaft vertreten sein sollten. Der Verein will dazu beitragen, dass sie auf dem Wege des Austauschs und der Vernetzung selbstbewusster und sichtbarer werden und mehr Einfluss gewinnen.

Das scheint recht gut zu gelingen, immerhin trifft sich die Münchner Gruppe regelmäßig an einem Donnerstag im Monat *After Work,* es gibt ein Frauenfrühstück von WIIS auf der Sicherheitskonferenz, und die größte Gruppe, die Berlinerinnen, veranstaltet Hintergrundgespräche und Coachings zu Karriereplanung, Rhetorik und Verhandlungsgeschick. Öffentliche Veranstaltungen planen auch die Münchnerinnen. Sie sind offen für Kooperationen, beispielsweise zum Thema *Cyber-Security.* Dafür gibt es unter den Münchner Mitgliedern nur wenige Spezialistinnen, obwohl ihnen die Bedeutung schon vor einiger Zeit deutlich geworden ist. Vielleicht ein Anlass für das FIfF zum Meinungsaustausch? Bei WIIS gibt es nicht nur Politikwissenschaftlerinnen. Die Gruppe ist sehr heterogen, das Spektrum der Meinungen vielfältig.

Themen

Es geht den Frauen bei WIIS um internationale Beziehungen, Ziele und Konzepte deutscher Außenpolitik, die europäische Sicherheits- und Verteidigungspolitik, Nachbarschaftspolitik, den Nahen Osten und den arabischen Frühling, um potenzielle Konfliktfelder und Politik im Cyberspace. (Immerhin hat das Auswärtige Amt mittlerweile einen Cyber-Beauftragten, natürlich einen Mann.) Zum Thema Cyberpeace findet auch Carina Schmidt, dass es den Akteuren weniger um Verteidigung als um Gegenangriff zu gehen scheint, nicht eben ein gutes Omen für ein friedliches Miteinander. Wäre das nicht eine gute Gelegenheit für eine gemeinsame Veranstaltung von WIIS und FIfF in München?

Mehr steht unter:

WIIS USA *http://wiisglobal.org/wordpress1/*
WIIS Deutschland *http://www.wiis.de/wir-sind-wiisde*

Kontakt

Wer in München Lust auf ein WIIS-Treffen *After Work* oder allgemeinen Gedankenaustausch hat, sollte sich bei Carina Schmidt melden: *Schmidtcarina@gmx.de*.

Sie ist eine von drei Regionalgruppenleiterinnen der Münchner Gruppe von Women in International Security e. V., hat in München Politische Wissenschaften, Ethnologie und Recht für Sozialwissenschaftler an der Ludwig-Maximilians-Universität studiert und ist derzeit Doktorandin am Lehrstuhl für Internationale Beziehungen der Universität der Bundeswehr München.

Kai Nothdurft

„Wir sind Ihre Bank, wir müssen wissen welcher Religion Sie angehören!“

Neulich bekam ich von meiner Bank einen Brief, in dem mir Änderungen an den Geschäftsbedingungen mitgeteilt wurden. Bei einem Punkt wurde ich stutzig und las genauer nach: automatischer Einbehalt der Kirchensteuer.

In dem Schreiben teilte mir meine Bank mit, dass ab dem *„1. Januar 2015 alle Banken verpflichtet sind, die Kirchensteuer auf abgeltend besteuerte Kapitalerträge ihrer Kunden automatisch einzubehalten und an die steuererhebenden Religionsgemeinschaften abzuführen.“*[1] Bei der Abfrage würde der Bank die entsprechende Kirche mitgeteilt, an die die Steuern abzuführen sind bzw. eine Information, dass man keiner der steuererhebenden Religionsgemeinschaften angehöre.

In den Erläuterungen wurde dann noch darauf hingewiesen, dass es möglich sei, dem Datenabruf zu widersprechen (Stichwort *Sperrvermerk*). Dieser Widerspruch[2] müsse beim Bundeszentralamt für Steuern bis spätestens 30. Juni 2014 eingehen. Der Sperrvermerk würde ab dann für alle anfragenden Kirchensteuerabzugsverpflichteten (Banken, Versicherungen, Bausparkassen, Fondgesellschaften) bis auf Widerruf gelten.

Tatsächlich hat der Gesetzgeber im Dezember 2013 das Steuerrecht im §51a EStG entsprechend geändert.[3] Mit dieser Änderung erhalten alle Finanzinstitute, bei denen ich Kunde bin und potenziell Kapitalerträge erziele, die Informationen über meine Religionszugehörigkeit, ein Datum, das nicht ohne Grund im Datenschutzrecht als besonders sensibel und schützenswert gilt. Zwar ist zur Zeit der religiöse Fanatismus in Deutschland nicht besonders stark ausgeprägt, aber das könnte sich in Zukunft auch ändern. Noch brisanter ist, dass die Information auch an Institute mit Hauptsitz im Ausland gehen dürfte. In Irland hat z. B. die Information, ob man katholisch oder protestantisch ist, eine ganz andere Bedeutung.

Bisher sind Diskussionen oder Informationen zu diesem Sachverhalt an mir vorbeigegangen. Ich verfolge auch nicht jede Änderung im Steuerrecht zeitnah mit.

Umso mehr ärgert mich, dass hier wieder einmal das Grundrecht auf informationelle Selbstbestimmung in einer Weise eingeschränkt wird, dass ich aktiv widersprechen muss, um eine Datenweitergabe zu unterbinden. Dies ist umso problematischer, weil der Widerspruch zeitlich lange vor der Weitergabe erfolgen muss und es neben einer Regelabfrage auch noch anlassbezogene Abfragen geben kann, für die andere Termine gelten.

Eine ähnlich unbefriedigende Situation gilt für den Widerspruch zur Herausgabe von Meldedaten etwa an Werbetreibende.

Datenschutzrechtlich müsste grundsätzlich der umgekehrte Weg vorgesehen sein oder bei entsprechenden Gesetzesänderungen wenigsten ergebnisoffen gefragt werden, ob man der Datenübermittlung zustimmt oder nicht.

Es wird immer schwieriger, sein Grundrecht auf informationelle Selbstbestimmung wahrzunehmen. Dieses Grundrecht ist aber zu wichtig, um die Ausgestaltung Bürokraten und einer Exekutive zu überlassen, die den Datenschutz immer noch eher als Arbeitsbehinderung denn als wichtigen Bestandteil unserer Demokratie betrachten.

Anmerkungen

1 *Bayerisches Landesamt für Steuern, Informationen vom 10.12.2013 unter www.iww.de/sl381; Beitreibungsrichtlinie-Umsetzungsgesetz, BGBl I 2011, S. 2592; Amtshilferichtlinie-Umsetzungsgesetz, BGBl I 2013, S. 1809*

2 *Formular unter https://www.formulare-bfinv.de/ffw/form/display.do?%24context=B8F8ED768AD9BC2EFC22*

3 *http://www.gesetze-im-internet.de/bundesrecht/estg/gesamt.pdf. http://www.gesetze-im-internet.de/estg/__51a.html*

Sara Stadler

Log 2/2014

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

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

Januar 2014

29. Januar 2014: Der bayerische Innenminister Joachim Herrmann (CSU) stellt die Cyber-Sicherheitsstrategie für Bayern vor. Demnach soll die Truppe der „Cybercops“ in diesem Jahr auf 50 verdoppelt und ein *Cyber-Kompetenzzentrum* zur Vernetzung der verschiedenen Cyber-Dienststellen im Land eingerichtet werden (Quelle: Heise).

31. Januar 2014: Wie der Fernsehsender *CBC* berichtet, habe der kanadische Geheimdienst CSEC Flugreisende, die das WLAN eines kanadischen Flughafens nutzten, lokalisiert und über zwei Wochen verfolgt. Bei der Maßnahme soll es sich lediglich um einen Testlauf für eine neue Überwachungssoftware gehandelt haben (Quelle: Heise).

31. Januar 2014: Das *Technology Review* berichtet über die 2011 aufgestellte Bundeswehr-Einheit *CNO – Computer-Netzwerk-Operationen –*, in deren Rahmen aktuell rund 60 SoldatInnen für gezielte Angriffe auf Drohnen ausgebildet würden. Künftig solle die CNO um eine vor Ort agierende mobile Einsatztruppe aufgestockt werden (Quelle: Technology Review, Heise).

Februar 2014

6. Februar 2014: Die New Yorker Polizei will die Datenbrille *Google Glass* im Streifendienst testen (Quelle: Heise).

10. Februar 2014: Wie *Netzpolitik.org* unter Berufung auf das *Bundeswehr Journal* berichtet, verfügt die Bundeswehr über eine neue mobile Abhörplattform, die derzeit in der Eifel getestet wird. Bislang wurde das *Mobile Geschützte Fernmeldeaufklärungssystem* (MoGeFA), das Kommunikationsdaten in allen „einsatzrelevanten Frequenzbereichen" mitschneiden kann, auf drei Fahrzeugen montiert. Die Bundesbeauftragte für Datenschutz, Andrea Voßhoff, will prüfen, ob im Rahmen der Erprobung auch zivile Handytelefonate mitgeschnitten wurden (Quelle: Netzpolitik.org, Heise).

10. Februar 2014: Wie die *Washington Post* berichtet, wurden in den USA und Mexiko verschiedene Städte auf Veranlassung der Behörden hin aus der Luft überwacht. Mit dem Überwachungssystem *Hawkeye II* der Firma *Persistent Surveillance Systems* werden durch an Flugzeugen montierte Kameras im Sekundenabstand hochauflösende Bilder geschossen, auf denen sich Bewegungen von Fahrzeugen und Personen erkennen lassen (Quelle: Washington Post, Heise).

10. Februar 2014: Das neue Online-Magazin *The Intercept* berichtet, dass sich die US-Geheimdienste bei der Auswahl ihrer Ziele für Drohnenangriffe im Rahmen der sogenannten „*Find, Fix & Finish*"-Missionen auf die Auswertung von Metadaten und die Handy-Ortung verlassen haben. Obwohl Handys leicht ihre BesitzerInnen wechseln können, werde die Identität der Zielperson vor der Tötungsmission nicht weiter geprüft. Der linke Bundestagsabgeordnete Andre Hunko wirft daraufhin die Frage auf, ob auch deutsche Dienste solche Metadaten, wie Telefonnummern, weitergegeben haben, und inwiefern Technik deutscher Hersteller im Rahmen der Missionen zum Einsatz gekommen sei (Quelle: The Intercept, Heise).

18. Februar 2014: Neu veröffentlichte Dokumente zeigen Details zur Repression gegen *Wikileaks*. Wie *The Intercept* unter Berufung auf Dokumente aus dem Fundus Edward Snowdens berichtet, hat der britische GCHQ Tracking-Tools installiert, um BesucherInnen von Internetseiten mit Verbindung zu Wikileaks zurückverfolgen. Aus weiteren Dokumenten gehe hervor, dass die NSA die Enthüllungsplattform zum „feindlichen Akteur" habe erklären wollen und ihr Gründer, *Julian Assange*, von den USA als Zielperson in einer sogenannten „Manhunting Timeline" erfasst worden sei (Quelle: The Intercept, Heise).

19. Februar 2014: Der türkische Staatspräsident *Abdullah Gül* bestätigt ein umstrittenes Gesetz zur Internetüberwachung, dem zufolge Behörden künftig Internetseiten auch ohne richterlichen Beschluss sperren dürfen. Weiter werden Internetanbieter mit dem Gesetz zur zweijährigen Speicherung von NutzerInnendaten verpflichtet (Quelle: Heise).

24. Februar 2014: Die Bundespolizei nimmt nach eigenen Angaben das automatische Grenzkontrollsystem *EasyPASS* an den Flughäfen München und Frankfurt am Main in Betrieb. Bei der biometriegestützten Grenzkontrolle wird das Bild auf dem von den Reisenden auf das Lesegerät gelegten elektronischen Reisepässen bzw. Personalausweisen mit einem zeitgleich angefertigten Kamerabild verglichen. Zudem erfolgt eine Fahndungsabfrage im *Schengener Informationssystem (SIS)* und die überwachenden Beamten werden informiert, sofern das Gerät eine besondere Prüfung der Reisenden für erforderlich hält (Quelle: Heise, Bundespolizei).

24. Februar 2014: Der US-Fernsehsender *NBC* und das Online-Magazin *The Intercept* berichten unter Berufung aus Dokumente aus dem Fundus *Edward Snowdens*, dass die Geheimdienste im Internet nicht nur mitlesen würden, sondern gezielt manipulierte Daten hochlüden, um Einzelpersonen oder Unternehmen zu diskreditieren (Quelle: The Intercept, Heise).

24. Februar 2014: Wie *heise online* berichtet, bemüht sich die EU-Kommission, die von DatenschützerInnen und Menschenrechtsorganisationen scharf kritisierte Gesetzesinitiative zu „intelligenten Grenzkontrollen" schnellstmöglich auf den Weg zu bringen. So sei, ohne dass das Paket bereits durch das EU-Parlament oder den Ministerrat verabschiedet worden ist, bereits eine kostenintensive Machbarkeitsstudie in Auftrag gegeben worden. Geprüft werden solle dabei auch der „technische Aspekt des Zugangs von Strafverfolgern" zu den im Rahmen des geplante Ein- und Ausreisesystems auf Vorrat gespeicherten Daten und Fingerabdrücken (Quelle: Heise).

25. Februar 2014: Im Internet werden Mitschnitte von Telefonaten veröffentlicht, die der türkische Ministerpräsidenten *Erdoğan* geführt habe und die diesen der Korruption überführen sollen. In der Folge lässt Erdoğan erst Twitter und schließlich auch Youtube sperren. Türkische Gerichte beurteilen die Sperren als eine illegale Einschränkung der Meinungsfreiheit (Quelle: Süddeutsche Zeitung, Heise).

27. Februar 2014: Wie der *Guardian* unter Berufung auf Dokumente aus dem Fundus *Edward Snowdens* berichtet, hat der britische Geheimdienst *GCHQ* in großem Umfang Webcam-Aufnahmen aus *Yahoo*-Videochats abgegriffen und gespeichert. Im Rahmen des Überwachungsprogramms *Optic Nerve*, das mindestens bis 2012 gelaufen sei, seien etwa 2008 Aufnahmen von 1,8 Millionen Yahoo-NutzerInnen gesammelt worden, denen dafür nicht einmal ein Fehlverhalten vorgeworfen werden musste. Gespeichert worden seien nicht komplette Chats sondern alle 5 Minuten aufgenommene Bilder. Die gespeicherten Bilder seien anschließend auf der Suche nach Zielpersonen oder neuen Überwachungszielen beispielsweise mit Methoden der Gesichtserkennung oder anhand von Metadaten durchforstet worden (Quelle: The Guardian, Heise).

28. Februar 2014: Wie *Netzpolitik.org* berichtet, speichert die Berliner Polizei seit 2004 personenbezogene Daten von AnmelderInnen politischer Veranstaltungen und Personen des öffentlichen Lebens, die an diesen teilnehmen, für 3 Jahre in einer

„Stadtweiten Veranstaltungsdatenbank". Die Ausgestaltung der Datenbank war durch eine Anfrage nach dem Informationsfreiheitsgesetz (IFG) öffentlich geworden. Demnach diene sie unter anderem der „Planung von Einsatzkräften" und der „Gefährdungsbewertung zukünftiger Veranstaltungen" und enthalte neben den personenbezogenen Daten auch verschiedene Informationen, die Verfassungsorgane, Vertretungen der Länder beim Bund, Bundesministerien, die Bundespolizei und das BKA sowie Parteien und Stiftungen liefern würden. Zugriff auf die gespeicherten Daten erhielten „Mitarbeiter aller Polizeidienststellen, wenn und soweit die Kenntnis der Daten zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist" (Quelle: Netzpolitik.org).

März 2014

6. März 2014: Auch US-Abgeordnete seien, wie unter anderem die *New York Times* berichtet, durch die CIA überwacht worden, die sich Zugang zu den Senatscomputern verschafft habe. Anlass sei der Umstand gewesen, dass ein Geheimausschuss des Senats ein Gutachten über Folter und Misshandlung von Terrorverdächtigen in Geheimgefängnissen in der Amtszeit von Präsident *Busch* erarbeitet habe, welches die CIA schwer belaste (Quelle: New York Times, Heise).

12. März 2014: *The Intercep*t veröffentlicht auf der Basis von Dokumenten aus dem Fundus *Edward Snowdens* neue Details zu bereits bekannten Überwachungsprogrammen, aus denen hervorgeht, dass die NSA daran arbeite, Spyware-Angriffe auf Rechner und Netzwerke automatisiert auszudehnen. So sei etwas das Programm *Turbine* so konzipiert, dass es seine Angriffe autonom ausweiten und so zukünftig Millionen Netzwerke angreifen könne. Ziel der Überwachung seien nicht nur „Terrorverdächtige" und „Extremisten" sondern auch SystemadministratorInnen von Telefonanbietern und Internet Service Providern (ISP) sowie Virtual Private Networks (VPN). Auf diesem Wege könnten Kommunikationsdaten von Zielpersonen besonders effizient abgegriffen werden. Zum Verbreiten der Malware würden unter anderem gefälschte Seiten von *LinkedIn* und *Facebook* genutzt (Quelle: The Intercept, Heise).

12. März 2014: Anlässlich einer entsprechenden Kleinen Anfrage der Linksfraktion im Bundestag berichtet *Heise online* über die Beteiligung der Bundesrepublik an EU-Projekten zur „proaktiven Verbrechensbekämpfung". Das Projekt *Proactive* will terroristische Anschläge mittels der massenhaften Datensammlung über Sensoren verhindern. *Carper* will organisierte Kriminalität mittels der Auswertung im Internet verfügbarer Daten (z. B. aus sozialen Netzwerken) bekämpfen (Quelle: Heise, Deutscher Bundestag Drucksache 18/707).

18. März 2014: Wie die *Washington Post* unter Berufung unter anderem auf *Snowden*-Dokumente berichtet, überwacht die NSA im Rahmen eines Programms namens *Mystic* die Telefongespräche eines ganzen Landes. Die abgegriffenen Gesprächsinhalte würden für mindestens 30 Tage gespeichert und mittels eines Computerprogramms namens *Retro* durchsucht. Um welches Land es sich handele, sei nicht bekannt, es gebe aber Anhaltspunkte, dass zukünftig oder bereits aktuell mindestens fünf weitere Länder von einer derart umfangreichen Überwachung betroffen seien (Quelle: Washington Post, Heise).

21. März 2014: Im Kontext interner Ermittlungen gegen einen Mitarbeiter, der Teile des Betriebssystems Windows 8 an einen Blogger weitergegeben haben soll, hat *Microsoft* die privaten Emails jenes Bloggers beim konzerneigenen Dienst *Hotmail* durchsucht. Der Konzern beruft sich dabei auf seine Nutzungsbedingungen, die den Zugang zu KundInnendaten erlaubten (Quelle: Heise).

23. März 2014: Wie *Spiegel online* berichtet, hat ein Berliner Anwalt beim Bundesverwaltungsgericht Klage gegen den *Bundesnachrichtendienst (BND)* eingereicht. Die Klage richtet sich gegen die massenhafte Durchleuchtung von Emails durch den Geheimdienst, die das parlamentarische Kontrollgremium in seinen Jahresbericht öffentlich gemacht hatte. Das Filtern von rund 37 Millionen Emails nach Schlagwörtern wie *Bombe* oder *Atom* bezeichnet der Kläger als unverhältnismäßig und damit rechtswidrig (Quelle: Der Spiegel).

24. März 2014: *Heise online* analysiert in einem Beitrag die Nutzungsbedingungen von *Apple*, *Google* und *Yahoo* und stellt heraus, dass auch diese Dienste es sich vorbehalten, auf die Inhalte von KundInnenkonten zuzugreifen (Quelle: Heise).

April 2014

1. April 2014: Medienberichten zufolge handelt es sich bei dem Land, dessen Telefongespräche im Rahmen des jüngst enthüllten *Project Mystic* vollständig überwacht worden sei, um den Irak (Quelle: Heise).

2. April 2014: Der Geheimdienstdirektor *James Clapper* bestätigt öffentlich, dass im Rahmen der Massenüberwachung in den USA auch Daten von US-BürgerInnen, die eigentlich rechtlich besser geschützt werden als Menschen ohne US-amerikanische Staatsbürgerschaft, gesammelt und durchsucht worden seien. Da die Datensammlung legal erfolge, gelte dies auch für deren Auswertung und zwar auch dann, wenn versehentlich Daten von einer Person gesammelt worden seien, die nicht hätte überwacht werden dürfen (Quelle: Heise).

3. April 2014: Wie die *Süddeutsche Zeitung* berichtet, lassen gemeinsame Recherchen mit dem *NDR* und dem *WDR* auf eine zentrale Rolle der *Ramstein Air Base* im US-Drohnenkrieg schließen. So seien den vorliegenden Quellen zufolge nicht nur Drohneneinsätze in Afrika, sondern auch solche im Jemen und in Pakistan, wo seit 2004 etwa 1000 ZivilistInnen bei Drohnen-

Sara Stadler

Sara Stadler studiert Informatik an der Hochschule Bremen und arbeitet in der FIfF-Geschäftsstelle.

einsätzen getötet worden seien, von dem Militärflugplatz aus gesteuert worden (Quelle: Süddeutsche Zeitung).

7. April 2014: Nach dem Rücktritt *Brendan Eichs* bekundet der *Mozilla*-Konzern seine Unterstützung für den rechts-konservativen Ex-CEO. Das *Board of Directors* hätte Eich, der wenige Tage zuvor aufgrund der massiven Kritik an seiner Unterstützung für einen Gesetzesentwurf zum Verbot gleichgeschlechtlicher Ehen zurückgetreten war, gerne auf einem anderen Posten behalten (Quelle: Heise).

7. April 2014: Mit dem wenige Wochen zuvor bekannt gewordenen Überwachungsprogramm *Mystic* sei, wie die österreichische Wochenzeitung *Format* berichtet, sehr wahrscheinlich auch die Kommunikation in Österreich vollständig überwacht worden. Den der Zeitung vorliegenden Quellen zufolge sei der komplette Datenverkehr des Landes mit dem Wissen des österreichischen Innenministeriums mitgeschnitten und mindestens 30 Tage lang gespeichert worden (Quelle: Format).

11. April 2014: Entgegen einer entsprechenden Klage durch Berliner Abgeordnete der Grünen, Linken und Piraten entscheidet der Verfassungsgerichtshof des Landes Berlin, dass die Berliner Polizei Demonstrationen und andere Protestaktionen unter freiem Himmel weiterhin videoüberwachen darf (Quelle: Heise).

16. April 2014: Wenige Tage nachdem der *Spiegel* berichtet hatte, dass sich die Große Koalition gegen eine Neuauflage der Vorratsdatenspeicherung ausgesprochen habe, fordern die Gewerkschaft der Polizei und verschiedene SicherheitspolitikerInnen aus den Reihen der CDU/CSU erneut deren Einführung (Quelle: Der Spiegel, Rheinische Post, Mitteldeutsche Zeitung).

22. April 2014: Im Dienste der „Terrorismusbekämpfung" verabschiedet das russische Parlament ein Gesetzespaket, das unter anderem eine Zunahme der Internet-Kontrolle vorsieht. So werden etwa Internet-Dienstleister verpflichtet, Kommunikationsdaten ihrer KundInnen für sechs Monate zu speichern. BloggerInnen sowie NutzerInnen von Twitter und sozialen Netzwerken, die mehr als 3000 BesucherInnen pro Tag oder mehr als 3000 FollowerInnen haben, müssen sich bei der Presseaufsicht registrieren lassen und dürfen keine „extremistischen oder persönlichkeitsverletzenden Beiträge" veröffentlichen. Verstöße können zu Geldstrafen von umgerechnet bis zu 10.000 Euro führen (Quelle: Heise).

24. April 2014: Wie das *Wall Street Journal* berichtet, hat die US-Regulierungsbehörde FCC eine neue Version der *Open-Internet-Regeln* aufgelegt, die es ermöglichen sollen, dass sich Webdienste eine bevorzugte Behandlung durch die Provider erkaufen können (Quelle: Wall Street Journal, Heise).

27. April 2014: Die norwegische Zeitung *Dagbladet* berichtet unter Berufung auf *Snowden*-Dokumente, dass der norwegische Militärgeheimdienst *Etteretningstjenesten* in Absprache mit der *NSA* einen Supercomputer mit immensem Rechenvolumen gekauft habe, für den gemeinsame Anwendungen entwickelt werden sollen. Helfen soll der Computer nicht nur beim Speichern und Auswerten massenhaft abgegriffener Kommunikationsdaten, sondern auch beim Dechiffrieren verschlüsselter Inhalte (Quelle: Heise).

28. April 2014: Wie die *New York Times* unter Berufung auf nicht namentlich genannte MitarbeiterInnen der US-Regierung berichtet, hat die USA in verschiedenen Staaten, darunter Kuba und Afghanistan, *Twitter*-ähnliche Netzwerke zur Beeinflussung der öffentlichen Meinung finanziert (Quelle: New York Times, Heise).

Werner Hülsmann

Ein Besuch auf dem LinuxTag 2014

Ein subjektiver Bericht über einen „Erstbesuch"

Zugegeben: Ich bin kein Linux-Freak, auch kein Nerd, sondern jemand, der PCs, Smartphones und andere EDV nicht um ihrer selbst Willen benutzt, sondern als Werkzeuge gebraucht. Von daher gehöre ich vermutlich nicht zum harten Kern *der Zielgruppe des LinuxTags[1], der vom 8. bis 10. Mai 2014 in Berlin stattfand.*

Der erste Eindruck: Zumindest der Einlass ist etwas chaotisch. Die Registrierungsschalter der *re:publica*[2] und der *droidcon*[3] sind da deutlich besser organisiert. Die re:publica ist allerdings an diesem Tag klar im Vorteil: Es ist der letzte Tag der Veranstaltung, die meisten BesucherInnen haben sich schon registriert und müssen beim Einlass nur noch ihr Bändchen vorzeigen. Der zweite Eindruck: Lebhaftes Treiben auf dem Innenhof, angenehme, zum Entspannen und Austauschen einladende Atmosphäre. Der neue Veranstaltungsort, die *Station Berlin*[4], ist eine gute Wahl: Ein alter Postbahnhof, der zu einem interessanten und eindrucksvollen Veranstaltungsort umgebaut wurde. Der dritte Eindruck: Auch das in den gesalzenen Eintrittspreisen für den LinuxTag – 109 € für das Tagesticket, 150 € für alle drei Tage – enthaltene Catering ist etwas chaotisch. Kurz nach offiziellem Beginn der Mittagspause gab es nur noch ein Gericht. Das war dafür vegetarisch und sehr lecker. Frisch gestärkt wage ich mich an die Ausstellung – oder besser gesagt, die Ausstellungen – heran. Alle BesucherInnen des LinuxTages und der droidcon können an den drei Veranstaltungstagen auch die Ausstellung und Vorträge der anderen Veranstaltung besuchen. Am Donnerstag ist auch ein Austausch zwischen re:publica, LinuxTag und droidcon möglich und erwünscht.

Die Ausstellungsflächen von LinuxTag und droidcon sind sehr überschaubar. Nicht jeder Aussteller ist wirklich mit oder zumindest an einem Stand vertreten. So gibt es den einen oder anderen Sponsor, der die ihm zugeteilte Ausstellungsfläche nur mit einem Banner schmückt. Einige VertreterInnen von Projekten, die auch Vorträge halten, reisten erst am Donnerstag an, so auch – wie ich leider feststellen musste – die beiden Vertreter des Projekts *Ubuntu Privacy Remix*[5], das Projekt, das mich am meis-

ten interessierte. Bis zur Kaffeepause, deren Catering genauso chaotisch verlief wie die Mittagspause, hatte ich einen ziemlich guten Überblick über Ausstellungen von LinuxTag, droidcon und auch der re:publica.

Da die mich besonders interessierende Session erst um 18:30 Uhr beginnt, verlasse ich erstmal das Veranstaltungsgelände um später wieder zu kommen. Wer sich nur für die Abendsessions interessiert, ist – zumindest was die Kosten angeht – fein heraus. Der Eintritt zu diesen Abendsessions ist auch ohne LinuxTag-Ticket frei. Dafür ist um diese Zeit die überwiegende Zahl der Ausstellungsstände nicht mehr besetzt. Dem meist ehrenamtlich tätigen *Personal* sei dies aber verziehen.

Die ersten drei Veranstaltungen der Session *Sicherheit für Praktiker*[6], zwei Vorträge und eine Art Podiumsdiskussion waren für mich, der ich mich schon über 30 Jahre mit Datenschutz, IT-Sicherheit und den gesellschaftlichen Auswirkungen der Informatik beschäftige, nicht so interessant. Von daher wäre die parallel laufende *BuddyNight* eine echte Alternative gewesen. Die *BuddyNight* von LinuxTag und droidcon wurde gemeinsam mit der Abschlussparty der re:publica auf dem Außengelände und in weiteren Räumlichkeiten veranstaltet. Zwei kleine Bonmots zu den Vorträgen: Der erste Referent, der sein Zielpublikum wohl etwas falsch eingeschätzt hatte, hatte bei seiner Präsentation Startschwierigeiten. Ob es daran lag, dass sich seine Präsentation zum Thema *Systemsicherheit* auf einem Windowsrechner befand? Auch der Referent von der *Free Software Foundation Europe* nutzte einen Rechner mit Windows 8, um seinen Vortrag zu präsentieren, was ja irgendwie weder zum LinuxTag noch zur Organisation passt. Mein Höhepunkt des Abends war aber der Vortrag[7] über das Projekt *Ubuntu Privacy Remix (UPR)*.

Ubuntu Privacy Remix: *Radikaler Ansatz gegen Bespitzelung durch NSA, Verfassungsschutz & Co.*

Dieser „radikale Ansatz" ist von der Idee her zwar nicht neu, aber sehr eindrucksvoll in der Umsetzung. Der Ansatz – nämlich die vollständige Trennung der sensiblen Datenverarbeitung von der Verbindung zu anderen Netzen – wird zumindest in Einzelfällen schon von JournalistInnen, RechtsanwältInnen und ÄrztInnen genutzt. Dabei werden meist zwei PCs eingesetzt. Der vom Netz abgeschottete PC dient dann zur Verarbeitung der sensiblen Daten. Die Texte für E-Mails werden bereits auf dem abgeschotteten PC verschlüsselt und dann z. B. über einen USB-Stick – auf dem sich dann nur noch verschlüsselte Daten befinden sollten – auf den vernetzten PC übertragen. Dort können dann die verschlüsselten E-Mails versandt und auch empfangen werden. Weder die Schlüssel noch andere sensible Daten befinden sich auf dem vernetzten PC. Das Projekt UPR setzt nun bei diesem abgeschotteten PC an und hat sich die Aufgabe gestellt, diesen PC – es kann selbstverständlich auch ein Laptop oder Notebook sein – mit einem möglichst sicheren System zu betreiben und zumindest technische Angriffsmöglichkeiten so gering wie möglich zu halten. Hier seien nur einige der Designansätze genannt:

- Das Livesystem bootet von einer CD oder einem USB-Stick und ist in einem *Read-Only*-Dateisystem abgelegt.
- Der Kernel ist so „kastriert", dass weder die lokalen Festplatten noch irgendwelche Netzwerkkomponenten genutzt werden können.
- Die sensiblen Daten werden in einem *Truecrypt-Volume* auf einem Wechseldatenträger (externe Festplatte, USB-Stick) sicher gespeichert. Derartige Volumes und Wechseldatenträger werden mit der Option *no-exec*, eingehängt, etwaige dort gespeicherte Schadprogramme sind also nicht ausführbar.
- Daten, die das System verlassen sollen, werden bereits auf diesem System mit GnuPG mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.

Diese Maßnahmen führen dazu, dass dieselbe Hardware als abgeschottetes oder vernetztes System genutzt werden kann und es nur darauf ankommt, von welchem Medium gebootet wird. Alles in allem ist dies ein sehr vielversprechender Ansatz, der mit entsprechenden Anpassungen und Erweiterungen – z. B. Einbindung eines Datenbankprogramms – auch in anderen Projekten genutzt werden kann. So stelle ich mir vor, dass ein auf UPR basierendes System mit den erforderlichen Anpassungen z. B. von Menschenrechtsgruppen genutzt werden kann, um die meist sehr sensiblen Daten von den Betroffenen auf eine sichere Art und Weise zu verarbeiten.

Der zweite Tag

Für ein konkretes Projekt, bei dem Beratungsstellen mit sehr sensiblen Daten der Betroffenen arbeiten, erscheint mir das Livesystem UPR eine sehr gute Basis zu sein. Zufällig hatte ich am Freitagmittag eine Besprechung mit VertreterInnen dieses Projekts, in dem es um die technische Umsetzung der sichere Speicherung hochsensibler Daten von Betroffenen geht. Mit den neuen Fragen, die sich in dieser Besprechung stellten, besuchte ich nochmals den LinuxTag, um mit den beiden Vertretern des UPR-Projektes diese Fragen zu erörtern.

Als ich zur Station Berlin kam, war deutlich zu bemerken, dass der Hauptanteil der Verköstigungsstände nur wegen der re:publica dagewesen ist. Mit diesen Ständen waren aber auch

Werner Hülsmann

Werner Hülsmann, Dipl. Inform., selbstständiger Datenschutzberater und Datenschutzsachverständiger, externer Datenschutzbeauftragter, Konstanz, Ismaning (bei München), Berlin, Beiratsmitglied des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V.

die verschiedenen Sitzgelegenheiten im Innenhof verschwunden, die zuvor noch zum Austausch und zur Entspannung eingeladen hatten. Im Innenbereich von LinuxTag und droidcon gab es hierzu aber noch genug Möglichkeiten, sich unabhängig von Standbesuchen und Vorträgen. Das Klischee, dass „der Computerfreak" an sich sowieso lieber ein Dach über und einen Bildschirm vor dem Kopf habe, wurde hier einmal mehr bestätigt. Einige der professionellen Ausstellungsstände waren auch nicht mehr besetzt. Das tat aber meinen konstruktiven und interessanten Gesprächen mit den beiden Vertretern des Projekts UPR und am *LibreOffice*-Stand keinen Abruch.

Fazit

Mein persönliches Fazit: Auch wenn ich nur an bestimmten Vorträgen Interesse hatte, fand ich meine Besuche beim LinuxTag sehr lohnenswert. Ob ich nächstes Jahr wieder komme, hängt allerdings ganz davon ab, zu welcher Zeit welche Vorträge stattfinden. Aber wer weiß, vielleicht entwickelt sich das oben erwähnte Projekt der Beratungsstellen so, dass ich nächstes Jahr einen kleinen Vortrag aus der Praxis anbieten kann. Zumindest werde ich in einer der nächsten FIfF-Kommunikationen näher über das Projekt berichten.

Anmerkungen

1 *http://www.linuxtag.org/2014/*
2 *http://re-publica.de/*
3 *http://de.droidcon.com/2014/*
4 *http://www.station-berlin.de/*
5 *https://www.privacy-cd.org/*
6 *http://www.linuxtag.org/2014/de/programm/donnerstag/sicherheit-fuer-praktiker/*
7 *http://www.linuxtag.org/2014/de/programm/vortragsdetails/?eventid=1154*

W&F Wissenschaft und Frieden 2/2014 – Gewalt(tät)ige Entwicklung

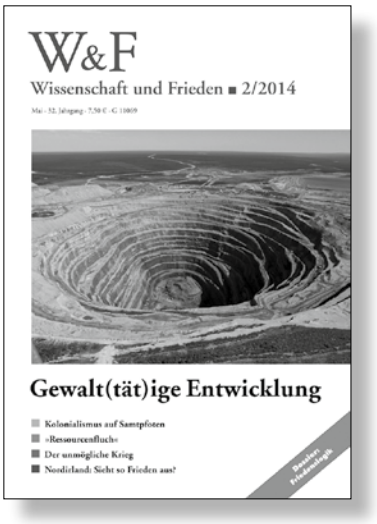
Vor 44 Jahren – im Oktober 1970 – beschloss die UN-Vollversammlung, „ein besseres und effektiveres System der internationalen Zusammenarbeit anzustreben, um die bestehenden Ungleichheiten in der Welt zu beseitigen und Wohlstand für alle zu gewährleisten". Dafür sollten die „entwickelten Länder" jährlich 0,7 Prozent ihres Bruttosozialprodukts als Entwicklungshilfe leisten. Ein Prozentsatz, von dem die große Mehrheit der Industrieländer auch heute noch meilenweit entfernt ist. Hinzu kommt, die geleistete „Entwicklungshilfe" ist weitgehend an Bedingungen gebunden, die die ungleichen Machtverhältnisse perpetuieren oder durch vorgeblich faire Regeln neu schaffen; sie fördern Armut, Ungleichheit und Konfliktdynamiken mit fatalen Folgen für die Zivilbevölkerung.

Mit dieser *Gewalt(tät)igen Entwicklung* befassen sich die Artikel im Schwerpunkt der Mai-Ausgabe von *Wissenschaft & Frieden*:

Guido Speckmann: *Kolonialismus auf Samtpfoten – die Handelspolitik der EU*, Matthias Basedau: *Konflikte durch Rohstoffausbeutung*, Lucas Renz: *Entwicklungspolitik und Rohstoffsicherung*, Peter Wahl: *IWF und Weltbank in der multipolaren Welt*, Vijay Prashad: *Die BRICS-Staaten – Neoliberalismus mit südlichem Antlitz*, Conrad Schetter: *Entwicklung und Intervention*, Norman Paech: *Der Internationale Strafgerichtshof – Schatten des Neokolonialismus*, Michael Brzoska: *Neoliberale Rüstungsexportpolitik*, Harry Grünberg: *Die radikale Antwort – Süd-Süd-Kooperation durch ALBA*.

Die übrigen Artikel des Heftes reichen von der *„Mechanik" des Ersten Weltkriegs* über *Nordirland – sieht so Frieden aus?* bis zu einer kritischen Sicht auf die jüngste *friedensethische Bilanz der EKD zum Afghanistan-Krieg*. Das W&F beiliegende Dossier befasst sich mit *Friedenslogik statt Sicherheitslogik – Theoretische Grundlagen und friedenspolitische Realisierung*.

Die *Versicherheitlichung* der internationalen und nationalen Politik wurde in den letzten Jahren zur allgemeinen Handlungsmaxime, woraus konkrete Konzepte für die *vernetzte Sicherheit* entstanden. Dies führte dazu, dass international tätige zivilgesellschaftliche Organisationen sich verstärkt mit der Anschlussfähigkeit an bzw. der Abgrenzung von sicherheitspolitischen Konzeptionen auseinandersetzten.



Die *Plattform Zivile Konfliktbearbeitung* setzt der *Sicherheitslogik* eine *Friedenslogik* gegenüber. Das Dossier nimmt die theoretische Fundierung und Gegenüberstellung der beiden *Logiken* vor und befragt die Praxis der eigenen, sehr unterschiedlichen Arbeitsfelder daraufhin.

Wissenschaft & Frieden, 2/2014: **Gewalt(tät)ige Entwicklung**, € 7,50 plus Porto.

W&F erscheint vierteljährlich. Jahresabo 30€, ermäßigt 20€, Ausland 35€, ermäßigt 25€, Förderabo 60€. Seit 2013 erscheint W&F auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5€ jährlich – als elektronisches Abo ohne Printausgabe 20€ jährlich.

Bezug: W&F, Beringstr. 14, 53115 Bonn, E-Mail: *buero-bonn@wissenschaft-und-frieden.de*, *www.wissenschaft-und-frieden.de*

Werner Koep-Kerstin und Stefan Hügel

Forderungen zur Ausspähaffäre

Am 6. Juni 2014 jährten sich die Enthüllungen, die einen beispiellosen weltweiten Überwachungsskandal offenlegten, zum ersten Mal. In der Folge wurden immer weitere Details der Überwachung – durch die US-amerikanische NSA, das britische GCHQ und weitere, auch deutsche Geheimdienste – bekannt.

Auch wenn die Öffentlichkeit erst durch die Enthüllungen Edward Snowdens alarmiert wurde – eigentlich ist diese Ausspähung nichts Neues. Bereits zuvor gab es öffentliche Debatten über Überwachung der Bevölkerung; sie verebbten freilich zumeist schnell wieder. Im Sog der aktuellen Enthüllungen fand auch eine bereits 2012 erschienene Studie größere Beachtung, in der der Freiburger Historiker Professor Dr. Josef Foschepoth die Überwachung der westdeutschen Bevölkerung seit dem zweiten Weltkrieg dokumentiert hatte, basierend auf umfangreichen Dokumenten, die ihm durch deutsche Behörden zur Verfügung gestellt worden waren.

Die Debatte, die seither geführt wird, hat das Bewusstsein in Öffentlichkeit und Wirtschaft deutlich geschärft. Obwohl sie aber nunmehr seit gut einem Jahr anhält, sind seitens der Politik wenig Konsequenzen zu erkennen. Erst die Ausspähung des Mobiltelefons der Bundekanzlerin führte zu Empörung und mittlerweile zu einem Ermittlungsverfahren – offensichtlich motiviert auch auf dieser Ebene erst persönliche Betroffenheit zu politischem Handeln.

Doch was soll nun geschehen? Im folgenden Text erheben wir eine Reihe von Forderungen, wie jetzt mit der Ausspähaffäre umgegangen werden muss.

Politische Forderungen

Aufklärung des Spähskandals und Information der Bevölkerung

In schneller Folge werden wir derzeit mit immer neuen Enthüllungen über die nachrichtendienstliche Überwachungspraxis versorgt. Mit großer Sorge verfolgt die deutsche Bevölkerung die Diskussionen über die Überwachung, die in erster Linie durch Edward Snowden, aber beispielsweise auch durch die wissenschaftlichen Erkenntnisse von Professor Dr. Josef Foschepoth an die Öffentlichkeit gekommen sind. Hier fehlt es an der Aufklärung durch die beteiligten Behörden und Organisationen. Auch der NSA-Untersuchungsausschuss droht zur Farce zu werden: Nicht nur tagte er in seinen ersten Sitzungen, bei denen über die zu ladenden Zeugen verhandelt wurde, geheim, was den durch ihn erreichten Transparenzgewinn sehr in Frage stellt. Auch die offenbar mangelnde Kooperationsbereitschaft der Bundesregierung und offene Drohungen, wie mit der Strafbarkeit der Mitarbeit im Ausschuss durch ein US-amerikanisches Rechtsgutachten, gefährden seine erfolgreiche Aufklärung des Skandals.

Der Skandal muss eingehend untersucht und die Öffentlichkeit umfassend über die Überwachung und die bis heute ergriffenen Maßnahmen dagegen aufgeklärt werden. Wenn sich dabei herausstellt, dass bei Überwachungsmaßnahmen gegen gesetzliche Bestimmungen verstoßen worden ist, sind die daran Beteiligten zur Verantwortung zu ziehen.

Verbesserung der öffentlichen Kontrollrechte

Die bisherige Kontrolle der Geheimdienste hat sich als ineffektiv erwiesen, wie auch die Aufarbeitung der Vorgänge um den *Nationalsozialistischen Untergrund* (NSU) bereits gezeigt hat. Da das parlamentarische Kontrollgremium – Aussagen von (ehemaligen) Mitgliedern zufolge – immer erst aktiv wird, wenn Vorwürfe bereits in den Medien präsent sind, deckt es keine Skandale und Fehlleistungen der zu kontrollierenden Behörden auf. Damit gewährleistet es keine effektive Kontrolle. Die strafrechtlich bewehrte Geheimhaltungspflicht hindert die Mitglieder der parlamentarischen Kontrollgremien darüber hinaus in weitem Maße, die Regierung öffentlich zu kritisieren (§10 II, III PKGrG).

Auch die gerichtliche Kontrolle und die Kontrolle durch Aufsichtsbehörden weisen schwere Mängel auf. Beispielsweise ist die Datenschutzaufsicht für Maßnahmen der Bundesbehörden nach dem G10-Gesetz ausgeschlossen, entscheiden Verfassungsschutzämter und Bundesnachrichtendienst (BND) selbst, welche Akten sie Gerichten vorlegen, und Auslandsüberwachungsmaßnahmen des BND unterliegen keiner Kontrolle.

Die Beschränkungen sollten modifiziert werden und beispielsweise bereits ein Minderheitenquorum Mitglieder der parlamentarischen Kontrollgremien zu öffentlichen Stellungnahmen berechtigen. Die Kontrollgremien sind personell und technisch erheblich besser auszustatten, ihre Mitglieder müssen effektive Arbeitsmöglichkeiten erhalten; Angehörige der Nachrichtendienste müssen sich an die Gremien wenden können. Die Mitglieder der Kontrollgremien sollten außerdem von ihrer Schweigepflicht

im Falle von Verstößen gegen das Grundgesetz, die Strafgesetze oder gegen von Deutschland abgeschlossene völkerrechtliche Abkommen kraft Gesetzes entbunden werden. Vorbild für eine solche Regelung könnte die 1951 geschaffene Vorschrift des §100 III StGB zum Schutz von Bundestagsabgeordneten vor Strafverfolgung wegen Landesverrats bei im Bundestag oder seinen Ausschüssen erfolgter Erwähnung oder Enthüllung von illegalen Staatsgeheimnissen sein, die im Rahmen der Notstandsgesetzgebung 1968 leider wieder abgeschafft wurde:

> *„Ein Abgeordneter des Bundestages, der nach gewissenhafter Prüfung der Sach- und Rechtslage und nach sorgfältiger Abwägung der widerstreitenden Interessen sich für verpflichtet hält, einen Verstoß gegen die verfassungsmäßige Ordnung des Bundes oder eines Landes im Bundestag oder in einem seiner Ausschüsse zu rügen, und dadurch ein Staatsgeheimnis öffentlich bekannt macht, handelt nicht rechtswidrig, wenn er mit der Rüge beabsichtigt, einen Bruch des Grundgesetzes oder der Verfassung eines Landes abzuwehren."*

Abschluss eines Datenschutzabkommens mit den USA

Der Schutz der persönlichen Daten europäischer Bürgerinnen und Bürger in den Vereinigten Staaten ist nicht ausreichend; das „Safe-Harbor"-Abkommen hat sich in der Praxis als ineffektiv erwiesen. Gleichzeitig werden US-amerikanischen Behörden umfassende Datenbestände zur Verfügung gestellt.

Ein effektives Abkommen ist zu schaffen, durch das Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte, Art. 8 EMRK, der unter anderem das Privatleben schützt und auch den Datenschutz umfasst, und Art. 8 EUGR-Charta sowie entsprechende Schutzrechte im US-Recht wirksamer als bisher gewährleistet werden. Es bedarf normenklarer Regelungen zur Datensicherheit, zur Begrenzung der Datenverwendung, zur Transparenz und zum Rechtsschutz. Sofern ein Betroffener vor Durchführung einer Maßnahme keine Gelegenheit hatte, sich vor den Gerichten gegen die Verwendung seiner Telekommunikationsverkehrsdaten zur Wehr zu setzen, ist ihm eine gerichtliche Kontrolle nachträglich zu eröffnen. Dies setzt auch eine Pflicht zur Benachrichtigung der Betroffenen voraus, die nicht außer Kraft gesetzt werden darf.

Beendigung der Ausspähung auch in Europa und Deutschland

Nicht nur amerikanische, sondern auch deutsche Behörden und Behörden unserer europäischen Partnerstaaten spähen, Medienberichten zufolge, die Bevölkerung aus. Neben der US-amerikanischen NSA und dem britischen GCHQ werden in der Öffentlichkeit eine Reihe weiterer Dienste genannt – unter anderem europäische und weitere, im Verbund *five eyes* mit Amerikanern und Briten kooperierende Dienste.

Die Bundesregierung muss Maßnahmen zur illegitimen Totalüberwachung der Bevölkerung durch deutsche Behörden sofort beenden und auf europäischer und internationaler Ebene auf dessen Beendigung durch Partnerstaaten hinwirken. Bei massiven Verstößen sollte ein EU-Vertragsverletzungsverfahren erwogen werden.

Stopp neuer Maßnahmen zur Ausspähung der Bevölkerung

Auch nachdem der EU-Richtlinie zu Vorratsdatenspeicherung 2006/24/EG vom Europäischen Gerichtshof (EuGH) eine klare Absage erteilt wurde, hält die Debatte über ihre Einführung an. Immer wieder werden Forderungen nach einer neuen, „gerichtsfesten" EU-Richtlinie, oder nach einer „verfassungsgemäßen" Umsetzung der Vorratsdatenspeicherung als deutschem Sonderweg erhoben. Weitere Maßnahmen wurden offenbar während der Koalitionsverhandlungen diskutiert, etwa die Abkehr vor der bisher vorgeschriebenen strikten Zweckbindung von Daten aus dem Mautsystem Toll Collect und das Abgreifen von Kommunikationsdaten an Netzknotenpunkten durch deutsche Behörden.

Angesichts des in den letzten Monaten bekannt gewordenen Umfangs der Massenüberwachungen ist ein Überwachungsmoratorium geboten; bis zur Aufklärung der Vorwürfe ist auf weitere Maßnahmen zur Ausspähung der Bevölkerung zu verzichten. Notwendige Überwachungsmaßnahmen müssen sich am Schutz der Privatsphäre orientieren und nicht am gerade noch verfassungsrechtlich Erlaubten.

Effektiver Schutz von Whistleblowern

Durch die Informationen von Edward Snowden wurde die Ausspähung der Bevölkerung – bis hin zur Bundeskanzlerin und ihrem Vorgänger – in der Öffentlichkeit bekannt. Vertraulichkeit im diplomatischen Verkehr ist zwischen Staaten und im innerstaatlichen Regierungshandeln essentiell. Doch illegales, unlauteres oder skandalöses Verhalten verdient keinen Schutz. Whistleblower leisten der Öffentlichkeit einen großen Dienst – nur durch sie ist es häufig möglich, solche Handlungen in Behörden und auch Unternehmen aufzuklären und für eine wirksame Durchsetzung des Rechts zu sorgen.

Die Kriminalisierung von Whistleblowern muss gestoppt werden, und auch bei befreundeten Staaten ist auf effektiven Rechtsschutz für Whistleblower hinzuwirken. Solange dies nicht gewährleistet ist, muss Whistleblowern, die vor Verfolgung und Repressalien Schutz suchen, Asyl gewährt werden. Sie sind gegebenenfalls in Zeugenschutzprogramme aufzunehmen und vor Auslieferung zu schützen.

Rechtliche Forderungen

Effektives Datenschutzrecht in der Europäischen Union und in Deutschland

In den europäischen Institutionen wird mit der EU-Datenschutz-Grundverordnung gerade das künftige Datenschutzrecht für die Europäische Union verhandelt. Diese Verhandlungen sind einem starken Lobby-Druck ausgesetzt; die Verordnung droht, in wesentlichen Punkten hinter dem notwendigen Schutz der Persönlichkeitsrechte zurück zu bleiben, so zum Beispiel durch eine weite Auslegung „berechtigter Interessen" zur Datennutzung oder unzureichende Beschränkung von Profiling.

Die Bundesregierung muss sich für ein starkes Datenschutzrecht in Europa einsetzen. Unternehmen, die unter Verletzung gelten-

den Rechts Daten an Behörden oder andere Stellen weitergeben, sind mit empfindlichen Strafen zu belegen, die sich am Umsatz orientieren.

Strafverfolgung von illegalen Überwachungsmaßnahmen

Die nachrichtendienstliche Ausspähung der deutschen Bevölkerung ist unzulässig und nach §§99, 202a, 202b StGB strafbar. Das Fernmeldegeheimnis ist nach Art. 10 GG geschützt. Die massive Einschränkung dieses Grundrechts durch ein Verwaltungabkommen widerspricht dem rechtstaatlichen Prinzip des Vorbehalts des Gesetzes für Grundrechtseingriffe sowie dem Publizitätsgebot, wie es sich aus Art. 19 Abs. 1 GG ergibt. Sowohl das Grundrecht auf informationelle Selbstbestimmung als auch das Telekommunikationsgeheimnis statuieren nicht nur Abwehrrechte gegenüber der deutschen Staatsgewalt, sondern auch Schutzpflichten des Staates gegenüber Eingriffen durch andere.

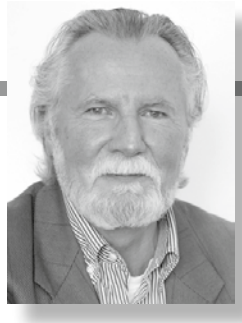
Auch wenn die Nachrichtendienste anderer Staaten nicht an das deutsche Grundgesetz gebunden sind, ist die Bundesregierung gleichwohl verpflichtet, die Bevölkerung in Deutschland vor Angriffen und den damit verbundenen Verletzungen deutscher Grundrechte zu schützen. Ebenso gelten internationale Menschenrechtsverträge; zu nennen ist Art. 17 des internationalen Pakts über bürgerliche und politische Rechte, der die Staaten zum Schutz der Privatsphäre und der Korrespondenz verpflichtet – auch wenn dessen Einhaltung nicht durch ein internationales Gericht, sondern „nur" durch den Menschenrechtsrat der UNO kontrolliert wird. Dieser hat ausdrücklich festgestellt, dass „… die Überwachung mit elektronischen oder anderen Mitteln, das Abfangen telefonischer, telegraphischer oder anderer Mitteilungen, das Abhören und die Aufnahme von Gesprächen verboten sein [sollten]." Großbritannien, dessen Geheimdienst GCHQ sich an der Globalüberwachung ebenfalls intensiv beteiligt, ist darüber hinaus an die Europäische Menschenrechtskonvention (EMRK) gebunden, deren Art. 8 ebenfalls den Schutz der Privatsphäre und der Korrespondenz statuiert.

Der Generalbundesanwalt muss gegen die Verantwortlichen effektiv ermitteln. Die Verantwortlichen für illegale Aktivitäten müssen zur Verantwortung gezogen werden. Die Bundesregierung muss ihrer Schutzpflicht gegenüber der Bevölkerung in Deutschland effektiv nachkommen. Der Schutz der Grundrechte darf nicht hinter die außenpolitischen Belange der Bundesrepublik Deutschland – wie die freundschaftlichen Beziehungen zu den USA – zurücktreten.

Schaffung effektiven Rechtsschutzes bei Überwachungsmaßnahmen inländischer Dienste

In §13 G10-Gesetz hat der Gesetzgeber den Rechtsschutz gegen Beschränkungen des Post- und Fernmeldegeheimnisses ausgeschlossen. Danach ist „gegen die Anordnung von Beschränkungsmaßnahmen nach den §§3 und 5 I 3 Nr. 1 G10-Gesetz und ihren Vollzug (…) der Rechtsweg vor der Mitteilung an den Betroffenen nicht zulässig." Das erfasst auch Überwachungsmaßnahmen für ausländische Dienste. An Stelle des gerichtlichen Rechtsschutzes wird das Parlamentarische Kontrollgremium (PKG) gemäß §14 G10-Gesetz vom Bundesinnenministerium in Abständen von höchstens sechs Monaten „über die Durchführung" des G10-Gesetzes unterrichtet. Außerdem entscheidet die G10-Kommission gemäß §15 G10-Gesetz als Kontrollinstanz über die Zulässigkeit und Notwendigkeit von Maßnahmen. Ihre Kontrollbefugnis erstreckt sich auf die Erhebung, Verarbeitung und Nutzung der nach diesem Gesetz erlangten personenbezogenen Daten durch Nachrichtendienste des Bunds einschließlich der Entscheidung über die (nachträgliche) Mitteilung an Betroffene. Die Betroffenen haben dabei nicht die Verfahrensrechte wie vor unabhängigen Gerichten – bis zu ihrer nachträglichen Benachrichtigung haben sie keinerlei Kenntnis von dem laufenden Verfahren und damit auch keinerlei Möglichkeit, ihre Rechte überhaupt wahrzunehmen.

Der gesetzliche Ausschluss des gerichtlichen Rechtsschutzes muss wieder beseitigt und die heutige Praxis durch ein rechtsstaatliches Verfahren ersetzt werden, das die Rechte der Betroffenen wahrt. Der notwendigen Geheimhaltung kann im Rah-



Werner Koep-Kerstin und Stefan Hügel

Werner Koep-Kerstin, Vorsitzender der Humanistischen Union, Studium der Politischen Wissenschaften (MA) und Staatsexamen als Historiker; früherer Mitarbeiter des Bundespresseamtes, Auslandsaufenthalt 1994-1998 (USA); Sprecher der Gustav Heinemann-Initiative bis 2009. Schwerpunkte: Frieden, Militär und zivile Konfliktlösungen, Medienpolitik, Kontakt zur Plattform Zivile Konfliktbearbeitung, Zeitschrift vorgänge.

Stefan Hügel, Vorsitzender des FIfF, studierte Informatik an den Universitäten Karlsruhe und Freiburg, wo er sein Studium mit der Diplomarbeit am Institut für Informatik und Gesellschaft abschloss. Er lebt in Frankfurt am Main und arbeitet als IT-Berater.

men der einschlägigen prozessrechtlichen Vorschriften über den Ausschluss der Öffentlichkeit und über die Einschränkung der Pflicht zur Vorlage der Akten (§99 VwGO) Rechnung getragen werden. Gerichte sind nur in der Lage, qualifizierte Entscheidungen zu treffen, wenn ihnen die relevanten Unterlagen vorliegen; Geheimdienste müssen gegebenenfalls zur Vorlage gezwungen werden können. Für alle rechtswidrig erlangten Erkenntnisse muss ein absolutes Verwertungsverbot gelten. Ausnahmen von der Pflicht zur Benachrichtigung Betroffener darf es nicht geben.

Technische Forderungen

Schaffung einer Sicherheitsinfrastruktur für die Bevölkerung in Deutschland

Ein Großteil der Kommunikation im Internet wird heute noch ungesichert abgewickelt – so haben Nachrichtendienste leichtes Spiel, die Daten abzugreifen und auszuspähen. Bestehende Sicherheitsmechanismen – wie Verschlüsselung durch PGP (Pretty Good Privacy) und Verschleierung des Kommunikationsweges und Absenders wie im TOR-Netzwerk – werden häufig nicht genutzt – sei es aus Unkenntnis, aus Bequemlichkeit oder aus fehlendem Bewusstsein für die bestehenden Bedrohungen.

Bisher werden von staatlicher Seite keine adäquaten Mechanismen angeboten, die dem Nutzer ohne vertieftes technisches Wissen einen einfachen Weg bieten, sicher im Internet zu kommunizieren. Bisherige Ansätze von Behörden zur Bereitstellung solcher Infrastrukturen sind unzureichend; die Menschen alleine zu lassen und praktisch ausschließlich auf private Ansätze wie die derzeit in Mode befindlichen – freilich durchaus unterstützenswerten – Crypto-Parties zu verweisen, ist nicht hinnehmbar.

Die Bundesregierung und die zuständigen Behörden sind aufgefordert, für eine sichere Möglichkeit der Kommunikation im Internet zu sorgen, die die Privatsphäre der Menschen wahrt und sie vor Angriffen von jeder Seite nach dem Stand der Technik schützt. Gleichzeit muss durch Awareness-Programme die Bevölkerung für Fragen des Datenschutzes und der Datensicherheit sensibilisiert werden.

Die Forderungen basieren auf einem Forderungskatalog der Humanistischen Union, der für die Koalitionsverhandlungen zur Bildung der Bundesregierung 2013 zusammengestellt wurde. Für diesen Beitrag wurde der Text neu strukturiert, die Forderungen aktualisiert und erweitert. Die Autoren danken Sven Lüders für eine Reihe konstruktiver Anmerkungen.

Referenzen

Dieter Deiseroth (2013): Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland: rechtspolitischer Handlungsbedarf? In: ZRP Zeitschrift für Rechtspolitik Bd. 46, Nr. 7, S. 194-197

Humanistische Union (2013): Schreiben der Humanistischen Union an die Verhandlungsführer von CDU/CSU und SPD. http://www.humanistische-union.de/nc/aktuelles/presse/pressedetail/back/presse/article/forderungen-der-humanistischen-union-an-die-koalitionsverhandlungen-von-cducsu-und-spd/

Maria Xynou

Surveillance in the world's largest democracy

Nowadays, trading off privacy for security appears to be a trend. Law enforcement agencies around the world appear convinced that surveillance is the solution to tackle crime and terrorism, and India is no exception. India's equivalent of a "09/11" was probably marked by the 2008 Mumbai terrorist attacks[1] as, ever since, the Indian Government has implemented a wide range of data sharing and surveillance schemes. Unlike the West, where terrorist attacks are rather rare, India has suffered from a series of terrorist attacks over the last twenty-five years. As such, it is rather hard to argue that terrorism is not an issue in India. And with a population that exceeds a billion people, the centralisation of databases appears to be the answer to keeping track of populations, and effectively tackling crime and terrorism in the country. However, with such widespread surveillance, how democratic is the world's largest democracy?

Data sharing schemes

In the aftermath of the 2008 Mumbai terrorist attacks, the *National Intelligence Grid (NATGRID)*[2] was set up by the Indian Government at an estimated cost of about USD 540 million[3] to enable the collection of sensitive information from databases of departments like the police, banks, tax and telecom to track terror suspects and incidents. NATGRID is an integrated intelligence grid that will link the databases of several departments and ministries of the Government of India in order to collect comprehensive patterns of intelligence that can be accessed by intelligence agencies. NATGRID will give 11 intelligence agencies real-time access to 21 citizen data sources to track terror activities,[4] which include bank account details, telephone records, passport data and vehicle registration details, among other types of data.

Along with NATGRID, the Indian Government also set up the *Crime and Criminal Tracking Network & Systems (CCTNS)*[5], which will automatically connect the databases of 14,000 police stations across all 35 States and Union Territories[6] of India. Around USD 320 million have been allocated to the CCTNS[7], which is part of the process of modernising the police force and which is an integrated system for the sharing of data of crimes and criminals across 21,000 locations. The CCTNS will supposedly enable Indian law enforcement agencies in tracking down criminals moving from one place to another. Home Secretary *R.K. Singh* stated:

> *"This will be a wide database. It will help in arresting criminals and investigating any case. This will be a big milestone."*[8]

Surveillance schemes

Apparently linking databases and sharing data is not enough. Following the 2008 Mumbai terrorist attacks, India has gone the extra mile by implementing various surveillance schemes, widely in secret.

So-called *lawful interception* is being carried out in India, largely through the various *Lawful Intercept and Monitoring (LIM)* systems. Over the last years, mobile operators in India have deployed their own LIM systems to monitor communications running through their networks and to provide requested data to authorised security agencies.[9] Legally, all requests for interception and monitoring in India can potentially include voice, SMS, GPRS, VAS, MMS, video calls or VoIP in targeted cases.[10]

Mass surveillance in India, however, appears to be a reality in the case of Internet traffic. The Government of India has secretly deployed LIM systems at the international gateways of large Internet Service Providers (ISPs) with the purpose of monitoring all Internet traffic in India.[11] In particular, LIM systems are installed between the ISP's Internet Edge Router and the core network and have an *always live* link to the entire traffic. This enables LIM systems to have broad surveillance capabilities which are not limited to IPs, email addresses, URLs or webmails, but which expand to a broad search across all Internet traffic using *keywords* and *keyphrases*. In other words, security agencies in India using LIM systems are capable of launching a search for suspicious words which results in the monitoring of the entire Internet indiscriminately, possibly without court oversight and without the knowledge of ISPs. As such, the function of LIM systems is beyond the control of ISPs, and these surveillance systems are completely controlled by the Government of India.

Suspicious *keywords* and *keyphrases* in social media, emails, blogs, tweets, instant messaging services and in other types of Internet content will also be monitored through India's new *Network Traffic Analysis (NETRA)* system.[12] Not only will this surveillance system be capable of monitoring Internet traffic in India—widely in secret and possibly without court oversight—but it will also be capable of capturing any "dubious" voice traffic through online communications.[13] An Indian government official recently stated:

> *"When NETRA is operationalised, security agencies will get a big handle on monitoring activities of dubious people and organisations which use the Internet to carry out nefarious designs."*[14]

And apparently, monitoring the entire Internet is not enough. While only 17% of India's population uses the Internet, roughly 73% of India's population uses mobile phones.[15] Thus, the Indian Government has expanded its surveillance capabilities to telecommunications through the implementation of the *Central Monitoring System (CMS)*.[16] This surveillance scheme was initially envisioned in 2009, following the 2008 Mumbai terrorist attacks, and was officially approved by the *Cabinet Committee on Security* in 2011, and it has been implemented ever since, widely in secret.[17]

Roughly USD 72 million have been allocated for the implementation of the Central Monitoring System[18], which centralizes the interception of communications data and enables access to it by law enforcement agencies. In particular, Telecom Service Providers (TSPs) in India are required to install *Interception Store & Forward* (ISF) servers in their premises and to integrate them with their pre-existing lawful interception systems, which are connected to *Regional Monitoring Centers*. Each Regional Monitoring Centre in India is connected to the Central Monitoring System, that ultimately stores all communications data which has been intercepted by service providers across India. This is illustrated in the chart Figure 1.

The Central Monitoring System essentially automates the entire process of interception in India, since all intercepted data is automatically transmitted to national and regional databases, thus allowing law enforcement agencies to bypass service providers when gaining access to such data. Voice calls, SMS and MMS, fax communications on landlines, CDMA, video calls, GSM and 3G networks will all be monitored by the Central Monitoring System, which is connected with the *Telephone Call Interception System (TCIS)*.[19] Agencies which will have access to this data, such as the Intelligence Bureau and the Central Bureau of Investigation, are equipped with various mining tools to identify the personal information of target numbers.

Interestingly enough, the above surveillance schemes have a few things in common: they all lack legal regulation, they lack public and parliamentary debate prior to their implementation, they lack oversight mechanisms and they are all being carried out widely in secret. Yet, they are all being carried out in the name of *public security*. Does this make sense?

Surveillance: an invisible threat

Modern slavery, poverty and corruption are just a few of the problems that India faces. Approximately 32.7% of India's po-

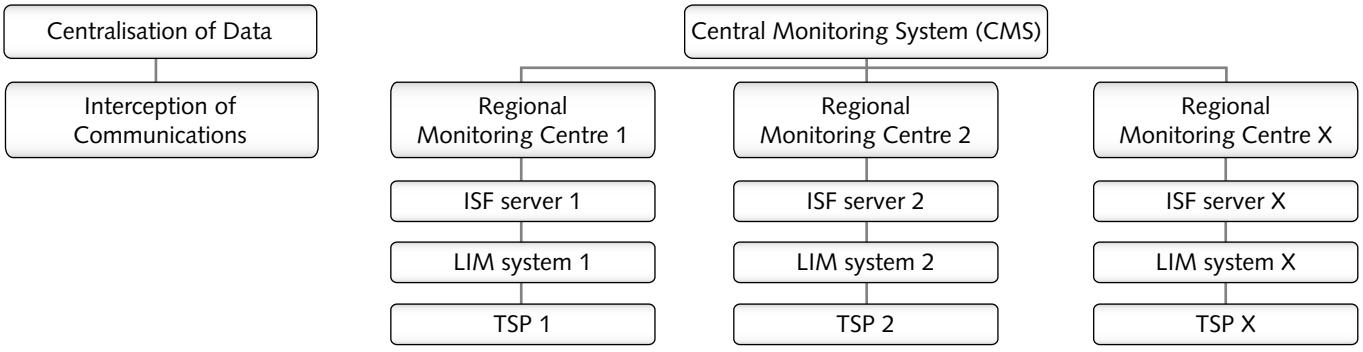


Figure 1

pulation falls below the international poverty line of USD 1.25 per day[20], while 68.7 % lives on less than USD 2 per day.[21] Around 14.7 million people in India are estimated to live in conditions of modern slavery[22], while child slavery and sex slavery are extremely prevalent in the country. All such issues inevitably lead people in India to consider surveillance a "Western, elitist" issue – if an issue at all.

"I'm not a terrorist, I have nothing to hide!" is probably one of the most mainstream parlance concerning surveillance that can be heard all the way from San Francisco's Bay Area to India's impoverished slums. After all, surveillance does not appear to present some type of direct threat to people's lives. It is probably quite comforting and reassuring to think that we are not *special* or *important* enough to be under surveillance. Why would governments be interested in the photos we share on *Facebook* or in the SMS we send to our friends? If people in the West – who have solved all of their survival issues and who enjoy a high quality of life – think along these lines, why shouldn't Indians? If people in the West don't necessarily perceive surveillance to be a direct threat to their human rights, why should people in India do so, especially when they have greater issues to deal with? Furthermore, terrorist attacks in India aren't nearly as rare as they are in the West, which possibly gives the Indian Government a greater reason to spy on its citizens.

Unfortunately though, it's not up to us to define the value of our data, but it is rather defined by some data analyst somewhere or, even worse, by some data mining software somewhere. The whole "I have nothing to hide, I am not a terrorist" parlance appears to be a psychological coping mechanism when dealing with surveillance, since we are likely in denial when it comes to our data being *important* or *interesting* enough to be monitored.[23] Edward Snowden's revelations over the last months have revealed that governments do indeed have an interest in our data. India's surveillance schemes illustrate that the Indian Government is extremely vested in monitoring its citizens communications. Yet, the real issue in India doesn't appear to be the centralization of data and the Government's surveillance schemes per se, but rather the fact that surveillance appears to be an *invisible threat*.

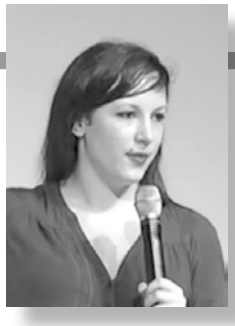
Most people in India live in poor living conditions and are as such oblivious to the dangers posed to their human rights by the government's widespread surveillance. India's middle class is increasingly becoming aware of the issue, but it appears to remain an *invisible threat*, since its potential implications on human rights are not yet visible. However, *invisible threats* are possibly extremely dangerous precisely because they do not appear to have direct implications on human rights and drastic measures are stalled – if taken at all.

India's middle class is expanding and so is surveillance in the country. Will people over the next decades challenge the authority when they feel that their human rights are being violated, or will they refrain from doing so out of fear from losing their new economic status? Will India's future middle class passively accept the state of surveillance, which will already be established and part of the status quo? Data retention is a huge element of surveillance which appears to be extremely concerning. Not only will the world's largest democracy monitor all communications, but it will also retain such data in the long term which could potentially be misused by future governments, especially without adequate safeguards in place.

Privacy is a fundamental human right which protects individuals from abuse by those in power.[24] Privacy should be at the core of all democracies, to ensure that individuals' liberty, autonomy and other human rights are protected. However, India is currently implementing widespread mass surveillance schemes, while no privacy law exists and while lacking all other adequate safeguards. How democratic is the world's largest democracy, in light of such surveillance? This should be a cause for concern for the future of all democracies today.

Anmerkungen

1 *http://edition.cnn.com/2013/09/18/world/asia/mumbai-terror-attacks/*
2 *http://www.pib.nic.in/newsite/erelease.aspx?relid=56395*
3 *http://www.deccanherald.com/content/181065/mha-seeks-over-rs-3400.html*
4 *http://articles.economictimes.indiatimes.com/2013-09-10/news/41938113_1_executive-order-national-intelligence-grid-databases*
5 *http://pib.nic.in/newsite/erelease.aspx?relid=49261*
6 *http://ncrb.nic.in/AboutCCTNS.htm*
7 *http://www.thehindu.com/news/national/govt-launches-crime-tracking-pilot-project/article4272857.ece*
8 *http://www.thehindu.com/news/national/govt-launches-crime-tracking-pilot-project/article4272857.ece*
9 *http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece*
10 *http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf*
11 *http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece*
12 *http://www.medianama.com/2014/01/223-indian-govt-internet-monitoring-system-netra/*



Maria Xynou

Maria Xynou is a Policy Associate on the Privacy Project at the *Centre for Internet and Society (CIS)*. She has previously interned with *Privacy International* and with the Parliament of Greece. Maria holds a Master of Science in Security Studies from the University College London (UCL).
maria@cis-india.org

13 *http://timesofindia.indiatimes.com/tech/tech-news/internet/Govt-to-launch-internet-spy-system-Netra-soon/articleshow/28456222.cms?referral=PM*
14 *http://www.dnaindia.com/scitech/report-indian-government-to-launch-internet-spy-system-netra-soon-1945867*
15 *http://wearesocial.net/tag/india/*
16 *http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system*
17 *http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about*
18 *http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about*
19 *http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system*
20 *http://povertydata.worldbank.org/poverty/country/IND*
21 *http://povertydata.worldbank.org/poverty/country/IND*
22 *http://www.globalslaveryindex.org/country/india/*
23 *https://www.youtube.com/watch?v=GMN2360LM_U*
24 *https://www.schneier.com/blog/archives/2008/03/privacy_and_pow.html*

Jens Crueger und Thomas Krämer-Badoni

Nichts als Hilflosigkeit

Privatheit und Freiheit in der digitalen Gesellschaft

Vorbemerkung: Der amerikanische Wissenschaftshistoriker Peter Galison *hat in der* FAZ *vom 8. April 2014 die These vertreten, dass die kontinuierliche Überwachung der digitalen Datenströme zu einer Selbstzensur führe, wie sie* Freud *zu Beginn des letzten Jahrhunderts in der Traumdeutung als Analogie zur tatsächlichen Zensur der Medien und des Schriftverkehrs nachgewiesen hatte. Damit wird angesichts der Unumkehrbarkeit der Überwachung digitalisierter Datenströme die Hilflosigkeit des überwachten Individuums zu Unrecht zementiert. Ähnlich wie Galison gehen auch wir davon aus, dass der Kampf gegen die umfassende Überwachung im Grunde nicht zu gewinnen ist. Wir glauben aber, dass der eigentliche Kampf zukünftig um die Frage geführt werden muss: Wer darf die gewonnenen Erkenntnisse der Überwachung nutzen, und was darf er damit machen? Dies wird ein langer Kampf mit vielen Rückschlägen werden. Wenn wir ihn aber nicht führen, verlieren wir all das, was die Freiheit einer Gesellschaft ausmacht.*

Seit wir gewahr wurden, dass die *National Security Agency (NSA)* der Vereinigten Staaten von Amerika sowie der Britische Geheimdienst *Government Communications Headquarters (GCHQ)* alle Daten sammeln, derer sie habhaft werden können, ist die Welt des Internet nicht mehr die, die sie davor zu sein schien. Aber es fällt schwer zu glauben, dass alle *Experten* so blind gewesen sein sollten, dass sie alle aus einem heilen Cyberspace plötzlich auf den Boden der politischen Realität stürzten – obwohl wir ihnen die Überraschung abnehmen. Sie wollten nicht sehen, und wer nicht sehen will, der wird auch gegenüber dem Sichtbaren blind. Und sichtbar wäre die offene Flanke digitaler Kommunikation schon lange gewesen.

Wie kam es zu dieser Blindheit? Zunächst einmal schlicht dadurch, dass der *Personal-Computer* (PC) und das für den Alltagsgebrauch nutzbar gewordene Internet eine so gewaltige kulturelle Innovation darstellten, dass nach der anfänglichen Skepsis (wie viele Arbeitsplätze kostet das? wird das Arbeitsleben intensiviert?) diese Instrumente mit einer großen Euphorie angenommen wurden. Die kontinuierliche Verbesserung der *Usability* (sprich Nutzbarkeit) mag zur Selbstverständlichkeit der optimistischen Technikakzeptanz beigetragen haben: Waren anfangs noch vergleichsweise umständliche DOS-Befehle erforderlich, verdeckte die ästhetische und funktionale Optimierung der Nutzeroberflächen bald jeglichen kritischen Blick in den zugrunde liegenden Quellcode. Der Siegeszug der internetbasierten Vereinfachung unseres Lebens vollzog sich mit historisch ungekannter Geschwindigkeit, von der Transformation ganzer Bücher in leicht zu handhabbare PDF-Dateien, über die Entwicklung von Suchmaschinen bis hin zum faktischen Monopol von Google, vom Heranwachsen gewaltiger Lexika wie der Wikipedia bis hin zur Entstehung der Social Media, also von Kommunikationsplattformen, über die es möglich wurde, in extrem kurzen Zeiträumen eine nahezu unbegrenzte Anzahl von Individuen zu vernetzen und zu Aktivitäten zu bewegen.

Bis zur öffentlichen Thematisierung der Überwachungspraktiken der Geheimdienste glich dieser Optimismus jenem, der nach dem Fall des Eisernen Vorhangs die Medien und die größten Teile der Öffentlichkeit bewegt hatte. Die immer wieder zutage tretenden Risiken des Kalten Krieges hatten die Wahrnehmung der politischen Weltlage so dominiert, dass nunmehr eine friedliche, abgerüstete Welt phantasiert wurde, eine Welt mit weniger Waffen und vor allem: ohne Kriege. Es war völlig übersehen worden, dass es gerade der Kalte Krieg war, die Aufteilung der Welt in zwei Blöcke, die den Ausbruch internationaler Kriege zwischen den Blöcken verhindert hatte, weil solche Konflikte in dem Augenblick, in dem sie kriegerisch geworden wären, das Risiko eines Weltkriegs mit unabsehbaren Folgen nach sich gezogen hätten. Man denke an Ungarn 1956, die Berlin-Blockade, den Bau der Mauer 1961 oder an die Kubakrise 1962, sowie schließlich an die sowjetische Invasion der Tschechoslowakei 1968. Kriegsrisiken, die im *Kalten* Krieg entstanden waren, wenn in die Interessensphäre des jeweils anderen Blocks eingegriffen wurde, die aber nicht zu einem Weltbrand wurden, weil das Gleichgewicht der Kräfte eine weitgehende Zerstörung sowohl des Angreifers wie auch des Angegriffenen bedeutet hätte. Diese Situation war also nun plötzlich mit der Auflösung des sowjetischen Blocks vorbei, aber statt einer friedlichen Welt, die etwa in Francis Fukuyamas populären Thesen als Ende der Geschichte phantasiert wurde, erlebten wir ein Ausufern kriegerischer Auseinandersetzungen. Der Deckel, der bislang Kriege weitgehend verhindert hatte, war verschwunden. Und statt Frieden und Abrüstung entstanden im Gegenteil immer deutlicher sichtbar: Kriege und Aufrüstung. Die Welt nach dem Verschwinden des Eisernen Vorhangs und dem Zerfall des Warschauer Paktes ist zur Zeit vermutlich gegen den Ausbruch eines Weltkriegs ganz gut gesichert, nicht aber gegen den Ausbruch vieler lokaler kriegerischer Konflikte, und die bergen natürlich Risiken für den Weltfrieden, erfordern ein hohes Maß an Kontrolle. Zusätzlich führen der Auftritt neuer Akteure

auf der politischen Agenda (Al Quaida) und das zunehmende politische Gewicht von Staaten wie China oder Indien zu weiter wachsenden Kriegsrisiken. Interessanterweise sind es gerade diese *neuen* weltpolitischen Risiken, welche die Entwicklung des Internet zu einem Konfliktschauplatz und zu einem staatlichen Überwachungsgebiet forciert haben.

Das alles hätte man wissen können, auch ohne die Belege von Snowden. Aber warum hat man solche Spuren trotz vielfältiger Hinweise nicht früher verfolgt? Warum hat man aus der Tatsache, dass selbst individuell agierende *Hacker* in hochsensible Netze wie das des Pentagon eindringen konnten, nicht die richtigen Schlüsse gezogen? Wieso tat man es nicht bei dem zum Massenphänomen gewordenen kriminell motivierten Datenraub? Warum blieben Viren, Trojaner und andere Schädlinge Randereignisse des öffentlichen Interesses, die lediglich auf individuelle Sorglosigkeit und/oder auf Sicherheitslücken zurückgeführt und damit in die private Sphäre jedes einzelnen Nutzers gedrängt wurden?

Um zu verstehen, warum die privaten Nutzer des Internet diese Alarmsignale nicht erblickt haben, muss man sich zunächst verdeutlichen, welche Illusionen gerade die Avantgarde des Internets pflegte. Da war zunächst die Illusion, Sicherheit im Internet sei eine Frage der technischen Entwicklung. Es reichte zu wissen, dass man den eigenen PC auf Viren und andere Schadensprogramme hin überprüfen lassen konnte. Kannte man die Schädlinge, dann konnte man sie auch unschädlich machen. Allerdings hatte man schon damals übersehen, dass Schadprogramme und Identifizierung der Schadprogramme sich zueinander verhalten wie Hase und Igel. Erst musste es ein Schadprogramm geben, bevor es identifiziert und bekämpft werden konnte. Der Hase konnte noch so schnell laufen, der Igel war schon vorher da. Was man schon da hätte lernen können: Die Entwickler von Schadenssoftware haben gegenüber den Entwicklern von Sicherheitssoftware einen strukturell bedingten Vorsprung. Aber selbst in den Fällen, in denen sich Banken, Internetprovider, Industrien oder politische und militärische Institutionen mit einer komplexen Sicherheitsarchitektur zu schützen suchen, muss festgehalten werden: jede dieser Techniken kann geknackt, gekapert und korrumpiert werden. Um es schlicht und einfach, aber keineswegs trivial, auszudrücken: Diese Techniken sind von Menschen gemacht, sie können auch von Menschen verstanden, durchschaut und umgangen, zerstört oder mit unerwünschten Intentionen genutzt werden. Natürlich werden solche Sicherheitsarchitekturen, wenn sie von Staaten entwickelt werden, viel Geld, Forschungskapazität und Personal benötigen, aber das bedeutet nicht, dass andere nicht in diese Sicherheitsarchitekturen eindringen könnten. Schon die Fähigkeiten einzelner Hacker verwiesen auf die Verwundbarkeit komplexer Systeme, und daran wird sich nichts ändern. Wir möchten an dieser Stelle daran erinnern, dass die Fiktion der frühen James-Bond-Romane und -Filme inzwischen längst Wirklichkeit geworden ist, die eine nationenunabhängige Macht imaginierte, die überall eindringen konnte. Wer hätte das geglaubt, damals, als die Filme *Liebesgrüße aus Moskau* oder *Goldfinger* in die Kinos kamen, wer hätte das ernsthaft geglaubt?

Die zweite große Illusion war die *Demokratieillusion*. Felsenfest waren die Aktivisten davon überzeugt, dass mit den Kommunikationsplattformen die Basis für eine direkte Demokratie, für eine schnelle und unbeeinflusste Meinungsbildung, für schnell herzustellende Kampagnen geschaffen worden sei. Und nun das, dass man bei all dieser Demokratie-Euphorie einem Instrument aufgesessen war, das potenziell von allen Geheimdiensten der Welt beobachtet, registriert und notfalls auch noch ausgewertet wird oder werden könnte. Das hat vielen diese Illusion geraubt und sie vom Glauben abfallen lassen. Plötzlich ist das Internet kaputt, ist der PC ein kontaminiertes Gerät, hat er sein Leben fast ausgehaucht. Der Sturz aus dem demokratischen Höhenflug ist steil, und der Aufprall hart. Aber das Ende der Demokratieillusion führt bislang nicht zu besseren Lösungen, sondern zu einer großen Hilflosigkeit. Die Ursache für den tiefen Sturz wird auch nicht in einem viel zu euphorischen Höhenflug gesucht, denn die vermeintlich Schuldigen haben wir ja schon ausgemacht: NSA, die Internetgiganten und die Deutsche Regierung, der es nicht gelungen ist, die Bürger gegen Ausspähung zu schützen, ja die nicht einmal richtige Anstrengungen für eine Sicherung des Internets zu unternehmen gewillt scheint.

Dabei hätte die Demokratieillusion schon frühzeitig als Illusion erkannt werden können. Zustimmung und Ablehnung per Mausklick führt in der Tat zu schnellen und auch quantitativ relevanten Meinungsäußerungen, aber selten auf der Grundlage eines Gedankenaustausches und einer argumentativen Auseinandersetzung, was nicht nur zu Kurzschlüssen und Schnellschüssen führt, sondern auch dem Populismus jedweder Couleur Tür und Tor öffnet. Es ist wie in der Studentenbewegung, als Unterschriftslisten mit dem Titel „*Weg mit …*“ fast schon alleine wegen der radikalen Überschrift ihre Anhänger fanden, nur dass Petitionen und *shitstorms* gerade auf der Grundlage der neuen Kommunikationsplattformen schnell tausende und hunderttausende Anhänger und Stimmen erhalten können. Nachdenklichkeit setzt oft erst dann ein, wenn der Schaden solcher Strategien bereits eingetreten ist, und sei es auch nur in der Form des Erschreckens darüber, wie leicht es war, solche Massen von Menschen zu einer spontanen Meinungsäußerung zu bewegen, für die man als Individuum nicht mehr grade zu stehen hat – anders als die von einem *shitstorm* betroffenen Personen, die dann tatsächlich bis zum Hals im Dreck stecken.

Damit möchten wir nicht sagen, dass die neuen Kommunikationsplattformen kein Potenzial zur Demokratieförderung in sich trügen, aber es wird noch lange dauern, bis wir über eine Internetkultur verfügen, die eine Nutzung dieser Instrumente ohne Risiko des Missbrauchs zulässt. Das eigentliche Problem bei der Entstehung einer solchen und so dringend benötigten Kultur, ist nicht die Technik, sondern das sind WIR: Wir sind das Problem, wir müssen Verhaltensregeln entwickeln und uns zu eigen machen, Maximen einer zivilisierten Kommunikation nicht nur selber befolgen, sondern deren Befolgung auch von unseren Kommunikationspartnern und -partnerinnen einfordern, was nichts anderes bedeutet als die Internalisierung von Verhaltensregeln, über die wir noch gar nicht verfügen. Denn bislang war unsere Kommunikationskultur geprägt von direkter persönlicher Kommunikation, vis-a-vis, telefonisch, schriftlich; oder indirekt durch Massenmedien. Aber immer waren Sprache, Schrift und Druck unsere Kommunikationsmedien, Privatheit die Voraussetzung dieser Art der Kommunikation. Briefgeheimnis, Schutz der Intimität des Wohnens, Telefongeheimnis, die Nichtöffentlichkeit unserer privaten Äußerungen, das waren die grundlegenden Bestandteile einer demokratisch verfassten Gesellschaft, struktu-

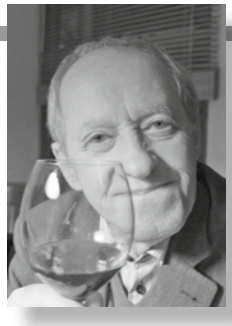
relle Voraussetzungen unserer individuellen Existenz. So sind wir aufgewachsen nach dem 2. Weltkrieg, und vermutlich wuchsen auch später die Kinder noch so auf, zumindest diejenigen, deren Denken und deren Kulturwahrnehmung sich noch vor dem Siegeszug der Kommunikationsplattformen und der Zerstörung der Privatsphäre etablieren konnten.

Denn das ist der zentrale Bestandteil der zukünftigen Gesellschaft, das wird sie maßgeblich von unserer heute noch existierenden Gesellschaft unterscheiden: Privatheit in der bisherigen Form wird es nicht mehr geben und nicht mehr geben können, es sei denn, die Weltgesellschaft zerfiele in Myriaden kommunikationslos nebeneinander existierender Gemeinschaften, in post-demokratische oder besser: post-zivilisatorische Stammesgesellschaften. Eine solche Entwicklung ist natürlich nicht wünschenswert, und es bleibt zu hoffen, dass sie auch nicht eintritt. Allerdings, ganz ausgeschlossen ist so eine Entwicklung nicht: Hunderte lokaler, räumlich begrenzter kriegerischer Konflikte sind letztlich die Folge der Auflösung der zwei großen gesellschaftlichen Machtblöcke und damit des Zusammenwachsens der Welt zu einer Welt, innerhalb derer die verschiedenen Ideologien und Teilstrukturen nicht mehr die Kraft haben, entweder einen neuen Block zu bilden oder die Welt als ganze zu dominieren. Dass solche Entwicklungen möglich sind, zeigte nicht zuletzt die Entwicklung in der Türkei. Die Regierung Erdogan ließ Anfang 2014 vor den Kommunalwahlen in der Türkei kurzerhand zunächst *Twitter*, dann aber auch *Youtube* abschalten, um so die Verbreitung von Gerüchten über die Korrumpierbarkeit der Regierung zu verhindern. Plötzlich ist eine Welt mit aus dem Internet herausgetrennten Teilstücken wieder denkbar geworden. Es bleibt zu hoffen, dass solche Entwicklungen, die ja auch von China und anderen autokratischen Staaten genutzt werden, nicht auf Dauer durchgesetzt werden können.

Wenn es stimmt, dass die neuen Kommunikationsformen und die Digitalisierung eine nicht reversible Entwicklung eingeleitet haben, dann folgt daraus natürlich auch, dass es eine Privatheit, wie sie sich als Strukturmerkmal der demokratischen Gesellschaften herausgebildet hatte, nicht mehr geben wird. Und wenn die Technik nicht reversibel ist, wenn jede weitere Technik zu nichts anderem als einem Ver- und Entschlüsselungswettrennen führt, dann gibt es nur noch eine einzige Instanz, auf die es ankommen wird: Wir, auf uns wird es ankommen.

Das mag nach Hybris klingen, anmaßend erscheinen, manche werden es für lächerlich halten. Aber tatsächlich ist nur der Mensch in der Lage, in einer solchen Situation Verhaltensentwürfe zu entwickeln, die eine zukünftige Gesellschaft entrümpeln und vom Ballast der alten Gesellschaft befreien, ohne die grundlegende Freiheit eines demokratischen Gemeinwesens preiszugeben. Wenn wir auch künftig frei leben und kommunizieren wollen, werden wir langfristig Gesellschaft nicht nur neu denken, sondern auch umfassend gestalten müssen. Wir werden auf das Internet, auf die Digitalisierung der Kommunikation weder verzichten können noch wollen, wir werden die Errungenschaften des Internet verteidigen müssen, ohne die analog organisierte Gesellschaft zum Maßstab aller Dinge zu machen, denn diese Gesellschaft wird nicht wieder auferstehen.

Eine *Privatheit*, wie wir sie kennen, wird es in der digitalen Gesellschaft nicht geben. Entweder wir geben die Nutzung des Internet auf, oder wir gehen das Risiko ein, dass alles, was wir schreiben und *posten*, was wir tun, wo wir sind, wen wir kontaktieren, öffentlich wird. Oder besser: öffentlich ist. Potenziell, denn nicht jeder Mensch wird jede Äußerung wahrnehmen, aber öffentliche Institutionen (und natürlich: die Geheimdienste) werden sich mit Hilfe von Algorithmen die Informationen suchen, von denen sie glauben, dass sie ihnen nützlich sind. Schulen, Arbeitgeber, Staatsanwälte, Polizei, alle diese Institutionen werden genau all die Bereiche durchforsten, die wir bisher als unsere ureigensten privaten Bereiche verstanden haben, wenn wir als Jugendliche auf Partys uns so verhalten, wie es weder unsere Eltern noch die Schulen oder Ausbildungsstätten akzeptabel finden, wenn unsere Pornosucht oder die Kontakte mit der Konkurrenz unseren Arbeitgebern nicht gefallen, wenn wir von unseren Krankenversicherungen Kündigungen erhalten, weil unsere Suche nach Stichworten wie „Niereninsuffizienz“, „Herzversagen“, „Myasthenia gravis“ oder „Geschlechtskrankheiten“ sie darin bestätigt hat, dass wir künftig zu teure Patienten sein werden, wenn alle diese Dinge passieren (sie geschehen ja heute schon), dann wird es auf zweierlei ankommen: Erstens darauf, sich nicht in dem, was wir tun und tun wollen, einschränken zu lassen. Wenn wir aus Angst vor Veröffentlichung alles das nicht mehr tun, was wir gerne tun wollen und was wir als unser Recht und als den Inbegriff unserer eigenen individuellen Freiheit begreifen, dann haben wir unsere Freiheit bereits aufgegeben, dann haben wir uns aufgegeben. Und zweitens wird es darauf ankommen, einen langen Kampf zu führen gegen all jene, welche die Informationen, derer sie habhaft werden, gegen uns richten. Wir werden *in the long run* nicht verhindern können, dass die digitalisierte Informationstechnik es allen gesellschaftlichen Institutionen ermöglicht, alles über uns



Jens Crueger und Thomas Krämer-Badoni

Jens Crueger, Jahrgang 1984, studierte Geschichte und Soziologie mit Schwerpunkt Wissenschaftsgeschichte und Kulturgeschichte der Digitalisierung. Forscht momentan über die Veränderungen wissenschaftlicher Fachkommunikation durch die Digitalisierung.

Thomas Krämer-Badoni, Jahrgang 1944, lehrte als Professor für Sozialwissenschaften an der Universität Bremen. Seit seiner Pensionierung geht er mit Jens Crueger der Frage nach, welche Auswirkungen die digitale Revolution auf das kommunikative Verhalten in der digitalisierten Gesellschaft haben wird.

Wissenswerte zu erheben. Wogegen wir aber kämpfen können und auch kämpfen sollten ist, dass diese Informationen zu unserem Nachteil verwendet werden. Dafür müssen wir Rechtsformen finden, aber angemessene Rechtsformen wird man nur dann finden können, wenn wir in einem zähen Ringen mit uns selber eine neue Kultur der Kommunikation entwickeln. Und genau darin liegt das Hauptproblem: Rechtsformen sind in Regeln gefasste Gesellschaft, unsere heutigen Rechtsformen lösen die Probleme der analogen Gesellschaft. Die Probleme der digitalen Gesellschaft müssen wir erst noch entdecken und verstehen, ihre Handhabung erfordert Offenheit und kulturelle Phantasie. Und erst nach der Entstehung neuer kultureller Strukturen werden wir die der digitalen Gesellschaft entsprechenden Rechtsformen entwickeln können. Angesichts der gesellschaftlichen Transformationen, die uns bevorstehen, wird die Entwicklung einer neuen Kultur der Kommunikation Jahre und Jahrzehnte, auch länger dauern. Der Weg wird lang und steinig sein, aber wir werden ihn gehen müssen. Auch für uns gibt es kein Zurück. Wohin auch?

Albrecht Funk

„The only problem is that the Internet, by its very nature, has no borders and if the U.S. takes on the mantle of the world's police; that might not go down so well."
Former NSA Director, Army General Keith Alexander, 2010[1]

Nationale Sicherheit im Cyberspace?

Vor achtzehn Jahren erklärte John Perry Barlow*, ein Netzaktivist der ersten Stunde, die Unabhängigkeit der Netzbürger im Cyberspace. „Im Namen der Zukunft bitte ich Euch …" – die Regierungen der Industriestaaten – „… uns alleine zu lassen. Ihr seid nicht willkommen bei uns. Ihr habt keine Souveränität wo wir uns versammeln."*[2]

Heute erscheint uns seine Unabhängigkeitserklärung nur noch als ein letzter, trotziger Aufschrei aus dem letzten Jahrhundert. Wie im 20. Jahrhundert, als die damaligen Großmächte ihre Herrschaft zu Wasser, zu Land und in der Luft absicherten, suchen heute die USA, China oder Russland, neben vielen kleineren Mitspielern, ihre Kontrolle auf den grenzenlosen, virtuellen Raum auszudehnen, in dem sich für die Mehrheit der Menschheit, gewollt oder nicht, ein Teil ihres Lebens abspielt. Machtstaat ist heute nur noch, wer über Macht im Cyberspace verfügt. Und wer immer über die vielen Meldungen von russischen und chinesischen Cyberattacken die Orientierung verlor, kann durch die Enthüllungen Snowdens den Sinn für Proportionen wiedergewinnen: Es sind die USA, die durch ihre militärischen und geheimdienstlichen Sicherheitsapparate die absolute Vorherrschaft im Cyperspace haben.

Es ist nun schon ein Jahr verstrichen, seit Snowden die Macht der NSA im Cyberspace zu einem Thema deutscher Politik machte. Doch alle Versuche, die Probleme, die sich aus der nationalen Sicherheitspolitik der USA für die Bürger der Bundesrepublik ergeben, zu benennen und politisch anzugehen, sind bis jetzt gescheitert. Die Reaktionen der Bundesregierung schwanken vielmehr zwischen der Hinnahme der amerikanischen Überwachungspraxis und trotzigen Forderungen nach nationalen Gegenmaßnahmen, sei es dem Ausbau der Geheimdienste, dem Boykott amerikanischer Softwarefirmen, oder gar dem Bau einer elektronischen *Berliner Mauer* im Cyberspace.

Die widersprüchlichen Reaktionen speist eine symbolische Politik, die nationale Souveränität suggeriert, wo Hilflosigkeit herrscht. Die Versuche, mit einer nationalen Strategie die Informationssicherheit der Bundesbürger zu schützen – oder sei es auch nur die der Bundesregierung – münden in einer Sackgasse. Sie reduzieren in offenen Netzen, die keiner zentralen Kontrollinstanz unterworfen sind und global genutzt werden, die Informationssicherheit aller Nutzer. Dies gilt nicht zuletzt auch für die USA. Im Kampf um informationelle Vorherrschaft untergräbt sie nicht nur die Informationssicherheit der Netzbürger in anderen Staaten, sondern auch die ihrer eigenen Bürger. Mehr noch, sie stellt die Existenz einer globalen Kommunikationsinfrastruktur selbst in Frage.

Verbessern lässt sich die prekäre Lage der *Netzbürger* nur durch eine Sicherheitspolitik, die den Cyberspace soweit wie möglich dem Zugriff und den potenziellen Angriffen der Nationalstaaten entzieht. Das mag utopisch und politisch naiv klingen. Doch an der Notwendigkeit, den Cyberspace gegen die Bemühungen der Nationalstaaten abzuschirmen, *Cybersecurity* als nationale Sicherheit zu buchstabieren, hat sich seit Barlows Aufschrei nichts geändert. Im Gegenteil, die Enthüllungen Snowdens verleihen dem Ruf nach einer globalen und zivilen Sicherheitspolitik nur eine größere Dringlichkeit.[3]

Die Sicherheit der National Security Agency

Dass die globale Überwachung digitaler Kommunikation die Reaktion auf die Terroranschläge des Jahres 2001 sei, steht ganz oben auf der Liste der Rechtfertigungslegenden, welche die NSA ihren Propagandisten nach den Snowden-Veröffentlichungen in die Hand drückte. Doch die Grundstruktur des elektronischen Leviathans, den wir heute bestaunen, war bereits um die Jahrtausendwende sichtbar, oder zumindest erahnbar, und – in den *Echelon*-Debatten des Europäischen Parlaments zum Beispiel – auch Gegenstand öffentlicher Diskussion.

Was die Terroranschläge Al-Quaidas offenbarten, war die Unzulänglichkeit einer Politik, die nach dem Ende des Kalten Krieges mit dem Drohgespenst eines elektronischen Pearl Harbor den militärisch-geheimdienstlichen Komplex zu sichern und auszubauen suchte. Die Folge dieses Versagens war aber nicht die Revision der bisherigen Politik, sondern die Generalisierung der

Bedrohungsszenarien. Die von Geheimdiensten und Sicherheitsanalytikern verkannte *asymmetrische Bedrohung* durch eine lose organisierte, aus den Höhlen Afghanistans heraus operierende Terrorgruppe verschmolz mit der Bedrohung des Cyberterrorismus und diente nun als Begründung für Überwachungsstrategien, die bis dahin rechtlich und politisch nicht durchsetzbar waren. Um eine Stecknadel im Heuhaufen zu finden bedürfe es einer *total information awareness*, der Sammlung aller erreichbaren Informationen, die potenziell die nationale Sicherheit schädigende Aktivitäten vorhersehen und verhindern können.

Das von Admiral John Poindexter propagierte *Terrorism Information Awareness Program (TIA)* scheiterte im Jahre 2003 noch am Widerstand des Kongresses. Das Gottesauge im Emblem seines *Information Awareness Office*, mit dem diese auch auf amerikanische Bürger zu schauen gedachte, überschritt selbst die hohen Toleranzschwellen der Abgeordneten und Senatoren. Das Scheitern des TIA-Programms führte jedoch nur dazu, dass es von der NSA im Geheimen, ohne die von Poindexter vorgeschlagenen Kontrollen weiterentwickelt wurde. Und solange deren Programme nicht auf amerikanische Staatsbürger abzielen, sondern *nur* auf Ausländer, fand die klandestine Wiedergeburt der TIA durch die NSA auch beim Kongress parteienübergreifende Unterstützung.

Die rund $11 Milliarden für die NSA, mit über 30.000 Angestellen und der – bis zu Snowdens Ausstieg – ebenfalls in die Zehntausende gehenden Zahl an privaten Vertragsangestellten standen nie in Frage. Für den Kongress wie das Weiße Haus, sowie die Mehrheit der US-Bürger sind die Bemühungen der NSA um eine globale Überwachungshoheit im Cyberspace allenfalls eine politische Kosten-Nutzenfrage, ansonsten aber *fair game* – wie Außenminister Kerry mit Blick auf Merkels Handy lapidar feststellte.[4] Bar effektiver politischer und rechtlicher Kontrollen war es die Funktionslogik und das Eigeninteresse der NSA, die nach der Jahrtausendwende den massiven Ausbau der Überwachungskapazitäten bestimmten.[5] Die Vielzahl der von Snowden aufgedeckten Programme, von *PRISM* bis *MYSTIC*, vom Data-Mining der Internet-Kommunikation, der Analyse von Massendaten bis zur vorsorglichen Speicherung des gesamten Telephonverkehrs ganzer Staaten belegen diese Entwicklung und zeugen zugleich von dem exponentiellen Wachstum der Überwachungskapazitäten der NSA, ermöglicht durch milliardenschwere Investitionen und die rapide sinkenden Kosten der Datenspeicherung.

Die Macht der NSA ist nicht mit Allzuständigkeit gleichzusetzen. Im Gegenteil: Die NSA hat alle Versuche, ihr eine Zuständigkeit für die Sicherheit der nationalen Informationsinfrastruktur insgesamt zuzuschreiben, strikt von sich gewiesen und an eine lange Reihe neu geschaffener Behörden und öffentlich-privater Partnerschaften delegiert. Deren endlose Geschichte von Misserfolgen ist hier kaum von Bedeutung, wohl aber die Lehre, die *Ron Beckstrom* daraus zog, als er 2009 nach nur neun Monaten von seinem Amt als Leiter des *National Cybersecurity Center* zurücktrat, das im *Department for Homeland Security* für den zivilen Schutz der nationalen Informationsinfrastruktur angesiedelt ist:

> *„NSA currently dominates most cyber security efforts … I believe this is a bad strategy on multiple grounds. The intelligence culture is very different from a network operations or security culture. In addition, the threats to our democratic processes are significant if all top level government network security and monitoring are handled by anyone organization."*[6]

Theoretisch repräsentieren die von Beckstrom angeführten Kulturen der *Cybersecurity* drei Sicherheitsparadigmen, die in einer Bewertung von Sicherheitsrisiken zur Anwendung kommen. In der Praxis wird Sicherheit konkret durch die politische Wahl der Institutionen, denen die Selektion von Risiken und deren Bewertung anvertraut wird. Mit der Entscheidung, die Federführung in Sachen Informationsicherheit der NSA anzuvertrauen, hat deren militärisch-geheimdienstliche Kultur eine hegemoniale Stellung errungen. Die Folgen für die Sicherheit unserer globalen Informationsökologie sind gravierend. Ich will hier drei stichwortartig benennen.

1. Vom *security engineering* zur (Total-)Kontrolle des Datenverkehrs.

Die Dominanz der NSA im Bereich *Cybersecurity* hat bereits in den neunziger Jahren dazu geführt, dass die politische Diskussion um Informationssicherheit zunehmend in den Wahrnehmungsmustern militärisch-geheimdienstlicher Apparate geführt wurde: reduziert auf gezielte Attacken, sei es von einzelnen Hackern, fremden Staaten, oder von terroristischen Gruppen. *Information Assurance* erwächst in dieser klassisch polizeilich-geheimdienstlichen Sicht aus dem Bemühen, ein Eindringen in kritische Informations- und Infrastruktursysteme zu unterbinden, und dem Versuch, potenzielle Angriffe im Vorfeld abzuwehren.

NSA und Militär haben in den letzten zwei Jahrzehnten Milliarden ausgegeben, um diesem Ziel näher zu kommen. Doch bei über 2 Milliarden Nutzern, die über ein offenes Netzwerk verbunden sind, bleibt die Gefahr von Attacken allgegenwärtig. Wichtiger noch, selbst für die hoch gesicherten geheimdienstlich-militärischen Systeme, lässt sich das Risiko einer erfolgreichen Attacke nicht ausschließen.

Effektiver Schutz – so läßt sich das Paradigma der *Security* und *Network*-Kultur zusammenfassen, *„involves … building security in as we create our systems, knowing full well that they will be attacked in the future"*[7]. Oberstes Ziel der NSA war es demgegenüber, ihren Zugriff auf die rasch expandierenden digitalen Netzwerke zu sichern. Vorangetrieben wurde die globale Überwachung des Datenverkehrs in den neunziger Jahren zunächst als ein Projekt, mit dessen Hilfe relevante Informationen für die Entscheidungsfindung der Regierung aus der wachsenden digitalen Datenflut abgeschöpft werden können. Nach 2001 begründete sie dann ihre wachsenden Budgetforderungen mit dem Argument, dass eine expansive Überwachung unabdingbar sei im *war on terror*. Das ultimative Ziel von NSA-Direktor Alexander war es, die NSA an alle Datenkanäle anzukoppeln (z. B. der Internet Service Provider), so dass die Behörde als eine Art nationaler Sicherheitswall potenzielle Angriffe abwehren kann, bevor sie den Endnutzer überhaupt erreichen. *„Maybe we could do this in real time"*, räsonierte Alexander ein Jahr, bevor Snowden das PRISM Program bekanntmachte

> *„and come up with a construct [in which] you and the American people know that we're not looking at civil liberties and privacy, [but] we're actually trying to figure*

out when the nation is under attack and what we need to do about it."[8]

Ob eine Totalkontrolle des Datenverkehrs in einer nationalen *Firewall* Attacken effektiv verhindern kann, ist mehr als fraglich. Politisch begraben wurde das Orwell Ehre machende Projekt – vorerst zumindest – jedoch nicht durch die willfährigen *Intelligence Committees* des Kongresses, sondern durch die Veröffentlichungen Snowdens.

2. Von der *Defense in Depth* zur *Active Cyberdefense.*

Die technischen und operativen Möglichkeiten, eigene Informations- und Kommunikationssysteme zu schützen und in fremde einzudringen, beschäftigte Militärstrategen weltweit schon, bevor eine globale Vernetzung von Systemen in Form des Internet stattfand. Dies gilt insbesondere für die USA, für die aufgrund ihrer weltweiten militärischen Präsenz die Sicherung ihres *global information grid (GIG)* von ausschlaggebender Bedeutung war. Das Pentagon erklärte den Cyberspace deshalb schon in den neunziger Jahren neben Land, Wasser, Luft und Weltraum zu einer eigenen Kampfzone und steckte Milliarden in die Verteidigung ihrer Systeme. In den letzten Jahren begann das DoD, systematisch die Kapazitäten des Militärs für Cyberattacken, also für aktive Formen der Kriegsführung, auszubauen. Bis 2016 wird das Pentagon die Zahl seiner *Cyberwarrior* von 2000 auf 6000 aufstocken, und Milliarden in die Entwicklung neuer offensiver *Cyberwaffen* investieren.[9]

Obgleich die NSA eine *combat support agency* des Pentagon ist[10], spielten offensive Operationen in ihren Bemühungen, die Kommunikationssicherheit aller für die nationale Sicherheit relevanten Systeme zu gewährleisten, zunächst nur eine untergeordnete Rolle. Die NSA war, wie die vom DoD finanzierten CERTs, der Doktrin einer *Defense in Depth* verpflichtet, der vielschichtigen Kontrolle von Informationssystemen – der genutzten Technologien, der Operationen wie der Nutzer und Betreiber.

Die im Drohnenkrieg sichtbar werdende Verschmelzung von *Cyberoperationen* und *Signal Intelligence* zeigt nun aber auch im Bereich Informationssicherheit ihre Wirkung. Die passive Verteidigung der nationalen Infrastruktur sei unzureichend, so das Argument der NSA. Erforderlich sei eine dynamische, offensive Verteidungsstrategie. *„My own view is"*, so General Keith Alexander *„that the only way to counteract both criminal and espionage activity online is to be proactive. If the U.S. is taking a formal approach to this, then that has to be a good thing …"*[11]

Noch funktioniert das Abschreckungsprinzip des Kalten Krieges, mehr schlecht als recht.[12] Im Cyberspace können wir jedoch noch sehr viel weniger als im Luftraum, der permanent auf den Abschuss von Atomraketen überwacht wird, darauf hoffen, dass rationale Staatsakteure Fehlkalkulationen und den Ernstfall mit allen Mitteln vermeiden werden. *„With both state actors and non-state actors joining the cyber game, the risks of miscalculation between states will increase, especially if a non-state hakker can infiltrate a country's military networks and launch an attack against another country."*[13] Sowohl China als auch Russland haben den Beginn von internationalen *Abrüstungsverhandlungen* vorgeschlagen. Ob diese Absichtsbekundungen ernst gemeint sind oder nicht, ist schwer zu sagen. Denn solange die US-Politik alles daran setzt, um *Information Superiority* zu gewinnen, *„in order to gain a decision advantage for the nation and our allies under all circumstances"*, wird es keine Verhandlungen geben.[14]

3. Von der Informations- zur Überwachungssicherheit

Nominell ist die NSA alleine für die Informationssicherheit im nationalen Sicherheitsbereich zuständig.[15] Faktisch ist sie weltweit die größte und bedeutsamste Behörde, die sich mit Informationssicherheit befasst. Zusammen mit DARPA, dem Forschungsarm des Pentagons, spendet die NSA Millionen für *Computer Emergency Alert Teams* (CERTs), für Trainingsprogramme in *Information Assurance* und *Defense in Depth*. Sie finanziert Grundlagenforschung in geheimen Laboratorien und öffentlichen Universitäten. Sie vergibt sogar Preise für die besten Arbeiten im Feld *Cybersecurity*, einschließlich Arbeiten zum Thema *Datenschutz*. An der NSA geht in den USA kein Weg vorbei, für jede und jeden, die sich in der *Security* oder *Network community* mit dem Thema befassen.

Die Sicherheitsarchitektur der NSA hat jedoch einen spezifischen Zuschnitt. Sie darf den Zugriff der NSA auf Datenströme nicht behindern. Der *Kryptokrieg* der neunziger Jahre illustriert dies in plastischer Form. In der klaren Voraussicht, dass die Verschlüsselung von Daten in komplexen Netzwerken eine immer wichtigere Rolle spielen wird, suchte die NSA, unter der tätigen Mithilfe des damaligen Vizepräsidenten Al Gore, einen für sie opportunen *Escrowed Encryption Standard* durchzusetzen. Der sogenannte *Clipper Chip* erlaubte jedem privaten Nutzer eine hinreichend sichere Form der Verschlüsselung, installierte jedoch zugleich die NSA als Schlüsselhalter, als *Trusted Third Party*.

Der Widerstand war heftig. Kryptologen und die *Security Community* im Allgemeinen entfachten eine öffentliche Diskussion über die Schwachstellen und enormen Sicherheitsrisiken des Projekts. Es wurde nie realisiert.[16]

Seit Snowden wissen wir, was manche Sicherheitsexperten schon lange vermutet haben: Der Sieg im Kryptokrieg war ein Pyrrhussieg für die Sicherheitsexperten. Die NSA hat nicht nur mit Millionenzahlungen minderwertige Verschlüsselungsstandards subventioniert. Sie hat auf dem grauen Markt Schwachstellen in Computersoftware aufgekauft und sie zum Eindringen in Computersysteme genutzt, oder Methoden, die von der florierenden illegalen Untergrundökonomie entwickelt und genutzt werden, aufgegriffen und für die höheren Zwecke nationaler Sicherheit genutzt (z. B. *Botnets*). Mehr als tausend Angestellte der Behörde sind darauf angesetzt, Fehler im Code von Programmen zu finden; nicht um diese auszumerzen, sondern um diejenigen Fehler ausfindig zu machen und geheim zu halten, die sich für die Wahrung der vielfältigen Interessen nationaler Sicherheit als nützlich erweisen könnten.[17] Die NSA hat systematisch eine Politik verfolgt, die die technischen Sicherungen von Computersystemen und Netzwerken schwächt, um die Überwachung von Datenströmen zu erleichtern.

Diese Politik stößt nicht nur bei Experten auf Kritik, die zum nationalen Sicherheitskomplex kritische Distanz halten. *„This strategy"*, stellt Jon Pea, Professor for computer engineering an der Carnegie Mellon University in einer Stellungnahme für eine Ar-

beitsgruppe im Büro des US-Direktors for National Intelligence fest, *„inevitably makes it easier for criminals, terrorists, and foreign powers to infiltrate these systems for their own purposes. Moreover, everyone who uses this technology is vulnerable, and not just the handful who may be surveillance targets for U.S. intelligence agencies."*[18]

Der Schaden, den die NSA mit dieser Politik angerichtet hat, reicht weit über die unmittelbare Verschlechterung von Sicherheitsstandards hinaus. Sie hat bei Nutzern weltweit zum Verlust einer für das Funktionieren komplexer Systemen wichtigen Voraussetzung geführt – zum Verlust von Vertrauen. Wer nicht mehr auf die Integrität, Authentizität, und Vertraulichkeit seiner Nutzerdaten und seiner Datenkommunikation vertrauen kann, operiert in einem Raum der Unsicherheit, der offene Kommunikation, selbstbestimmtes Handeln, und produktive Kooperation erschwert.

Auf den ersten Blick mögen Attribute wie *offen* oder *selbstbestimmt* als rhetorischer Rückgriff auf hehre, aber abstrakte Grund- und Menschenrechte erscheinen, das *Recht auf informationelle Selbstbestimmung* eingeschlossen. Bei genauer Hinsicht zeigen sich die Folgen des Vertrauensverlustes, der nach den Veröffentlichungen der letzten Monate sichtbar wurde, in konkreter Form. Sie zeigen sich gerade dort, wo in der Vergangenheit ein sehr enges Vertrauensverhältnis herrschte: In den Beziehungen zwischen der NSA und der amerikanischen IT-Industrie.

Dem General Council der NSA, Rajesh De, ist nur schwer zu widersprechen, wenn er feststellt, dass Yahoo, Apple, Google, Microsoft, Facebook and AOL sehr wohl über den Zugriff auf ihre Daten im Rahmen des PRISM Program der NSA Bescheid wussten. Die weltweit größten Sammler von Massendaten, Google und die NSA, hatten über Jahre hinweg eine vertrauliche Kooperationen im gegenseitigen Interesse entwickelt – um etwa eine *„highly sophisticated and targeted attack on [Googles] infrastructure"* aufzuklären, die laut Google-Blog von China ausging und im Diebstahl von intellektuellem Eigentum mündete.[19] Auch die Implementation des PRISM-Programms führte zu keinen Konflikten zwischen NSA und Google.

Zugleich verschaffte sich die NSA jedoch in ingeniöser Weise Zugang zum Datenverkehr zwischen Googles gesicherten Datenzentren. Die Konzernspitze und die Sicherheitsingenieure fühlten sich hintergangen. Das Vertrauensverhältnis, das viele der IT-Konzerne auf Kosten der Nutzer und ihrer Rechte problemlos geopfert haben, steht nun für die Konzerne selbst in Frage. *„When or if the NSA … exploits its position of trust within the security community, then that´s a problem"*, stellte Art Coviello fest, CEO derselben Firma RCA, die mutmaßlich zehn Millionen für eine *Backdoor* in der Software eines ihrer Programme kassiert hat.[20]

Dass sich nun willfährige Gehilfen wie Art Coviello selbst missbraucht fühlen, ist kein Problem, allenfalls Anlass zur Schadenfreude. Wenn aber nicht mehr nur Regierungen im Namen der Staatssicherheit, sondern Geheimdienste, private Konzerne und die Gemeinde der Sicherheitsexperten gemeinsam die Rechte auf Privatheit, Informationssicherheit und eine transparente Struktur der globalen Informationsökologie untergraben, dann führt das Misstrauen der Netzbürger zu einem wirklichen Problem, dem Verlust eines jeglichen *Systemvertrauens*.

Wer kontrolliert den Cyberspace?

Am 1. Mai 1997 unterzeichneten in Genf Vertreter der damals noch kleinen Internetgemeinde, die Gründergeneration der *Internet Society* und Repräsentanten der IT-Industrie, ein *Memorandum of Understanding*, das eine neue Ära effektiver, globaler *Internet Governance* einläuten sollte. *„We the people of the Internet Community"*, heisst es in einer kurz darauf veröffentlichten *Internet Constitution „insure harmonious relations between the various Networks that constitute the Internet, and to secure the Blessings of Liberty to all the Networks that constitute the Internet …"*[21]

Die US-Regierung war nicht bereit, eine solche Unabhängigkeitserklärung hinzunehmen und Ira Magaziner, Clintons Internetbeauftragter, machte dies den potenziellen Deserteuren unmissverständlich klar: *„The United States paid for the Internet, the Net was created under its suspices, and most importantly, everything Jon (Postel) and network Solutions did was pursuant to government contracts."*[22] Jon Postel, der allseits anerkannte Verwalter der *Domain Names*, war machtlos gegenüber Washingtons Druck. Er war Angestellter in dem aus Forschungsmitteln des Pentagon finanzierten *Stanford Research Institute*.

Mit ihrem Anspruch auf *Root Authority* etablierte sich die US-Regierung zum Systemherr des globalen Internet, ohne die Verwaltung des explosionsartig wachsenden World Wide Web mit zu übernehmen. Sie verzichtete darauf, in der 1998 gegründeten und privatrechtlich organisierten *Internet Corporation for Assigned Names and Numbers* (ICANN) formell vertreten zu sein.

Für die Netzaktivisten der ersten Stunde war ICANN zwar nicht die *Internet Governance*, die sie angestrebt hatten. Doch auf die USA als wohlmeinenden, die Freiheit des Netzes verteidigenden Kustoden zu vertrauen, sei immer noch besser – argumentierte

Albrecht Funk

Albrecht Funk ist Sozialwissenschaftler und Mitbegründer des Instituts für Bürgerrechte und öffentliche Sicherheit in Berlin. Er war von 1994-1999 German Academic Exchange Professor an der University of Pittsburgh und lehrt jetzt an der Carnegie Mellon University, unter anderem über Cybersecurity Policies in den USA und der EU.

die Mehrheit der amerikanischen und europäischen Internetgemeinde – als das Internet in der Internationalen Fernmeldeunion zur Beute der Nationalstaaten zu machen.

Das weltweite Vertrauen in die USA als guter Sachwalter einer globalen Informationsökologie haben die Regierungen von Clinton bis Obama verspielt.

Die USA sind sicher nicht der einzige Staat, der mit Hilfe klandestiner Strategien versucht, Schwachstellen vernetzter Systeme zu nutzen oder gar bewusst zu schaffen und für nationale Sicherheitszwecke auszubeuten. Im Gegensatz zu China oder Russland haben die USA jedoch die Rolle eines guten Sachwalters beansprucht: nicht nur als technischer Systemherr der Internetadressen, sondern als Garant einer transparenten, offenen, die Freiheit und Privatheit der Netzbürger stärkenden Informations- und Kommunikationsökologie. Diese Rolle des *Good Steward* für die globale Informationsökologie können die USA nicht mehr für sich beanspruchen.

Für die sogenannten Realisten des internationalen Rechts und der internationalen Politik ist dies keine neue Erkenntnis. *„It´s not just that nations have the power to shape the Internet´s architecture in different ways"*, antworten Jack Goldsmith, *Assistant Attorney General* in der Bush-Administration, und Tim Wu auf ihre rhetorische Frage, wer das Internet kontrolliert.

> *„It is that the United States, China, and Europe are using their coercive powers to establish different visions of what the Internet might be. In so doing, they will attract other nations to choose among models of control ranging from the United States as relatively free and open model to Chinas model of political control. The result is the beginning of a technological version of the cold war, with each side pushing its own version of the Internet´s future."*[23]

An Goldsmiths und Wus Schlussfolgerung geht kein Weg vorbei: Der virtuelle Raum des Cyberspace hat sich in eine reale Kampfzone von Groß- und Regionalmächten entwickelt, in der diese um Vorherrschaft kämpfen. Auch J.P. Barlow, dessen Vision eines von niemandem beherrschten Allgemeinguts *Cyberspace* Goldsmith und Wu als virtuelles Luftschloss zu entlarven suchen, teilt diese Einsicht ausdrücklich.

Realpolitik ernst zu nehmen, bedeutet jedoch nicht, sie hinzunehmen, oder mit naiven Aufrüstungsprogrammen für BND oder Verfassungsschutz schlicht zu untermauern. Realpolitiker sind Gefangene des Machtmythos, des Glaubens, dass machtvoll gesetzte Realitäten keine Alternativen mehr zulassen. Sie übersehen geflissentlich die vielen Situationen, in denen Einzelne, Gruppen, soziale Bewegungen ihr *Recht auf eine nicht vorgezeichnete Zukunft* einfordern.[24] Schon die Geschichte der Territorialstaaten und ihrer Machtkämpfe war immer auch eine Geschichte möglicher Alternativen. Im Cyberspace eröffnen sich Netzaktivisten, kritischen Softwareingenieuren, Hackern, wie normalen Netzbürgern mit der „Leidenschaft für das Mögliche" (Albert O. Hirschman) noch weit größere Chancen alternative Entwicklungspfade durchzusetzen.

Unser globales Informations- und Kommunikationssystem ist zu komplex geworden, um selbst von Hegemonialstaaten wie den USA beherrscht zu werden. Nischen, in denen deren Macht auf Grenzen stößt, leer läuft, Widerspruch hervorruft, sind überall zu finden – wie Snowdens Tätigkeit für die NSA zeigt. Die Möglichkeiten der Vernetzung sind nur schwer unter Kontrolle zu bekommen. Viele der von Staaten entwickelten *Operationen* im Cyberspace lassen sich schnell und ohne größeren Kostenaufwand gegen sie selbst wenden. Und die Chancen staatlicher und ressourcenreicher privater Akteure im Cyberspace, ihren Willen gegen Widerstand durchzusetzen, verflüchtigen sich noch sehr viel leichter, als dies in sozialen Beziehungen generell der Fall ist.

Es bedarf der Mithilfe vieler Gruppen, von der Open-Software-Bewegung bis zu einer sich in den Cyberspace ausdehnenden Menschenrechtsbewegung. Es erfordert auch die Unterstützung von Regierungen, die sich als sichere Verlierer des Wettrüstens der *Cyberwarrior* sehen. Und es setzt schließlich einen politischen Bezugsrahmen voraus, der die nationalstaatlichen Grenzen und die Sicherheitsversprechen nationaler Parlamente, Kontrollkommissionen und Regierungen hinter sich lässt.

In diesem Sinne ist Barlows Aufruf nach wie vor gültig. Wir alle leben in einem neuen Grenzgebiet. Die zukünftige Gestalt dieser *Electronic Frontier* aber wird entscheidend davon abhängen, ob die alten Territorialstaaten in der Lage sind, dieses Gebiet zu dominizieren, bevor sich die Netzbürger darüber klar geworden sind, wie sie es zu ihrem Zuhause machen können. Die Zeit des Abwartens ist vorbei, das ist die zentrale Botschaft der Enthüllungen von Edward Snowden.

Anmerkungen

1 *BBC News, US needs digital warfare force, 5. May 2009 at: http://news.bbc.co.uk/2/hi/technology/8033440.stm*

2 *John Perry Barlow, A Declaration of the Independence of Cyberspace, February 1996, at: https://projects.eff.org/~barlow/Declaration-Final.html*

3 *Vgl. die Übersicht in: Ingo Ruhmann, Ute Bernhardt: Information Warfare und Informationsgesellschaft. Zivile und sicherheitspolitische Kosten des Informationskriegs. In: Wissenschaft und Frieden; FIfF Kommunikation, Heft 1, 2014, Dossier Nr. 74*

4 *Kerry downplays spy scandal as nothing unusual, Euronews, 17.1.2013, at: http://www.euronews.com/2013/07/01/kerry-downplays-spy-scandal-as-nothing-unusual/*

5 *Siehe zu Kerrys „autopilot"-Metaphorik Dan Roberts and Spencer Ackermann, US surveillance has gone too far, John Kerry admits, The Guardian, 1. November 2013, at: http://www.theguardian.com/world/2013/oct/31/john-kerry-some-surveillance-gone-too-far*

6 *Ron Beckstrom, Letter to Secretary Janet Napolitano, March 5, 2009, at: http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf*

7 *Gary McGraw, Proactive defense prudent alternative to cyberwarfare, at: http://searchsecurity.techtarget.com/news/2240169976/Gary-McGraw-Proactive-defense-prudent-alternative-to-cyberwarfare*

8 *Jim Garamone, NSA chief discusses challenges, opportunities of cyberworld, American Forces Press Service, July 11, 2012, at: http://www.defense.gov/News/NewsArticle.aspx?ID=117060*

9 *Welcher Anteil von den 26 Milliarden, die in dennächsten fünf Jahren für Cybertechnologie ausgegeben werden, auf Offensivprogramme*

und- waffen entfällt, ist unklar. Siehe Washington Post, U.S. cyberwarfare force to grow significantly, defense secretary says, March 28, 2014; The New York Times, U.S: Tries candor to assure China on Cyberattacks, April 7 2014

10 *U.S. Department of Defense Directive 5100.20: National Security Agency / Central Security Service (NSA/CSS), January 26, 2010, S. 2; http://www.dtic.mil/whs/directives/corres/pdf/510020p.pdf*

11 *BBC News, US needs digital warfare force, siehe FN 1*

12 *Nach der massiven Aufrüstung der USA für die Kriegsführung im Cyberspace bemüht sich nun Verteidigungsminister Hagel um vertrauensbildende Maßnahmen, die verhindern sollen, dass es zu„ fast escalating series of attacks and counterattacks between the United States and China" kommt. Siehe David E. Sanger, U.S. tries candor to assure China on Cyberattacks, New York Times, 7. April 2014.*

13 *China Daily, Cyber cooperation needed, 22.11.2011, at: http://www.chinadaily.com.cn/opinion/2011-11/22/content_14138092.htm*

14 *So das offizielle Missionstatement der NSA, siehe http://www.nsa.gov/about/mission/index.shtml*

15 *Die Zuständigkeit für Cybersecurity erstreckt sich auf die Bereiche „National Security Information and Information Systems." Siehe zu der Aufgabe „Information Assurance" in der NSA: http://www.nsa.gov/ia/ia_at_nsa/index.shtml*

16 *Vgl.: Ingo Ruhmann, Christiane Schulzki-Haddouti: Kryptodebatten. Der Kampf um die Informationshoheit; in: Christiane Schulzki-Haddouti (Hg.): Bürgerrechte im Netz, Bundeszentrale für politische Bildung, Bonn, 2003, S. 162-177*

17 *Siehe Wendy M. Grossman, Heartbleed Software Snafu: The Good, the Bad and the Ugly, Scientific American, April 16, 2014, at: http://www.scientificamerican.com/article/heartbleed-software-snafu-the-good-the-bad-and-the-ugly/*
Der Überprüfungsprozess sei – so die Sprecherin des National Security Council, C. Hayden – „biased toward responsibly disclosing such vulnerabilities". Mit einer wichtigen Einschränkung: „Unless there is a clear national security or law enforcement need". NSC statement on heartbleed at: http://www.fiercegovernmentit.com/pages/nsc-statement-heartbleed

18 *John M. Pea, The Dangerous Policy of Weakening Security to Facilitate Surveillance, Comments to the Review Group on Intelligence and Communications Technologies, Office of the U.S. Director of National Intelligence, Oct. 4, 2013 at: http://users.ece.cmu.edu/~peha/Peha_on_weakened_secuirty_for_surveillance.pdf*

19 *Stephanie A. DeVos, The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed, in: Fordham Intellectual Property, Media and Entertainment Law Journal, Volume 21, Issue 1, 2011, 198*

20 *Josepf Menn, Secret contract tied NSA and security industry pioneer, Reuters Dec. 20, 2013, at: http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220*

21 *"Comments of the Internet Service Providers Consortium", August 18, 1997, zitiert nach Jack Goldsmith, Tim Wu, Who controls the Internet? Illusions of a borderless world, Oxford 2006, 39f.*

22 *Ebenda, 41*

23 *Ebenda, 184*

24 *"The right to a non-projected future", Albert O. Hirschman, A Bias for Hope: Essays on Development and Latin America, Westview Press, Boulder, CO1985, page 37*

Helge Peters

FIfF-Studienpreis 2013 Sonderpreis

Biopolitische Simulationen

FuturICT und die Regierung des Lebens

Nichts weniger als die Simulation des „Lebens auf der Erde" und von „allem, was damit zusammenhängt" hatten sich die Initiatoren von FuturICT vorgenommen.[1] *Im Zeichen wiederkehrender globaler Krisen versprach FuturICT durch massives Datamining und computergestützte Simulation, Vorhersagekapazitäten zu entwickeln, um die Regierung komplexer sozialer Systeme zu unterstützen. Das von Dirk Helbing (ETH Zürich) federführend verantwortete Forschungsprojekt stand im Rahmen des* Future and Emerging Technologies*-Programms der Europäischen Kommission im Wettbewerb um eine Milliarde Euro an Forschungsgeldern. Letztlich wurden die Gelder zwar an einen Mitbewerber vergeben. Dennoch bleibt das Projekt FuturICT instruktiv. In der FuturICT eigentümlichen Konvergenz von Lebenswissen und Informationstechnologie lässt sich ein biopolitischer Zugriff beobachten, der sich auf die menschliche Gesellschaft als einer lebendigen Entität erstrecken sollte – und das im globalen Ausmaß.*

Wie sich zeigen wird, steht das Leben selbst dabei in dreierlei Weise auf dem Spiel: Nämlich als Gegenstand der Simulation, als Inspiration für die spezifische Simulationstechnologie des Projekts und als Ressource für biomimetische Regierungstechnologien. Schließlich lässt sich angesichts der Verheißungen von FuturICT auch die Frage nach den Grenzen und den politischen Folgen des Objektivitätsanspruchs eines technowissenschaftlichen Zugriffs auf soziale Tatbestände stellen, der durch die digitale Datenschwemme gegenwärtig wieder Konjunktur hat.

Biopolitik als Regierung des Lebens

Mit dem vom Philosophen und Sozialtheoretiker Michel Foucault geprägten Begriff der Biopolitik werden allgemein jene Regierungspraktiken umschrieben, die auf das Leben einer Bevölkerung zugreifen.[2] Etwa mit der Herausbildung moderner Staatlichkeit um 1900 lässt sich eine Vervielfältigung von Praktiken beobachten, mit denen ein Wissen über die Bevölkerung als einer Menge lebendiger Individuen hergestellt und ihre Lebensbedingungen zu regulieren versucht wird: Statistiken über Geburten, Krankheits- und Todesfälle aber auch Kriminalstatistiken machten die Bevölkerung als eine Regelmäßigkeiten aufweisende Menge erfassbar und stellten ein Wissen bereit, das einer Regierungsweise zur Grundlage werden konnte, die weniger das einzelne Individuum mit einem Regime von Verboten einschränkte sondern vielmehr die Bedingungen vorstrukturierte, in denen sich die lebendige Aktivität der Staatsbürger selbsttätig entfalten konnte.

Britta Schinzel übergibt im Rahmen der FIfF-Jahrestagung 2013 den Sonderpreis an Helge Peters
Foto: Benjamin Kees

Abgesehen von diesem Zugriff des modernen Staates auf die biologische Existenz seiner Subjekte, so argumentiert die Philosophin Maria Muhle, zeigt sich in der historischen Genese der Biopolitik ein mimetisches Verhältnis zwischen der Regierung und dem Leben selbst.[3] In dem Maße, wie der Staat seine Bevölkerung als eine lebendige Entität begriff, modellierte er auch seine Regierungspraktiken nach dem Vorbild biologischer Prozesse. Beispielsweise nahmen sich frühe Formen des Wirtschaftsliberalismus physiologische Modelle der Blutzirkulation zum Vorbild, um die Tauschprozesse innerhalb der Gesellschaft frei zirkulieren zu lassen, so dass sich durch die lebendige Aktivität der Wirtschaftssubjekte eine selbst-regulierende Homöostase auf gesellschaftlicher Ebene herstellen könne.[4] Die Vorstellung eines selbsttätig zum Gleichgewicht strebenden Marktes lässt sich damit auch als Ausdruck eines spezifischen historischen Lebenswissens lesen, das mit dem Verweis auf biologische Prozesse ein Funktionsmodell für die Einrichtung von Gesellschaften bereitzustellen suchte.

Stand bis ins frühe zwanzigste Jahrhundert noch der Organismus in seiner Einheit im Fokus der Biologie, so rückte in der Nachkriegszeit mit der Molekularbiologie die im genetischen Code enthaltene Information ins Zentrum der Wissenschaften vom Leben. Das Leben selbst wurde nun als Informationsübertragungsprozess von DNA zur RNA zum Protein in den Blick genommen und der Organismus als ein kybernetisches System verstanden, das gleichsam vom genetischen Code programmiert wird. Dieser Paradigmenwechsel bedingte nicht nur eine rhetorische Entkörperlichung des Lebens durch die Auflösung des lebendigen Organismus in zu dekodierenden Informationen, sondern versprach dadurch auch einen kontrollierenden Zugriff auf das Leben selbst, das sich nun als berechen- und gestaltbar zu präsentieren schien.[5] Wie jedoch der Biologe und Sozialwissenschaftler Nikolas Rose bemerkt, vollzieht sich seit der Jahrtausendwende ein weiterer Paradigmenwechsel hin zu einem postgenomischen Ansatz in den Lebenswissenschaften, der vom genetischen Reduktionismus und seinem Zentraldogma linearer Informationsübertragung vorsichtig abrückend nicht-lineare Funktionszusammenhänge zu verstehen sucht. In den gegenwärtigen Lebenswissenschaften, so argumentiert Rose, rückt die Simulation und Vorhersage komplexer Dynamiken innerhalb verteilter Netzwerke in den Vordergrund.[6] Dabei konvergieren Informatik, Komplexitätsforschung und Lebenswissenschaften nicht zuletzt auf der Grundlage rechnergestützter Simulationsverfahren.

Simuliertes Leben, biomimetische Regierung

Die Simulation und Vorhersage komplexer Dynamiken innerhalb technisch-sozialer Systeme ist das Kernanliegen des FuturICT-Projekts, das sich davon die Unterstützung rationaler Regierungsentscheidungen in einer globalisierten, vernetzten und krisengeschüttelten Welt verspricht. Zentrale Bestandteile, mithilfe derer diese Simulations- und Vorhersagekapazitäten realisiert werden sollen, sind der *Living Earth Simulator* und das *Planetary Nervous System*: Letzteres soll die Daten in einem weltumspannenden Datamining-Verfahren bereitstellen, die von ersterem in Simulationen globaler sozialer Prozesse verarbeitet werden. Beides sind jedoch biologische Metaphern, die somit die Frage aufwerfen, inwiefern ein zeitgenössisches Lebenswissen in den prospektiven Verfahren des FuturICT-Projekts auf dem Spiel steht.

Eine im Projektentwurf an prominenter Stelle verhandelte Simulationsmethode ist das *agent-based modelling (ABM)*. Hierbei wird eine Population künstlicher Agenten in einer simulierten Umwelt platziert, um anhand der Interaktionen zwischen Agenten auf der Mikroebene die sukzessive Emergenz von Strukturen auf der Makroebene studieren zu können. Die ABM-Methode blickt dabei auf eine Geschichte zurück, die eng mit dem Versuch verbunden ist, rechnend auf das Leben selbst zuzugreifen. Unter InformatikerInnen wohlbekannt dürfte dabei das von John Conway entwickelte *Game of Life* sein, das aufbauend auf dem Prinzip zellulärer Automaten die Selbstorganisation komplexer Muster durch simple Interaktionsregeln demonstrierte. Innerhalb der Artificial-Life-Forschung wurde dieser Ansatz fortentwickelt, um schließlich zu behaupten, das Leben selbst sei als emergentes Phänomen zu verstehen, das sich unabhängig seiner spezifischen materiellen Verkörperung – ob in silico oder in vivo – nach denselben Gesetzmäßigkeiten entwickele.[7] In den Sozialwissenschaften schließlich wurde durch die Arbeit von Joshua M. Epstein und Robert Axtell die Methode der agentenbasierten Simulation formalisiert: als *Growing Artificial Societies* wird ein Verfahren vorgestellt, in dem menschliche Gesellschaften in silico gleichsam wachsen bzw. gezüchtet werden, die mit Darwin'schem Anklang als temporär stabilisierte Ergebnisse erfolgreicher Anpassungsstrategien innerhalb eines Verteilungskampfs um knappe Ressourcen erklärt werden.[8] Heutzutage sind ABM auch in der Erklärung des Schwarmverhaltens von Tieren und der Simulation menschlicher Massendynamiken weit verbreitet.[9]

Im Versuch, soziale Prozesse mithilfe agentenbasierter Simulation zu erklären, werden soziale Phänomene wie Konflikte und Krisen als Effekte gleichsam natürlicher Dynamiken in den Blick genommen, die komplexen Systemen eigen seien und Gesetzmäßigkeiten gehorchten, die quer durch natürliche wie soziale Systeme beobachtbar seien. Das darin angelegte Versprechen, soziale Prozesse mit naturwissenschaftlicher Methode erklärbar und schließlich technisch steuerbar zu machen, wird im Projektentwurf von FuturICT an prominenter Stelle expliziert. Die Explosion verfügbarer Datenmengen über menschliches Verhalten im Zuge der sog. Big Data-Revolution wird von den Autoren als

Gelegenheit gesehen, das „objektive Wissen über soziale und ökonomische Systeme zügig zu erweitern“[10] und mit dem Transfer von Supercomputing-Methoden aus den Natur- in die Sozialwissenschaften ein „Sozioskop“[11] zu errichten, mit dem sich gleich einem Mikroskop soziale Phänomene beobachten und experimentell untersuchen ließen. Schließlich ginge es um nicht weniger als die Entdeckung der „fundamentalen Gesetzmäßigkeiten und Prozesse, die Gesellschaften zugrunde liegen“.[12] Die Erklärung sozialer Prozesse als natürliche Dynamiken komplexer Systeme ruft dabei ein technisches Steuerungspotenzial auf, das sich wiederum dem Leben selbst als Wissensressource zuwendet.

So entwerfen die Autoren eine Steuerungsvision, die sich biomimetischen Verfahren zuwendet, um menschliche Gesellschaften zu regieren. Kontrollproblemen in komplexen Systemen, deren nichtlineare Dynamiken den Planungsoptimismus der klassischen Moderne problematisch erscheinen lassen, soll mit biomimetischen bzw. bionischen Steuerungsmechanismen begegnet werden, die, u. a. in Verkehrsplanung und Logistik bereits erprobt, sich etwa metabolische Transportvorgänge auf zellulärer Ebene zum Vorbild nehmen, um damit flexible und adaptive Logiken der Selbstorganisation zu realisieren. Zwar scheint diese Vorgehensweise im Verkehrswesen mit seiner relativ begrenzten Bandbreite sozialer Handlungsoptionen noch schlüssig. Jedoch schwebt den FuturICT-Autoren die Verallgemeinerung biomimetischer Gestaltungsprinzipien auf den politischen Prozess insgesamt vor. Die Projektbeschreibung entwirft eine zukünftige Welt, in der optimale *Policies* mithilfe genetischer Algorithmen generiert und vor ihrer Implementierung innerhalb von Simulationsumgebungen erprobt werden. Ausdrücklich wird hervorgehoben, dieser Regierungsprozess antworte nicht nur auf die in komplexen Systemen enthaltenen Steuerungsprobleme, sondern orientiere sich auch an evolutionären Prinzipien und sei somit besonders erfolgversprechend.[13] Demokratische Willensbildung wird damit suspendiert und der politische Prozess fällt in die Hände von Experten, die vorgeblich natürliche Gesetzmäßigkeiten beobachten und auf ihrer Grundlage steuernd eingreifen. Infolge der Naturalisierung des Sozialen im Zeichen der Komplexität wird somit ein scheinbar entpolitisierter Modus des Regierens entworfen, der lebendige Systeme mithilfe von Technologien steuern soll, die dem Leben selbst entlehnt sind.

Welt außer Kontrolle

Welcher politische, kulturelle und wissensgeschichtliche Kontext muss gegeben sein, in dem die im FuturICT-Projekt entworfene Vision überhaupt plausibel erscheinen kann? Die kulturelle Signifikanz der Komplexitätsforschung befragend, bemerkte die Chemikerin und Literaturwissenschaftlerin Katherine Hayles bereits Anfang der neunziger Jahre, dass sich in der zweiten Hälfte des zwanzigsten Jahrhunderts ein epistemischer Wandel vollzogen habe, der angesichts globaler Krisen wie dem Ölschock die Erforschung von Phänomenen der Instabilität und nichtlinearer Kausalzusammenhänge zwischen lokalen Fluktuationen und global kaskadierenden Effekten in den Fokus rückte.[14] Die hier entworfene Welt tendiert nicht länger selbstregulierend zu den Gleichgewichtszuständen, wie sie noch in der Biopolitik zu Beginn der Moderne vorgestellt wurden, sondern ist immerfort von Schocks bedroht, die steuernde Eingriffe erfordern. Biologische Prozesse stellen hier Funktionsmodelle für Steuerungsmechanismen bereit, die auf eine außer Kontrolle geratene Welt antworten sollen.

Entsprechend werden in der Projektbeschreibung die „großen Herausforderungen der Menschheit im 21. Jahrhundert“ als potenziell katastrophale Krisen vorgestellt, die durch „systemische Instabilitäten und andere ansteckende, kaskadenhafte Prozesse“ ausgelöst werden.[15] Aktuelle politische Krisen wie die Finanzkrise oder die Aufstände gegen die griechische Austeritätspolitik dienen zugleich zur Illustration eines Analyserahmens, der auf nichtlineares Systemverhalten abstellt, und zeigen eine „moralische Verpflichtung“ auf durch „schnellen wissenschaftlichen Fortschritt“ die „Kaskadeneffekte“ [16] zu stoppen, die der „hoffnungslosen Komplexität“[17] einer globalisierten und vernetzten Welt eigentümlich seien. Das visuelle Narrativ von FuturICT unterstreicht diese Figuration einer zugleich lebendigen und lebensbedrohenden, katastrophenträchtigen Welt. Ein in Videos und Illustrationen wiederkehrendes Motiv ist der Planet Erde, wie er vom Weltall gleichsam aus der Gottesperspektive gesehen wird. Als photographisches Produkt des *Space Race* im Kalten Krieg symbolisiert das Bild des ganzen Planeten das Spannungsverhältnis zwischen technowissenschaftlicher Ermächtigung und der Interdependenz und Fragilität irdischen Lebens.[18]

In der Erzählung von FuturICT enthält die Vernetzung der Welt durch Informations- und Kommunikationstechnologien (IKT) zugleich das Risiko der Verstärkung systemischer Instabilitäten und das Versprechen, dieser Instabilitäten durch eine gottgleiche Allwissenheit Herr zu werden. In einem noch vor dem NSA-Skandal publizierten Beitrag spricht Dirk Helbing, führender Kopf des FuturICT-Projekts, vom Potenzial der Proliferation von IKT, eine „Gottesperspektive“ zu ermöglichen, in der die Gesamtheit menschlicher Interaktionen sichtbar wird, und ruft dazu auf, dieses Potenzial für eine effektivere Regulierung komplexer politischer und ökonomischer Prozesse zu nutzen.[19] Erzählungen von bevorstehenden Apokalypsen, die sich jedoch mittels Wissenschaft und Technik abwenden lassen, gehören zum Standardrepertoire moderner Fortschrittsnarrative.[20] Im Hinblick auf den Komplexitätsdiskurs analysiert die Philosophin Isabelle Stengers wiederkehrende Themen wie Instabilität, Krise und Katastrophe als strategische Mittel, um Komplexität als ein neues Paradigma zu etablieren.[21]

Gottestrick und situiertes Wissen

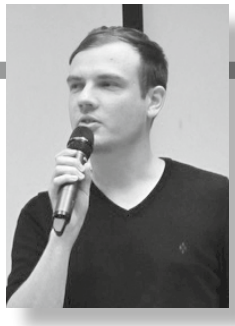
Jedoch birgt diese Vorstellung von naturalisierten techno-sozialen Systemen, die außer Kontrolle geraten zu drohen und nur durch einen allwissenden Blick zu bändigen seien, auch eine geschlechterpolitische Dimension: Traditionell wurde in der westlichen Wissenschaftskultur die Natur als eine ungehörige, instabile und wilde Frau imaginiert, die durch die rationalen Manipulationen der wissenschaftlichen Methode zu bändigen und zu unterwerfen sei.[22] Die wissenschaftliche Methode schließlich wurde mit dem (weißen) Mann identifiziert, der allein eine entkörperlichte, gottgleiche Position reiner Rationalität anzunehmen behauptete. Von feministischen und postkolonialen Stimmen wurde diese von keiner Subjektivität beeinträchtigte und damit objektives Wissen bildende Epistemologie dahingehend kritisiert, dass sie das Wissen weißer Männer als allgemeingültig

setzt, obgleich eine wissenschaftssoziologische Untersuchung der spezifischen Bedingungen (natur-)wissenschaftlicher Wissensproduktion den „Gottestrick" enthüllt, der eine notwendig partielle Perspektive als objektiv und allgemein ausgibt.[23]

Was also mit der Geste der Objektivität gleichsam der zu beherrschenden Natur zugeschlagen wird, verlässt den Raum demokratischer Willensbildung als Aushandlung differenter Interessen und Wissensbestände und wird stattdessen zur Domäne des technischen Managements unbestreitbarer Fakten. Abgesehen von der technischen Machbarkeit eines Großprojekts wie FuturICT, die zu bewerten entsprechend ausgebildeten Fachleuten überlassen sei, mag im Objektivitätsanspruch auch ein zentraler Kritikpunkt an dem Vorhaben liegen. So kommentiert der Komplexitätsforscher Peter Allen im *European Physical Journal*, dass kein Modell alleine einen Konsens stiften kann. Vielmehr bleibe es immer Gegenstand differierender Interpretationen welche gegebene Machtverhältnisse widerspiegeln.[24] Die Frage der Macht steht auch in der Kritik von Isabelle Stengers im Vordergrund, die mit Blick auf den universalwissenschaftlichen Anspruch der Komplexitätsforschung die Unterschiede zwischen physikalischen, biologischen und sozialen Systemen hervorhebt: Während eine Beschreibung aller möglichen Interaktionen in einem physikalischen System prinzipiell denkbar sei, so wiesen schon biologische Systeme ein hohes Maß an Kontingenz auf, welches im Falle sozialer Systeme noch einmal in einem Ausmaß potenziert werde, das es fraglich erscheinen lässt, ob sie sich sinnvoll mit den Mitteln beschreiben lässt, die den Naturwissenschaften zur Verfügung stehen.[25] Kontingenz heißt in diesem Falle auch die Offenheit zur grundlegenden Veränderung historisch stabilisierter (Macht-)Verhältnisse. Wer aber die gegebenen Verhältnisse in einer Gesellschaft als natürliche Gesetzmäßigkeiten technisch zu verwalten trachtet, der stellt diese Verhältnisse zugleich auf Dauer. Gerade Wissenschaftler, die mit der Modellierung komplexer sozialer Phänomene beauftragt sind, trifft damit eine besondere Verantwortung, ihre Wissensproduktion kritisch zu reflektieren. Ein solches situiertes Wissen würde Abstand nehmen von großtechnischen Steuerungsvisionen und sich der Privilegierung des eigenen sozialen Standpunkts eingedenk der Begegnung mit und dem Wissen jener öffnen, die von Krisen und gesellschaftlichen Machtverhältnissen unmittelbar betroffen sind, anstatt sie als Datenpunkte auf Abstand zu halten.

Anmerkungen

1 *Helbing, D. & Balietti, S.: From social simulation to integrative system design, in: European Physical Journal Special Topics 195 (2011), S. 69-100, hier: S. 76. Meine Übersetzung.*
2 *vgl. Foucault, M.: Security, territory, population: lectures at the Collège de France, 1977-78. Basingstoke: 2007.*
3 *Muhle, M.: Eine Genealogie der Biopolitik. Zum Begriff des Lebens bei Foucault und Canguilhem. Bielefeld: 2008.*
4 *Christensen, P.: Fire, motion and productivity: The proto-energetics of nature and economy in Francois Quesnay, in: P. Mirowski (Hg.), Markets read in tooth and claw. Natural images in economic thought, Cambridge, Massachusetts: 1994, S. 249-288.*
5 *Vgl. Kay, L.: Who wrote the book of life? A history of the genetic code. Stanford: 2000. Siehe auch Doyle, R.: On beyond living. Rhetorical transformations of the life sciences. Stanford: 1997.*
6 *Rose, N.: Politics of life itself. Biomedicine, power and subjectivity in the twenty-first century. Princeton: 2007.*
7 *Kember, S.: Cyberfeminism and artificial life. London und New York: 2003.*
8 *Epstein, J. & Axtell, R.: Growing artificial societies. Social science from the bottom-up. Cambridge, Massachusetts: 1996.*
9 *Vehlken, S.: Zootechnologien. Eine Mediengeschichte der Schwarmforschung. Zürich und Berlin: 2012.*
10 *Helbing, D. & Balietti, S.: From social data mining to forecasting economic crises, in: European Physical Journal Special Topics 195 (2011), S.3-68, hier: S. 4. Meine Übersetzung.*
11 *Helbing, D. & Balietti, S.: From social simulation to integrative system design, S. 73. Meine Übersetzung.*
12 *Bishop, S. et al.: The European Future Technologies Conference and Exhibiton 2011. FuturICT: FET Flagship Pilot Project, in: Procedia Computer Science 7 (2011), S. 34-38, hier: S. 34. Meine Übersetzung.*
13 *Helbing, D. & Balietti, S.: From social simulation to integrative system design, S. 86ff.*
14 *Hayles, K.: Chaos bound. Orderly disorder in contemporary literature and science. Ithaca: 1990.*
15 *Helbing, D. & Balietti, S.: From social data mining to forecasting economic crises, S. 3. Meine Übersetzung.*
16 *Siehe http://www.futurict.eu/sites/default/files/docs/files/FuturICT_32p_Project%20Outline%20WITH%20LHS.pdf*
17 *Bishop, S. et al.: The European Future Technologies Conference and Exhibiton 2011. FuturICT: FET Flagship Pilot Project, S. 34. Meine Übersetzung.*
18 *Franklin, S. et al.: Global nature, global culture. London: 2000. Siehe auch: Diederichsen, D. & Franke, A.: The Whole Earth. Kalifornien und das Verschwinden des Außen. Berlin: 2013.*
19 *Siehe http://edge.org/conversation/a-new-kind-of-social-inspired-technology*
20 *Haraway, D.: Modest_Witness@Second_Millennium. FemaleMan_meets_OncoMouse. London und New York: 1997.*
21 *Stengers, I.: Power and invention. Minneapolis: 1997.*
22 *Harding, S.: The science question in feminism. Ithaca 1986.*
23 *Haraway, D.: Situated knowledge. The science question in feminism and the privilege of partial perspective, in: Feminist Studies 14:3 (1998), S. 575-599.*
24 *Allen, P.: Comments by P. Allen on the Visioneer white papers by D. Helbing and S. Balietti European Physical Journal Special Topics 195 (2011), S. 165-186.*
25 *Stengers: Power and invention, S. 74f.*



Helge Peters

Helge Peters studierte Medien- und Kommunikationswissenschaften an der Universität der Künste Berlin sowie am Goldsmiths College, University of London. Zur Zeit ist er wissenschaftlicher Mitarbeiter am Centre for Digital Cultures, Leuphana Universität Lüneburg.

Schwerpunkt Videoüberwachung

Überwachungskameras Autohof in Thüringen, Foto: Dirk Ingo Franke, CC BY

Peter Bittner

Videoüberwachung durchschauen

Strukturen des gesichtslosen Blicks

Ein Blick zurück nach vorn

Der kritische Blick auf Überwachungstechnologien gehört zum FIfF von Beginn an. Das erste Schwerpunktheft zum Thema *Videoüberwachung* (FIfF-Kommunikation 1/2002, siehe Abbildung 1) kam nach längerer Vorarbeit im März 2002 unter dem Motto *„Alle(s) im Bilde …"* (siehe Editorial) heraus – in einer heißen Phase der Diskussion. Kurz darauf initiierten die damaligen SchwerpunktredakteurInnen und einige AutorInnen die Gründung des Arbeitskreises *Videoüberwachung und Bürgerrechte*, der zunächst im FIfF als überregionaler Arbeitskreis seine Arbeit begann. Auf der Konferenz *Safe Privacy* im Juni 2002 öffnete er sich bundesweit und auch Mitwirkenden aus den angrenzenden Ländern. Nach einer Hochphase mit vielen Workshops, Vorträgen, Publikationen, Beratungen, Videoüberwachungsrundgängen etc. entschlief der AK um 2007 (v.a. im Zuge der beruflichen Neuorientierung einiger seiner Mitglieder).

In diese Zeit fallen auch die letzten Versuche disziplinübergreifender Evaluation und die auslaufende Finanzierung von Forschungsprojekten zur Videoüberwachung. Einige *Bürgerrechtsgruppen* – wie das Seminar für angewandte Unsicherheit[1] (SaU, Berlin) – haben überlebt, andere nicht – wie die Leipziger Kamera[2] (Leipzig). Wieder andere nahmen das Thema auf – wie *die*Datenschützer Rhein Main[3] (Frankfurt) – oder wurden kürzlich wiederbelebt – wie unser bundesweiter Arbeitskreis *Videoüberwachung und Bürgerrechte*[4].

Mythen und Wildwuchs

Leider ist die Welt der Videoüberwachung von vielen Mythen geprägt:

1. Sie biete einfache Lösungen für Sicherheitsprobleme.
2. Sie ermögliche eine leichte Überwachung auch unübersichtlicher Räume.
3. Videoüberwachungssysteme seien zentral mit wenig Personalaufwand betreibbar.
4. Die Technik sei erschwinglich und ohne besondere Kenntnisse in Betrieb zu nehmen

Insbesondere im privaten Bereich erleben wir einen kaum einzudämmenden Wildwuchs. Anlagen entstehen, ohne dass die Betreiber sich darum kümmern würden, unter welchen Voraussetzungen Videoüberwachung zulässig ist und welche gesetzlichen Vorgaben dabei einzuhalten sind.[5] Die Orientierungshilfe *Videoüberwachung durch nicht-öffentliche Stellen* bietet auf 20 Seiten ein gut lesbares Kompendium zum Thema. Die dort auf S. 19f abgedruckten Fragen ermöglichen Betroffenen einen strukturierten Kontakt mit Betreibern, wenn man dort nachhakt oder von diesen keine begründeten Ergebnisse der Vorabkontrolle oder keine Einsicht in das zugehörige Verfahrensverzeichnis bekommt. Der überregionale Arbeitskreis *Videoüberwachung und Bürgerrechte* unterstützt mit Partnern Betroffene bei der Aufklärung und Beseitigung von illegaler Videoüberwachung.

Aus dem Inhalt

Die Beiträge dieses Schwerpunkts gehen auf den Workshop *Strukturen des gesichtslosen Blicks – revisited* vom 26. Oktober 2013 im Rahmen der FIfF-Jahrestagung *Cyberpeace – Frieden*

Abbildung 1: Cover der FIfF-Kommunikation 1/2002

gestalten mit Informatik in Siegen zurück, ergänzt um einige eingeladene Beiträge.

Walter Schmidt von der Bürgerrechtsgruppe *die*Datenschützer Rhein Main schildert in seinem Beitrag *Videoüberwachung in Frankfurt am Main* die Erfahrungen mit den Frankfurter Videokameras, die den öffentlichen Straßenraum *bestreifen*. Auch wenn das von der Gruppe initiierte Videokataster für Hessen zunächst gescheitert ist, zeigen die Gespräche mit Betreibern vor Ort nicht nur gelegentlich Wirkung, und eine erhebliche Anzahl von Eingaben bei den zuständigen Aufsichtbehörden haben zur *datenschutz-(rechts)konformen Umgestaltung* oder zum Abbau von Anlagen(-bestandteilen) geführt.

Benjamin Kees argumentiert in seinem Beitrag *Über den Wunsch, Überwachung zu automatisieren*, dass der Ausbau von Videoüberwachung nur auf einen starken, „kaum zu begründenden Glauben an ein Konzept" zurückzuführen sei und bei dessen offenkundigen Schwächen ein Befürworter von Videoüberwachung nur argumentieren kann mit

1. „der Bilderflut, die wegen Personalmangels nicht ausreichend ausgewertet werden könne oder

2. den Unzulänglichkeiten menschlicher Operateure bei der Bildauswertung."

Der „Technikgläubige" sucht folglich nach Computern, die unerwünschtes Verhalten nicht nur erkennen, sondern auch vorhersagen können. Die Folge(-koste)n dieser mit Videoüberwachung verbundenen Automatisierung werden uns unnachgiebig vor Augen geführt.

Auch wenn uns Videoüberwachung in Deutschland schon seit den späten 50er Jahren begegnet, kennen wir erst seit den späten 80er Jahren Formen der rechtlichen Einhegung von Videoüberwachung.[6] Nachdem im Jahr 1989 mit den §§ 12a, 19a Versammlungsgesetz erstmalig ausdrückliche Regelungen für die polizeiliche Anfertigung von Bild- und Tonaufnahmen bei Versammlungen geschaffen wurden, hat es sowohl in technischer als auch in rechtlicher Hinsicht erhebliche Änderungen und Weiterentwicklungen gegeben. Die Grenzen der Nutzung von Kameras (und Drohnen) im Rahmen des polizeilichen Handelns bei Versammlungen beschreibt *Stephan Schindler* in seinem Beitrag *Kamera- und Drohneneinsatz bei Versammlungen*. Man beachte: Mit der Föderalismusreform 2006 ist die Gesetzgebungskompetenz im Versammlungsrecht auf die Länder übergegangen. Da einige Bundesländer eigene versammlungsrechtliche Regelungen erlassen haben, gelten in Deutschland teilweise unterschiedliche Regelungen.

Der Frage der Regulierung von Videoüberwachung durch die EU-Datenschutz-Grundverordnung (EU-DS-GVO) geht *Bernd Seifert* in seinem Beitrag *Nichts Genaues weiß man nicht* mit Bezug auf die parlamentarische Fassung nach. Im März 2014 hat das Europäische Parlament seinen Standpunkt (zum im Januar 2012 von der EU-Kommission vorgelegten Entwurf einer EU-Datenschutz-Richtlinie) verabschiedet. „So begrüßenswert und zugleich diskussionswürdig der Entwurf auch sein mag, einen Schönheitsfehler hat er leider. Er enthält kaum konkrete Vorgaben zur Zulässigkeit der […] Videoüberwachung. […] Dem Rechtsanwender bleibt einstweilen nichts anderes übrig, als die Zulässigkeit einer Videoüberwachung anhand der allgemeinen Vorschriften der EU-DS-GVO zu ermitteln."

Wenn wir schon in einer überwachten Welt leben, dann sollte zumindest unsere Wohnung als Rückzugsraum funktionieren. Wohnen ist „konstitutiv für […] fundamentale Merkmale des Menschseins – wie beispielsweise die ermöglichung von Sozialisation durch die Trennung der Lebenssphären des Privaten und des Öffentlichen". Was passiert aber, wenn der Wohnraum gerade diese Trennung aufgrund der baulichen Bedingungen nicht zulässt? *Jens Gulden* geht dieser Frage und den Folgen minderwertiger Wohngebäude in seinem Beitrag *Privacy in da House* nach und sucht nach Lösungsmöglichkeiten.

Ein kleiner Ausblick

Bei Redaktionsschluss erreichte uns eine spannende Nachricht aus Hessen. Zum 3. April 2014 hatte die Fraktion der FDP einen dringlichen Entschließungsantrag betreffend Videoüberwachung des öffentlichen Straßenraums in den Hessischen Landtag eingebracht. Das Anliegen wurde zur Behandlung in den Unterausschuss Datenschutz verwiesen, der am 15. Mai 2014 über alle Fraktionsgrenzen hinweg und *einstimmig* beschlossen hat, einer widerrechtlichen Überwachung des öffentlichen Straßenraumes durch privat betriebene Überwachungsanlagen eine

Peter Bittner

Peter Bittner ist Grenzgänger zwischen den Disziplinen, er arbeitet in und zwischen Informatik, Wirtschaftswissenschaften, Philosophie und Soziologie. Als wissenschaftlicher Mitarbeiter beschäftigte er sich mit der Ethik und Profession der Informatik, arbeitete zu gesellschaftlichen, politischen und juristischen Fragen der Informatik, zur informationellen Selbstbestimmung und über Überwachungstechniken (mit dem Schwerpunkt auf Videoüberwachung und Biometrie). Viele seiner Arbeiten bündelte er in einem Entwurf einer Kritischen Theorie der Informatik. Er lehrte an den Universitäten TU Kaiserslautern, TU Darmstadt und HU Berlin sowie an der Berufsakademie Berlin. Daneben betreute er Studierende an der Hochschule München. Als IT-System-Berater konfigurierte er ERP-Systeme und entwickelte Betriebs-, Datenschutz- und Sicherheitskonzepte. Als Berater für Betriebsräte kämpfte er für *datenschutzgerechte* IKT-Systeme in den Betrieben und den Beschäftigtendatenschutz. Er war zehn Jahre im Bundesvorstand des FIfF und ist derzeit Mitglied des Beirats.

klare Absage zu erteilen und dem Plenum des Landtages empfiehlt, den o.g. Entschließungsantrag LT-Drs. 19/299 mit den Änderungen aus LT-Drs. 19/421 anzunehmen.

Mit dem Entschließungsantrag ist die ausdrückliche Unterstützung des Landtages für den Hessischen Datenschutzbeauftragten bei seinem Einsatz gegen unrechtmäßige Videoüberwachungsanlagen im öffentlichen Raum verbunden.

Ohne Meldepflicht bzw. Videokataster fehlt allerdings die Datenbasis für eine systematische Bearbeitung.

Hier kommt das ***Projekt ~~Vorab~~Nachkontrolle***[7] des überregionalen Arbeitskreises *Videoüberwachung und Bürgerrechte* ins Spiel. Neben den Aktivitäten regionaler Bürgerrechts- und Datenschutzgruppen (wie *die*Datenschützer Rhein Main) soll es die Betroffenen in die Lage versetzen, sich wirksam gegen widerrechtliche Videoüberwachung im öffentlichen Raum zu wehren.

Um uns über die aktuellen Entwicklungen zum Thema Videoüberwachung auszutauschen, wird es auch auf der FIfF-Jahrestagung *Der Fall des Geheimen – Blick unter den eigenen Teppich* vom 7.-9. November 2014 in Berlin wieder einen Workshop[8] des Arbeitskreises *Videoüberwachung und Bürgerrechte* geben.

Auf eine anregende Lektüre und hoffentlich viele Rückmeldungen zu den Beiträgen.

Mit FIfFigen Grüßen

Peter Bittner

Referenzen

Düsseldorfer Kreis (2014): Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", Stand. 19.02.2014, Version 1.1, Redaktion: Der Landesbeauftragte für den Datenschutz Baden-Württemberg. Abrufbar unter: http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2014/03/OH-V%C3%9C-durch-nicht-%C3%B6ffentliche-Stellen.pdf (zuletzt 19.05.2014)

FIfF-Kommunikation (2002): Lächeln … gleich kommt das Vögelchen. Gedanken zur Videoüberwachung. FIfF-Kommunikation 1/2002. Mit dem Editorial „Alle(s) im Bilde … Gedanken zur Videoüberwachung" von Peter Bittner, Hardy Frehe, Julia Stoll und Jens Woinowski.

Hessischer Landtag (2014a): Dringlicher Entschließungsantrag der Fraktion der FDP betreffend Videoüberwachung des öffentlichen Straßenraums in Hessen, LT-Drs. 19/299 vom 03.04.2014. Abrufbar unter: http://starweb.hessen.de/cgi-bin/webhltlinks.pl?form=/webhlt_links.html&typ=drs&title=Drucksache&nb=19/299 (zuletzt 19.05.2014)

Hessischer Landtag (2014b): Beschlussempfehlung und Bericht des Unterausschusses Datenschutz zu dem Dringlichen Entschließungsantrag der Fraktion der FDP betreffend Videoüberwachung des öffentlichen Straßenraums in Hessen Drucksache 19/299, LT-Drs. 19/421 vom 15.05.2014. Abrufbar unter: http://starweb.hessen.de/cgi-bin/webhlt-links.pl?form=/webhlt_links.html&typ=drs&title=Drucksache&nb=19/421 (zuletzt 19.05.2014)

Anmerkungen

1 *Siehe http://www.unsicherheit.tk*
2 *Siehe http://leipzigerkamera.twoday.net/*
3 *Siehe http://diedatenschuetzerrheinmain.wordpress.com/*
4 *Siehe https://wiki.fiff.de/wiki/AkVue*
5 *Allerdings gibt es auch im öffentlichen Bereich beanstandungswürdige Anlagen, wenn z. B. trotz jahrelangen Betriebs die Vorabkontrollen nicht durchgeführt wurden, (gemeinsame) Verfahrensverzeichnisse fehlen oder man der Hinweispflicht nicht oder nicht ausreichend) nachkommt.*
6 *Mittlerweile regeln etwa 40 Gesetze und Normen den Einsatz von Videoüberwachung.*
7 *Siehe https://wiki.fiff.de/wiki/AkVue*
8 *Siehe https://wiki.fiff.de/wiki/AkVueWShop1411*

Benjamin Kees

Über den Wunsch, Überwachung zu automatisieren

*Wenn Informatiker versuchen, Systeme zu bauen, die Politiker in Science-Fiction-Filmen toll fanden, so schafft den Sprung von der Fiktion in die Realität meist nur die Technik-*Idee *– die Technik-*Kritik *bleibt in der Regel unberücksichtigt.*

Von Hollywood inspiriert …

Hier und jetzt beobachten kann man das an Steven Spielbergs Science-Fiction-Thriller *Minority Report.* Der Film spielt in einer Welt, in der modernste lebenserleichternde Geräte, aber auch Überwachungs-Infrastruktur allgegenwärtig sind. Die Polizeibehörde *Precrime* besitzt das Mittel zur ultimativen Sicherheit. Verbrechen werden vorhergesehen und zukünftige StraftäterInnen ohne weiteren Prozess aus dem Verkehr gezogen. Systematisch wird jedoch der Bevölkerung und sogar den Agenten verheimlicht, dass es zu Fehlern kommt, dass Unschuldige verhaftet werden und Schuldige davonkommen.

Im Film kommen die Vorhersagen von drei hellsehenden, unter Drogen stehenden Kindern, deren Visionen direkt aus den Gehirnen auf Bildschirme übertragen werden. Da diese Art der Lösung nicht in Frage kommt, wird in der echten Welt daran geforscht, wie in Zukunft *Computer* die Voraussagen generieren können. Dazu werden Daten benötigt – viele Daten.

… von der EU finanziert

Eines von vielen dieser IT-Projekte zur Sammlung und Auswertung von Überwachungsinformationen ist das Forschungsprojekt INDECT, das seit Projektbeginn im Jahr 2009 mit fast 11 Millionen Euro von der EU finanziert wurde. Erklärtes Ziel von INDECT ist es, ein System für Sicherheits- und Polizeibehörden zu schaffen, das Informationen aus verschiedensten Quellen zusammenführt. Diese sind neben Überwachungskameras z. B.

auch Gesichtsdatenbanken und Kommunikationsdaten, wie sie bei der Vorratsdatenspeicherung erhoben werden. Außerdem sollen Informationen aus dem Internet ausgewertet werden. Dazu gehört das Interpretieren sozialer Beziehungen und Profile in Diensten wie Facebook und Twitter und auch die Suche nach verdächtigen Inhalten in Foren, Blogs, auf Dateiservern, im Usenet und auf persönlichen Computern [1]. Einerseits sollen diese Datensammlungen als Informationsquelle für Polizeibeamte dienen, andererseits sollen sie von Computern automatisiert und in Echtzeit nach möglichen Gefahren und Auffälligkeiten durchsucht werden und Warnungen generieren.

Man könnte erwarten, dass ein so heikles Forschungsprogramm, das von der EU finanziert wird, Ergebnisse produzieren sollte, die tatsächlich angewendet werden können – unter anderem also mit den Grundrechten vereinbar sind. Um solchen Fragen und der Kritik am Projekt zu begegnen, hat INDECT eine sogenannte Ethik-Kommission eingesetzt. Man muss jedoch feststellen, dass diese Kommission lediglich die Rechtmäßigkeit und Ethik der Forschungs*arbeit* im Blick hat. Verletzungen der Grundrechte und Auswirkungen auf die Gesellschaft, die beim *Einsatz* der Forschungs*ergebnisse* zu erwarten sind, werden rhetorisch umschifft oder ignoriert. In einer Stellungnahme der Europäischen Kommission heißt es kurz: *„Für die genaue Ausgestaltung und den rechtmäßigen Einsatz sind die Benutzer verantwortlich"* [2]. Der Berliner Datenschutzbeauftragte Alexander Dix meint, derartige Projekte *„drohen im Grunde Geld zu verschwenden, wenn die Ergebnisse hinterher nicht rechtskonform angewendet werden können."* Ob solche Überwachungsmaßnahmen zum Einsatz kommen dürfen, hängt unter anderem davon ab, ob sie verhältnismäßig sind: Wie gut sie funktionieren, muss abgewogen werden gegen die Nachteile für Betroffene.

Vom Glauben an zwei vermeintliche Wundermittel

Die *Effektivität* von Videoüberwachung zur Verhinderung von Straftaten und Vandalismus konnte bisher nicht mit Studien nachgewiesen werden. Dass Tausende von Kameras, wie z. B. in London, nicht die erhoffte Sicherheit gebracht haben, liegt meist nicht an der Qualität der Bilder oder fehlenden Aufnahmeperspektiven, sondern am Umgang der Überwachten mit den Kameras: Kriminelle planen die Kameras ein, bei Gewalt im Affekt werden Kameras oft einfach ignoriert; daran kann kein hochauflösendes Objektiv und keine zusätzlich aufgehängte Kamera etwas ändern. Dass der Ausbau von Videoüberwachung trotzdem weltweit vorangetrieben wird, kann nur auf einen starken, kaum zu begründenden Glauben an das Konzept Videoüberwachung zurückgeführt werden. Mit Scheuklappen für die grundsätzlichen konzeptuellen Mankos verbleiben nur zwei Dinge im Problembewusstsein der Befürworter:

1. Die Bilderflut, die wegen Personalmangel nicht ausreichend ausgewertet werden kann und

2. die Unzulänglichkeiten menschlicher Operateure bei der Bildauswertung.

Noch stärker als der Glaube an das Konzept Videoüberwachung scheint der Glaube an Technik zu sein, denn als Lösung der beiden Probleme gilt das von Entscheidern oft unverstandene und überschätze Wundermittel: der Computer. Er soll in den Videobildern nicht nur unerwünschtes Verhalten von Personen erkennen, sondern es auch vorhersagen.

Die Informatik versucht diese Aufgabe so zu lösen: Aus einer Folge von Pixeln (den Videoaufnahmen) soll eine Interpretation und Bewertung der Geschehnisse und letztlich ein Alarm errechnet werden. Dazu werden die bewegten Pixel zu Objekten zusammengefasst und durch Vergleich mit Modellen in Gegenstände und Personen eingeteilt. Bewegungen einzelner Körperteile werden verfolgt, zusammengesetzt und typisiert: Rennen, Werfen, Lächeln. Für komplexere Bewegungen und Interaktionen mit anderen Personen und Gegenständen müssen komplexere Modelle gefunden werden.

Um Vorhersagen zu treffen, kann entweder die Abweichung von vorher definierter *Normalität*, oder die Übereinstimmung mit Modellen unerwünschter oder verdächtiger Geschehnisse gemessen werden. Ein paar Beispiele: Person A hat eine zu 78% aggressive Körperhaltung, Person B weicht beständig dem Sicherheitspersonal aus, Person D weicht vom üblichen Weg vom Check-In zum Gate 24 ab, Person E entfernt sich mehr als 3 Meter von Kinderwagen X, Person F verweilt auf dem Bahnsteig, obwohl bereits alle Linien ein Mal eingefahren sind, Transporter G, der sonst nie in der Gegend gesichtet wird, sondern nur in fragwürdigen Randbezirken, hält direkt vor der Botschaft.

Solche Modelle manuell zu erstellen, ist zeitaufwendig und teuer, daher wird auch die Automatisierung automatisiert. Computern wird beigebracht, selbstständig Modelle zu erstellen. In der Praxis geschieht das so: ein Algorithmus wird mit Videodaten gefüttert und dieser macht sich dann selbst einen Reim auf die Pixel. Präsentiert man ihm 40 Stunden Videomaterial von *normalem* Parkplatz-Geschehnissen, so soll eine Person, die in Stunde 41 von Auto zu Auto schlendert, dem Algorithmus als abweichend auffallen, ohne dass ein Mensch je darüber nachdenken musste, was genau an den vorherigen 40 Stunden *normal* war. Nach diesem Verfahren, so wünscht man sich, sollen für beliebig komplexe Zusammenhänge und Geschehnisse Muster und Modelle erstellt werden.

10 Minuten im automatisiert überwachten Berlin 2023

Schaut man nicht nur auf Bildverarbeitung und künstliche Intelligenz, sondern auch auf wissenschaftliche Veröffentlichungen der Biometrie, Kamera-, Sensor- und Netzwerktechnik, Textanalyse, Flugdrohnen, Datamining und Mensch-Technik-Interaktion, so zeichnet sich anhand der vielen einzelnen Forschungsergebnisse jedoch das Szenario eines Systems ab, das weit über eine bildauswertende Kamera, die einen Alarm auslöst, hinaus geht:

Rebecca Schneider, 187 cm groß, rennt aus nur ihr bekannten Gründen in einem Bahnhofsgebäude entlang. Eine von tausenden über die ganze Stadt verteilten, mit Rechenkapazität und Software ausgestatteten Kameras erfasst Rebeccas Bewegung. Anhand von Rebeccas Proportionen, dem Laufstil und Merkmalen ihrer Kleidung bekommt sie von der Kamera eine Identifikationsnummer zugeordnet und kann so über mehrere Kameras hinweg wiedererkannt werden. Im Vergleich mit zuvor auto-

matisiert gelernten Modellen *normaler* Bewegungen wird ihre Bewegung als auffällig der Stufe #5 klassifiziert und in Kombination mit der ID an einen zentralen Analyseserver übertragen. Stufe #5 führt noch nicht zu einem Alarm, ist aber schon hoch genug, so dass Rebecca genauer vom System beobachtet wird. Die Kameras in ihrer Umgebung beginnen höher aufgelöste Aufnahmen und ein genaues 3D-Modell ihres Körpers und ihres Ganges anzufertigen, für den Fall, dass später etwas passiert und Beweise benötigt werden. Gleichzeitig wird an ihrem Laufstil und Rebeccas Gesicht ihre Identität über den Abgleich mit einer Biometriedatenbank festgestellt. In einem zweiten Schritt werden weitere Informationen von externen Informationsquellen abgefragt und analysiert. Rebecca kommt aus dem *Problembezirk Marzahn*, ihr Facebookprofil verrät, dass sie Mitglied der Facebookgruppe des als *gewaltbereit* geltenden *1. FC Union Berlin* ist. Außerdem hat sie in einem Internet-Forum Begriffe benutzt, die auch in Bekennerschreiben der *militanten Gruppe* verwendet wurden. All dies zusammen übersteigt einen internen Schwellwert des Überwachungssystems für Gefahrenpotenzial. Anhand des gespeicherten Videomaterials wird Rebeccas Laufweg der letzten Stunden zurückverfolgt und festgestellt, dass sie in Charlottenburg (einem Bezirk in dem sich Marzahner statistisch gesehen mit geringer Wahrscheinlichkeit aufhalten) einen kleinen Gegenstand entgegen genommen hat, von einer Person, deren Identifikation per Biometrie wegen Basecap und langem Mantel missglückt. Auch diese Tatsache lässt Rebecca in eine höhere Gefahrenkategorie aufsteigen.

In diesem Moment verlässt Rebecca den Bahnhof in Richtung eines leider noch nicht vollständig mit Kameras ausgestatteten Straßenzuges. Nur ein paar private Kameras von Imbissläden, die an das System angeschlossen sind, liefern hier Bilder. Einer Operateurin, der auf einem riesigen Bildschirm wie in einem Computerspiel der ganze Bahnhof als Modell mit hineinprojizierten Videobildern angezeigt wird, wird vorgeschlagen, der für sie unkenntlich gemachten Person mit der Verdächtigkeitsstufe #7 und einem Gewaltpotenzial von 67% zu folgen, die soeben den beobachtbaren Bereich verlässt. Die Operateurin gibt dem System wegen der zwei überdurchschnittlich hohen Zahlen und der Eiligkeit grünes Licht. Daraufhin wird eine autonome winzige Flugdrohne gestartet, die Rebecca unbemerkt auf ihrem Weg begleitet, um weitere Aufnahmen anzufertigen. Als sie in einen Hauseingang abbiegt und nicht weiter verfolgt werden kann, wird der Vorgang nach einer Weile des Wartens abgebrochen und, weil der Auffälligkeit nichts Ungesetzliches folgte, lediglich ein Vermerk zu Rebeccas ungewöhnlichem Verhalten in der Systemdatenbank abgelegt. Dieser wird bei der Einschätzung einer zukünftigen Situation, in die Rebecca involviert ist, berücksichtigt.

So – oder so ähnlich – gestaltet sich Überwachung in ein paar Jahren, wenn man die einzelnen Komponenten, an denen InformatikerInnen zurzeit forschen, zusammen nimmt. Schon jetzt ist in New York ein System vernetzter öffentlicher, größtenteils aber privater Kameras mit Objekterkennung und Suchfunktion im Einsatz. Es können beispielsweise Anfragen gestellt werden, wie *„zeige alle Menschen in der Nähe der Botschaft, die etwas Rotes tragen"*.

Und was kostet es …

Da beobachtbares Verhalten nicht eindeutig interpretierbar ist und kriminelle Geschehnisse nicht unbedingt beobachtbar sind, kommt es zwangsläufig zu Fehlalarmen und nicht gegebenen Alarmen. Um die Genauigkeit der Alarme zu erhöhen, müssen eher mehr als weniger Daten erhoben und genutzt werden. Diese Notwendigkeit des Datensammelns ist mit den Datenschutzgrundsätzen der Datensparsamkeit und der Zweckbindung nicht vereinbar.

Doch wie das Beispiel *Rebecca Schneider aus Marzahn* zeigt, besteht nicht nur das Problem, dass das Recht auf informationelle Selbstbestimmung gefährdet ist. Es findet auch automatisierte Diskriminierung statt: Rebecca wird nicht nach ihrem *tatsächlichen Verhalten* beurteilt, sondern sieht sich auf Grund von *automatisierter Kategorisierung*, allein schon durch die intensivere Überwachung, einer anderen Behandlung ausgesetzt als etwa Sophia Weidenfeld, 157 cm groß, aus Charlottenburg, die einen Blog übers Strohsternfalten schreibt; die jedoch *ebenfalls* über den Bahnhof rennt. Wissen Rebecca und Sophia über die Überwachung Bescheid, werden sie ihr Verhalten bewusst oder unbewusst an die vermeintlich hinter der Überwachung stehende Norm anpassen. Sie können nicht prüfen, wie die erhobenen Daten verarbeitet werden, wie lange sie wo gespeichert werden und ob vielleicht auch an Orten überwacht wird, wo dies nicht ersichtlich ist. Durch die Möglichkeit der langfristigen Speicherung der erhobenen Daten, die auch Jahre später noch ausgewertet werden könnten, kann es sogar dazu kommen, dass sie an legitimen Geschehnissen wie Demonstrationen nicht teilnehmen, weil sie befürchten, dass die Teilnahme ihnen später von jemandem, der an die Daten gelangt, zum Nachteil ausgelegt wird. Vielleicht würde Sophia ohne solche Befürchtungen statt über Strohsterne über Asylpolitik schreiben.

Benjamin Kees

Diplom-Informatiker und FIfF-Mitglied **Benjamin Kees** hat an der Humboldt-Universität zu Berlin Informatik und Ingenieurpsychologie studiert. Er denkt über die Verantwortung und das Selbstverständnis der Informatik nach und hat geforscht, welche gesellschaftlichen Probleme eine Automatisierung von Videoüberwachung nach sich zieht.
Links zum Thema: *www.algoropticon.de*, Kontakt: *Kees@Algoropticon.de*

Oft wird von Befürwortern solcher Systeme die Funktion der Operateure und Operateurinnen als Legitimation für eine umfangreiche Automatisierung dargestellt. Angeblich sorgen diese dafür, dass Betroffene keiner Beeinträchtigung durch automatisierte Entscheidungen unterworfen sind, wie es die europäische Datenschutzrichtlinie vorsieht. Tatsächlich jedoch sind die Entscheidungsprozesse in einem solchen System so komplex und verarbeiten so viele Informationen, dass die Entscheidungsfindung des Systems und mögliche alternative Interpretationen der Geschehnisse nicht für OperateurInnen nachvollziehbar dargestellt werden können. Hinzu kommt, dass bei Assistenz durch Computer aus psychologischen Gründen eine erhöhte Wahrscheinlichkeit besteht, dass der Empfehlung des Assistenzsystems ohne weitere Prüfung gefolgt wird, zumal wie in Rebeccas Fall, die drohte, außer Sichtweite zu geraten, oft Eile besteht, eine Entscheidung zu treffen.

Während wir also durch Automatisierung von Videoüberwachung eventuell ein nur geringes Maß an Sicherheit gewinnen, greifen wir stark in persönliche Rechte ein und gefährden eine positive gesellschaftliche Entwicklung – Nutzen und Nachteil stehen nicht im Verhältnis.

Wenn derartige Techniken in Europa nicht zum Einsatz kommen dürften und die Investitionen in INDECT und anderen Forschungsbemühungen nicht umsonst gewesen sein sollen, dann müssten die Forschungsergebnisse entweder als Drehbuch-Idee für *Minority Report 2* an Steven Spielberg verkauft werden oder aber exportiert werden in Länder, in denen innovationshemmende Bürgerrechte nicht ganz so genau genommen werden. Eines von beidem ...

Referenzen

[1] Dziech, Andrzej (2009): Präsentationsfolien zu INDECT, SRC'09 – Security R&D Innovations for the Citizens, Stockholm, 29.-30. September 2009. Abrufbar unter: http://www.src09.se/upload/Presentations/Day_1/Sessions-1100-1245/Session-1-Hall-B/Dziech.pdf (zuletzt 10.05.2014).

[2] Europäisches Parlament (2010): Parlamentarische Anfrage E-3190/10 „Indect – Grundrechtecharta Art. 8" von Alexander Alvaro (ALDE), hier: Antwort von Herrn Tajani im Namen der Kommission. Abrufbar unter: http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-3190&language=DE (zuletzt 10.05.2014).

Bernd Seifert

„Nichts Genaues weiß man nicht"

Videoüberwachung in der EU-Datenschutz-Grundverordnung

Im Januar 2012 legte die EU-Kommission als Kernstück ihres Datenschutz-Maßnahmenpakets den Entwurf einer Datenschutz-Grundverordnung (DSGVO)[1] vor. Sie geht damit einen bedeutenden Schritt voran auf dem Weg zu einem einheitlichen Datenschutzniveau in Europa. Im März 2014 hat das EU-Parlament seinen Standpunkt[2] verabschiedet und den Kommissionsentwurf großflächig verändert. So begrüßenswert und zugleich diskussionswürdig der Entwurf auch sein mag, einen Schönheitsfehler hat er leider: Er enthält kaum konkrete Vorgaben zur Zulässigkeit der in der Praxis stetig zunehmenden, gesellschaftlich aber auch zunehmend umstrittenen Videoüberwachung, die mittlerweile alle Lebensbereiche durchdringt. Der folgende Beitrag geht der Frage nach, wie sich die Regelung der Videoüberwachung in der parlamentarischen Fassung der DSGVO darstellt.

„Ein Blick ins Gesetz …"

„… erleichtert die Rechtsfindung." Wenn Juristen – zumindest deutsche – sich auf die Suche nach der sachgerechten Lösung eines Falles begeben und zu diesem Zweck das zur Verfügung stehende Gesetzesmaterial auswerten, dann leitet sie dabei stets diese alte Binsenweisheit, die ihnen gleich im ersten Semester vermittelt wird. Als langjähriger Rechtspraktiker ist man geneigt hinzuzufügen: Das Gesetz erleichtert die Rechtsfindung mitunter sogar ganz *kolossal* – vielleicht nicht immer die Findung des *richtigen* Rechts, aber zumindest die Findung eines vertretbaren Ergebnisses. Gegenstand der Auslegung rechtlicher Bestimmungen ist eben in erster Linie der Gesetzestext, wobei – so zu Recht das Bundesverfassungsgericht[3] – der mögliche Wortsinn des Gesetzes zugleich die äußerste Grenze zulässiger Interpretation markiert. Dort, wo ein hinreichend konkreter Text fehlt, wird es freilich schwierig, den genauen Verlauf dieser absoluten Grenze ausfindig zu machen, jenseits derer eine verfassungskonforme Rechtsfindung zur verfassungswidrigen Willkür mutiert. Hier ist man also gezwungen, die Lösung anhand der zur Verfügung stehenden Generalklauseln und allgemeinen Wertungsprinzipien zu ermitteln.

Während das deutsche Recht unter Berücksichtigung der sehr umfangreichen einschlägigen Rechtsprechung mittlerweile ein einigermaßen konkretes Normprogramm zur Beurteilung der Rechtmäßigkeit einer Videoüberwachung bereitstellt, schweigt sich der Verordnungsentwurf dazu weitgehend aus. Die Textstellen, in denen auf solche Kontrollmaßnahmen überhaupt explizit Bezug genommen wird (so z. B. in Art. 32a Abs. 1 lit. e und Art. 82 Abs. 1c lit. b DSGVO), sind an einer Hand abzuzählen. Dass dies nicht reicht, um wenigstens die juristischen Grenzsteine eines so brisanten Themas in angemessener Art und Weise im Gesetz abzubilden, liegt auf der Hand. Rechtssicherheit – ex ante – für die Betroffenen sieht anders aus.

Was ist (juristisch relevante) Videoüberwachung?

Den Rechtsanwendern bleibt einstweilen nichts anderes übrig, als die Zulässigkeit einer Videoüberwachung anhand der allgemeinen Vorschriften der DSGVO zu ermitteln. Dabei stellt sich zunächst die ganz elementare Frage, welche Fälle der optisch-elektronischen Überwachung – so die Terminologie in Art. 82 Abs. 1c lit. b) DSGVO – die Verordnung überhaupt erfasst. Be-

trachtet man einmal die Diskussionen der an diesem Thema interessierten Kreise insbesondere im Internet, dann läuft man schnell Gefahr, dem Irrglauben zu erliegen, der Entwurf regele die Kontrolle anderer mit einer Kamera mehr oder minder umfassend. Bei näherem Hinsehen ist gerade dies aber nicht der Fall.

Schon der sachliche Anwendungsbereich der Verordnung ist nur dann eröffnet, wenn eine Verarbeitung personenbezogener Daten im Sinne des Art. 2 Abs. 1 DSGVO stattfindet. Zwar definiert Art. 4 Nr. (3) DSGVO den Begriff der Verarbeitung eher großzügig als einen *„mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten"*. Danach wäre die visuelle Kontrolle zunächst einmal nur dann eine relevante Datenverarbeitung, wenn einzelne Menschen in einer zu deren Identifizierung geeigneten Qualität abgebildet oder doch zumindest live am Bildschirm in Augenschein genommen werden. Das hat weiter zur Folge, dass die Installation bloßer Kameraattrappen, die nach deutschem Recht wegen des damit verbundenen psychischen Überwachungsdrucks nicht ohne Weiteres zulässig ist, schon von vornherein aus dem Anwendungsbereich der DSGVO herausfällt, weil hier keine personenbezogenen Daten i.S.d. Art. 4 Nr. (2) DSGVO erhoben werden. Ein schwacher Trost ist in diesem Zusammenhang die Tatsache, dass nach Art. 15 Abs. 1 DSGVO jeder ein Recht darauf haben soll, zu erfahren, ob Daten über ihn oder sie verarbeitet werden. Selbst dieser Anspruch besteht wiederum nur dann, wenn die Überwachungsmaßnahme tatsächlich eine Verarbeitung im Sinne der DSGVO darstellt. So kann sich z. B. der Betreiber einer Kameraattrappe des Auskunftsanspruches mit dem einfachen Argument entledigen, er verarbeite überhaupt keine Daten. Letztlich hat der Gefilmte also nicht einmal die generelle Möglichkeit zu erfahren, ob er tatsächlich beobachtet wurde oder nicht.

Darüber hinaus gilt die Verordnung nur für solche Daten, die zumindest teilweise automatisiert verarbeitet werden (s. Art. 2 Abs. 1 DSGVO). Diese Formulierung ist bereits aus Art. 3 Abs. 1 der EU-Datenschutzrichtlinie[4] bekannt und darf daher entsprechend ausgelegt werden. Durch das Automationserfordernis verengt sich der Anwendungsbereich der Verordnung weiter, denn die bloße Beobachtung mittels Kamera und selbst die Aufzeichnung solcher Bilder ist an sich noch keine *automatisierte* Verarbeitung.[5] Erst dann, wenn sie im Rahmen eines Systems erfolgt, das zwischen Daten verschiedener Personen unterscheiden kann (z. B. durch Koppelung der Bilddaten mit einer Software zur Gesichtserkennung), gelangt eine Videoüberwachung in den Fokus der Verordnung. Zwar erstreckt Art. 2 Abs. 1 DSGVO den Anwendungsbereich auf die Datenspeicherung in Dateien. Das hilft aber nicht immer weiter, denn zum einen müssen Bilddaten dann erst einmal gespeichert werden, so dass auch hier weder die bloße Beobachtung ohne Aufzeichnung noch die Scheinüberwachung ausreicht. Zum anderen muss eine Datei gem. Art. 4 Nr. (4) DSGVO nach bestimmten Kriterien auswertbar sein, was bei einer einfachen Videoaufnahme, der nicht mindestens ein Timecode beigefügt wird, regelmäßig nicht der Fall ist. Von einer generellen Erfassung der optischen Überwachung ist der Verordnungsentwurf daher weit entfernt. Aus deutscher Sicht mag man das noch relativ gelassen sehen, weil subsidiär die Rechtsprechung zum allgemeinen Persönlichkeitsrecht greifen würde, die auch gegen solche Kontrollmaßnahmen einen brauchbaren Rechtschutz bietet. Für diejenigen Bürger anderer EU-Staaten, in denen vergleichbare verfassungsrechtliche Garantien nicht im selben Umfang vorgesehen sind, wäre das natürlich kein tröstlicher Gedanke.

Keine Regel ohne Ausnahme

Selbst dann, wenn eine Überwachungsmaßnahme den Anforderungen der o. g. Definitionen gerecht wird und damit immerhin prinzipiell in den sachlichen Anwendungsbereich der DSGVO fällt, bedeutet das noch nicht, dass die Verordnung im Einzelfall ohne Weiteres Geltung beanspruchen könnte. Zunächst will die EU die von ihr aufgestellten Regeln zwar für an einer Datenverarbeitung beteiligte Dritte, nicht aber für sich selbst gelten lassen (s. Art. 89a Abs. 1 DSGVO). Die Institutionen der EU sind nämlich i.d.R. schon durch die Verordnung 45/2001[6] und die speziell für die Videoüberwachung vom Europäischen Datenschutzbeauftragten entwickelten Leitlinien[7] derzeit einem eigenständigen Datenschutzregime unterworfen, das sich nicht in jeder Hinsicht mit demjenigen der DSGVO deckt. Dieses Problem hat das Parlament zwar erkannt und will der Kommission in Art. 89a Abs. 2 DSGVO aufgeben, diese Vorschriften an den Standard der Verordnung anzupassen. Weshalb dann aber überhaupt zwei Regelwerke erforderlich sein sollten, bleibt offen und zweifelhaft. So könnte es am Ende mit ein wenig praktischer Phantasie doch noch zu dem merkwürdigen Ergebnis kommen, dass die Überwachung eines EU-Gebäudes nach der Richtlinie 45/2001 zulässig ist, die Überwachung eines privaten Bürogebäudes auf der gegenüber liegenden Straßenseite nach der DSGVO aber nicht – oder umgekehrt.

Zu dieser Beschneidung des Anwendungsbereichs gesellen sich in Art. 2 Abs. 2 DSGVO weitere Ausnahmen, z. B. für Tätigkeiten, die nicht dem Unionsrecht unterliegen, und für die Strafverfolgung.[8] Wenn auch diese Beschränkungen zumindest teilweise dem Umstand geschuldet sind, dass die EU eben keine allgemeine Rechtsetzungskompetenz hat, so führen sie doch im

Bernd Seifert

Bernd Seifert ist Rechtsreferent und Datenschutzbeauftragter der Oldenburgischen IHK, Mitglied im Arbeitskreis Datenschutz des Deutschen Industrie- und Handelskammertages (DIHK) sowie Lehrbeauftragter der Carl von Ossietzky-Universität Oldenburg.

Ergebnis dazu, dass der rechtliche „Flickenteppich" europäischer und nationaler Vorschriften, den Jan Philipp Albrecht in seinem Ausschussbericht nicht ohne Grund beklagte[9], gerade im Hinblick auf die Videoüberwachung auch weiterhin Bestand hätte.

Materielle Rechtmäßigkeit visueller Kontrolle

Mit diesen Unzulänglichkeiten mag man sich vielleicht arrangieren können. Viel misslicher ist allerdings, dass auch diejenigen Vorschriften, welche die materielle Rechtmäßigkeit einer Datenerhebung und -verarbeitung und damit das eigentliche Herzstück der juristischen Prüfung einer solchen regeln, die Videoüberwachung weder explizit noch zureichend behandeln. Auch hier muss man sich mit Generalklauseln (insbesondere Art. 5-10 DSGVO) abfinden, was erfahrungsgemäß nicht nur den Laien, sondern gelegentlich auch den Juristen Probleme bereiten dürfte, solange es keine Rechtsprechung gibt, an der man sich orientieren kann. Immerhin sind die dogmatische Konstruktion der Rechtfertigungsgründe und die dabei verwendeten Begrifflichkeiten aus deutscher Perspektive durchaus geläufig. Rechtmäßig ist die Datenverarbeitung nur dann, wenn entweder eine Einwilligung des Betroffenen vorliegt oder die Verordnung selbst sie legalisiert. Im Hinblick auf die Einwilligung hatte der Kommissionsentwurf in Art. 7 Abs. 4 DSGVO in Verbindung mit Erwägungsgrund 34 noch vorsehen wollen, dass diese als Rechtfertigung im Rahmen eines Beschäftigungsverhältnisses wegen vermeintlich strukturell fehlender Freiwilligkeit prinzipiell nicht in Betracht kommen sollte. Weil damit die Einwilligung auch in den Fällen unwirksam wäre, in denen eine Datenverarbeitung für den Betroffenen durchaus vorteilhaft sein kann – beispielsweise eine Videoüberwachung, durch die der auf ihn gefallene Verdacht der Begehung von Straftaten gegen den Arbeitgeber entkräftet werden könnte –, hat das Parlament sich darauf verständigt, die Einwilligung auch im Arbeitsverhältnis zuzulassen, sofern sie freiwillig erteilt wird (Art. 82 Abs. 1b DSGVO). Ob die Parallelen der Regelungstechnik und der Begrifflichkeiten perspektivisch auch zu vergleichbaren Ergebnissen im Einzelfall führen würden, bliebe natürlich abzuwarten, denn die Interpretationshoheit in Zweifelsfragen hätte letztinstanzlich der EuGH, der an die nationale Rechtsprechung beispielsweise des Bundesarbeitsgerichts oder des Bundesverfassungsgerichts in keiner Weise gebunden ist.

Neues aus dem Schilderwald

Die Videoüberwachung hat in aller Regel offen zu erfolgen. Das setzt auch voraus, dass der Betroffene – üblicherweise durch Hinweisschilder – so deutlich und rechtzeitig auf den Umstand der Beobachtung aufmerksam gemacht wird, dass er entscheiden kann, ob er sich dieser aussetzen will (s. § 6b Abs. 2 BDSG). Unterrichtungspflichten kennt auch der Verordnungsentwurf, wobei er sie ganz allgemein anordnet, ohne dabei die Besonderheiten der Videoüberwachung zu berücksichtigen. Schon der Kommissionsentwurf sah in Art. 14 Abs. 1 DSGVO umfangreiche Pflichtinformationen vor, die mangels spezieller Vorschriften grundsätzlich auch für die visuelle Kontrolle gelten müssen. Das Parlament geht noch einen Schritt weiter und schreibt in Art. 13a DSGVO zusätzlich vor, dass dem Betroffenen noch vor der ausführlichen Unterrichtung nach Art. 14 DSGVO standardisierte Informationen unter Verwendung der Piktogramme des neuen Anhangs X zur Verfügung gestellt werden müssen. Ausweislich des Erwägungsgrundes 49 ist das ganze Konzept der Unterrichtungspflichten darauf angelegt, den Betroffenen schon bei der Erhebung der Daten zu informieren, sofern sie direkt bei ihm abgefragt werden. Werden Daten ohne sein Zutun erhoben, was bei der optischen Überwachung der Regelfall ist, dann kann die Information unter bestimmten Voraussetzungen auch nachträglich erfolgen. Sofern kleine oder Kleinstunternehmen Daten nur als Nebentätigkeit verarbeiten, soll nach Art. 14 Abs. 4 lit. ba) DSGVO eine Unterrichtung sogar nur auf Antrag und damit grundsätzlich erst nach der Datenerhebung erforderlich sein.

Das alles passt ersichtlich nicht zu einer vernünftigen Kenntlichmachung der Videoüberwachung. Auch hier rächt sich der Umstand, dass man den Besonderheiten dieser Form der Kontrolle keine eigene Vorschrift gewidmet hat. Nimmt man die Transparenzanforderungen der Art. 13a, 14 DSGVO ernst, dann müsste neben jeder Überwachungskamera künftig ein riesiges Hinweisschild hängen, es sei denn, die Kamera gehört einem kleinen oder Kleinstunternehmen, dessen Videoüberwachung nicht den Hauptgeschäftszweck ausmacht und das deshalb initiativ über gar nichts informieren muss. Woraus sich die unterschiedliche Behandlung großer und kleiner Unternehmen gerade mit Blick auf die Videoüberwachung rechtfertigen sollte, bleibt dabei unklar. Mit dem Argument, eine umfassende Vorabinformation sei im Sinne des Art. 14 Abs. 5 lit. b) DSGVO unmöglich oder nur mit unverhältnismäßigem Aufwand machbar, könnte sich ein Großunternehmen seiner Offenbarungspflicht jedenfalls kaum entledigen, da es durchaus möglich – wenn auch auf Dauer in ästhetischer Hinsicht vielleicht eher fragwürdig – wäre, alle oder zumindest den Großteil der vorgeschriebenen Informationen auf ein Hinweisschild zu drucken.

Kameras am laufenden (Montage-)Band

Für den Bereich der Arbeitnehmerüberwachung sah der Kommissionsentwurf in Art. 82 noch vor, dass die nationalen Gesetzgeber befugt sein sollten, eigene Vorschriften für die Erhebung und Verarbeitung von Beschäftigtendaten „in den Grenzen" der DSGVO zu erlassen, ohne sich dabei sklavisch an deren Normen halten zu müssen. Auch hier konnte die Kommission allerdings die Spielregeln durch Erlass eines delegierten Rechtsaktes nach Art. 82 Abs. 3 DSGVO diktieren. Das Parlament hat diesen Ansatz in zweierlei Hinsicht nachhaltig geändert. Zum einen hat es die Rechtsetzungskompetenz der Kommission dadurch beschnitten, dass diese den Arbeitnehmerdatenschutz erst nach Einholung einer Stellungnahme des Europäischen Datenschutzausschusses regeln darf. Zustimmen muss der Ausschuss danach zwar nicht, denn das Parlament sieht ihn lediglich in einer Gutachterrolle (Erwägungsgrund 129). Bedeutsam ist die Änderung gleichwohl, denn der Datenschutzausschuss ist im Reigen der neuen Kontrollinstanzen ein durchaus beachtlicher Sparringspartner, dessen Einwände die Kommission nicht leichtfertig ignorieren dürfte.

Zum zweiten hat das Parlament die Anforderungen an eventuelle nationale Vorschriften gegenüber dem Kommissionsentwurf nachhaltig konkretisiert und Mindeststandards vorgesehen (Art. 82 Abs. 1c DSGVO). Für die Regelung der Videoüberwachung durch den nationalen Gesetzgeber bedeutet das vor allem, dass die Überwachung nicht öffentlich zugänglicher Teile eines

Unternehmens, die überwiegend der privaten Lebensgestaltung des Arbeitnehmers dienen, insbesondere Sanitär-, Umkleide-, Pausen- und Schlafräumen, unzulässig ist. Gleiches gilt für die heimliche Videoüberwachung, die in jedem Fall verboten sein soll (s. Art. 82 Abs. 1c lit. b DSGVO), wie dies auch die Bundesregierung vor einigen Jahren im ihrem Entwurf eines Beschäftigtendatenschutzgesetzes geplant hatte.[10] Schließlich wird klargestellt, dass die Mitgliedstaaten die Möglichkeit eröffnen können, konkretisierende Datenschutzregeln auch in Kollektivverträgen, d. h. in Tarifverträgen und Betriebsvereinbarungen, vorzusehen.

Unter dem Aspekt der Rechtsklarheit sind diese Ergänzungen zweifellos ein Fortschritt. Vor allem das generelle Verbot verdeckter Videoüberwachung im Betrieb wäre nicht nur aus deutscher Sicht ein echtes Novum. Ob es auch für den Betroffenen in jedem Fall einen Mehrwert hätte, müsste sich in der Praxis erst noch zeigen. Wenn sich ein Arbeitgeber nämlich zum Zweck der Aufklärung von Diebstahl und Unterschlagung im Betrieb in keinem Fall mehr einer auch nur vorübergehenden, räumlich und zeitlich eng begrenzten, verdeckten und mit dem Betriebsrat abgestimmten Videoüberwachung bedienen darf, was nach der Rechtsprechung des Bundesarbeitsgerichts derzeit durchaus machbar ist[11], so bleibt ihm kaum etwas anderes übrig, als entweder das Instrument der *Verdachtskündigung* ausgiebig zu nutzen, und damit vielleicht einen unschuldigen Mitarbeiter zu entlassen, oder jede Straftat zur Anzeige zu bringen. Dann kann nämlich die Staatsanwaltschaft selbst eine Überwachung mit den Mitteln der Strafprozessordnung in Gang setzen. Die Konsequenz für den später in flagranti erwischten Arbeitnehmer wäre aber regelmäßig, dass er nicht nur die Kündigung erhält, sondern – was derzeit mangels entsprechender Anzeige des Arbeitgebers bei Weitem nicht in jedem Fall geschieht – dass er zusätzlich noch vorbestraft wäre. Ob diese ganz praktischen Konsequenzen am Ende für den betroffenen Gesetzesbrecher ein persönlicher Gewinn sind, mag jeder für sich selbst bewerten.

Datenlöschung und Datenportabilität

Der Kommissionsentwurf wollte in Art. 17 ein in der Sache eher fragwürdiges und im Übrigen gerade im Internet praktisch auch gar nicht durchsetzbares generelles „Recht auf Vergessenwerden" einführen. Das Parlament hat diesen Begriff gestrichen und den Anspruch inhaltlich auf die einfache Datenlöschung beschränkt. Auch das in Art. 18 des Kommissionsentwurfs vorgesehene Recht auf Herausgabe von Daten an den Betroffenen in elektronischer Form hat das Parlament konkretisiert und begrenzt. Nach der ursprünglichen Fassung hätte der Betroffene möglicherweise einen Anspruch auf Herausgabe einer Kopie des von seiner Person angefertigten Videos gehabt, was mit einigen Folgeproblemen verbunden gewesen wäre.[12] Demgegenüber stellt Art. 15 Abs. 2a DSGVO jetzt klar, dass nicht die Herausgabe aller, sondern nur solcher Daten verlangt werden kann, die der Betroffene selbst zur Verfügung gestellt hat.

Ausblick

Der Entwurf der DSGVO schlägt auch in seiner vom EU-Parlament beschlossenen Fassung tiefe Schneisen in das Datenschutzrecht der europäischen Mitgliedstaaten. Dennoch regelt er gerade die Videoüberwachung nur unzureichend. Er ignoriert damit eine in der juristischen Praxis und im gesellschaftlichen Alltag außerordentlich wichtige Regelungsmaterie. Sinnvoll ist das nicht – und tragbar auch nicht. Unabhängig davon, aus welcher Perspektive man die Zulässigkeit der optisch-elektronischen Kontrolle betrachten mag – ob aus Sicht der Überwachenden, die naturgemäß ein großes Interesse an möglichst wenig Restriktionen haben, oder aus Sicht der Betroffenen, die ihr Persönlichkeitsrecht geschützt wissen wollen –, es muss jedenfalls eine so konkrete Regelung geschaffen werden, dass alle Beteiligten im Voraus wenigstens in Grundzügen erkennen können, was erlaubt ist und was nicht. Alles andere nutzt am Ende weder dem Überwacher noch dem Überwachten.

Ein solchermaßen belastbares Regelungskonzept zu erstellen, ist originäre Aufgabe des Verordnungsgebers. Er selbst muss die Pflöcke einschlagen. Diese Verantwortung bei der Exekutive, der Aufsicht oder den Gerichten abladen zu wollen, würde sich schon bald nach dem Inkrafttreten einer DSGVO als nicht zu unterschätzender konzeptioneller Fehler erweisen. Einstweilen mag man hier Entwarnung geben, weil der gegenwärtige Entwurf zumindest bis zur Parlamentswahl 2014 nicht mehr verabschiedet wird. Man wird aber davon ausgehen dürfen, dass der EU-Gesetzgeber in der kommenden Legislaturperiode einen neuen Entwurf auf den Weg bringen wird. Bleibt zu hoffen, dass er dann zumindest die wesentlichen Rahmenbedingungen der Videoüberwachung gesetzlich regelt. Um es einmal mit Harry S. Truman auf den Punkt zu bringen: „The buck stops here!"

Anmerkungen

1 *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.1.2012, KOM(2012) 11 endg.*

2 *Sofern nicht anders gekennzeichnet, beziehen sich die Verweise auf den Text des Verordnungsentwurfs im Folgenden auf den vom Parlament am 12.3.2014 in erster Lesung beschlossenen Standpunkt.*

3 *Siehe BVerfG, Beschluss vom 23.10.1985, 1 BvR 1053/82, NJW 1986, S. 1671 (1672).*

4 *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24.10.1995, ABl. EG Nr. L 281 vom 23.11.1995, S. 31.*

5 *Dammann/Simitis, EG-Datenschutzrichtlinie (1997), Art. 3 Erläuterung 3.*

6 *Verordnung (EG) Nr. 45/2001 vom 18.12.2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. EG Nr. L 8 vom 12.1.2001, S. 1.*

7 *Leitlinien des Europäischen Datenschutzbeauftragten zur Videoüberwachung vom 17.3.2010, abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_DE.pdf (letzter Abruf: 10.5.2014).*

8 *Vgl. dazu näher B. Seifert, DuD 2013, S. 650 (651).*

9 *Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) vom 21.11.2013, A7-0402/2013, S. 233.*

10 *Vgl. die Regierungsbegründung zu § 32i Abs. 5 BDSG-E, BT-Drucks. 17/4230, S. 22; dazu ausführlich B. Seifert, DuD 2011, S. 98 (106 f.).*

11 *Siehe dazu zuletzt BAG, Urteil vom 21.11.2013, 2 AZR 797/11, NJW 2014, S. 810.*

12 *Vgl. B. Seifert, DuD 2013, S. 650 (653 f.).*

Stephan Schindler

Kamera- und Drohneneinsatz bei Versammlungen

Einleitung

Nachdem im Jahr 1989 mit den §§ 12a, 19a VersammlG erstmalig ausdrückliche Regelungen für die polizeiliche Anfertigung von Bild- und Tonaufnahmen bei Versammlungen geschaffen wurden, hat es sowohl in technischer als auch in rechtlicher Hinsicht erhebliche Änderungen und Weiterentwicklungen gegeben. Die Digitalisierung und Miniaturisierung der Aufnahmetechnik hat die Anfertigung und Verarbeitung von Videoaufnahmen stark vereinfacht. Damit einher geht ein Ausbau der Videoüberwachung des öffentlichen Raums.[1] Dies soll die öffentliche Sicherheit verbessern, führt aber gleichzeitig zu erheblichen Bedrohungen für die Persönlichkeitsrechte betroffener Personen. Ein zusätzliches Überwachungspotenzial ergibt sich durch den polizeilichen Einsatz unbemannter Luftfahrtsysteme, sogenannter (Video-)Drohnen.[2] Mit entsprechender Kameratechnik ausgerüstet können diese flexibel – und gegebenenfalls unbemerkt – Personen videotechnisch erfassen; so etwa im Rahmen der Demonstrationen gegen den Castortransport im Jahr 2010.[3] Rechtlich hat die Föderalismusreform im Jahr 2006 die Gesetzgebungskompetenz im Versammlungsrecht vom Bund auf die Länder übertragen.[4] Während Berlin, Bayern, Niedersachsen, Sachsen und Sachsen-Anhalt eigene versammlungsrechtliche Regelungen erlassen haben[5], nutzen die übrigen Länder weiterhin das Versammlungsgesetz des Bundes, so dass in Deutschland teilweise unterschiedliche Regelungen gelten.

Der polizeiliche Kamera- und Drohneneinsatz bei Versammlungen wirft verschiedene rechtliche Probleme auf, wovon einige im Folgenden kurz dargestellt werden sollen. Die Ausführungen beschränken sich dabei auf die Anfertigung von Bildaufnahmen bei öffentlichen Versammlungen unter freiem Himmel, da insbesondere der Nutzung von Drohnen in geschlossenen Räumen wohl keine größere Bedeutung zukommt.[6]

Beeinträchtigte Grundrechte

Der Kamera- und Drohneneinsatz bei Versammlungen betrifft zum einen das Recht auf informationelle Selbstbestimmung. Dieses gewährleistet als Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[7] Dem liegt die Annahme zugrunde, dass der (unkontrollierte) Umgang mit personenbezogenen Daten[8], wozu auch Bildaufnahmen gehören können[9], die Persönlichkeitsentfaltung und Selbstbestimmung des Einzelnen beeinträchtigen kann.[10] Zum anderen ist die Versammlungsfreiheit (Art. 8 GG) betroffen[11], mithin das Recht, sich ohne Anmeldung oder Erlaubnis friedlich und ohne Waffen zu versammeln. Versammlungen in diesem Sinne sind *„örtliche Zusammenkünfte mehrerer Personen zur gemeinschaftlichen, auf die Teilhabe an der öffentlichen Meinungsbildung gerichteten Erörterung oder Kundgebung."*[12] Müssen Versammlungsteilnehmer damit rechnen, dass ihre Teilnahme registriert wird, könnte sie das von der Teilnahme abhalten.[13] Dies ist insoweit problematisch, als die Versammlungsfreiheit zu den *grundlegenden Funktionselementen* eines demokratischen Gemeinwesens gehört und den Bürgern die Möglichkeit gibt, jenseits von Wahlen durch gemeinschaftliche Meinungskundgabe auf den politischen Willensbildungsprozess einzuwirken.[14]

Für das Vorliegen eines Grundrechtseingriffs als solches macht es nach vorzugswürdiger Auffassung keinen Unterschied, ob Übersichts- oder Nahaufnahmen gefertigt werden. Übersichtsaufnahmen, zum Beispiel zur Lenkung und Leitung des Polizeieinsatzes, wurden in der Vergangenheit teilweise als nicht grundrechtsrelevant eingestuft, da sie nicht zur Identifizierung von Personen geeignet sind.[15] Beim heutigen Stand der Technik ist eine solche Differenzierung abzulehnen. Regelmäßig können auch auf Übersichtsaufnahmen Personen durch Vergrößerung des betreffenden Bildausschnitts individualisiert werden; jedenfalls aber müssen die Versammlungsteilnehmer jederzeit damit rechnen. Für die Frage des Grundrechtseingriffs ist ebenfalls unerheblich, ob lediglich eine Beobachtung im Kamera-Monitor-Prinzip oder eine Aufzeichnung (Speicherung) der aufgenommenen Bilder stattfindet.[16]

Insoweit mit der Anfertigung von Bildaufnahmen ein Grundrechtseingriff verbunden ist, verlangt der Vorbehalt des Gesetzes (Art. 20 Abs. 3 GG) das Vorhandensein einer gesetzlichen Ermächtigungsgrundlage, die das Handeln der Polizei abdeckt. Diese muss so klar und bestimmt gefasst sein, dass staatliche Maßnahmen für die Bürger vorhersehbar sind, die Verwaltung steuernde und begrenzende Handlungsmaßstäbe vorfindet und den Gerichten eine wirksame Rechtskontrolle ermöglicht wird.[17] Überdies ist das Gebot der Verhältnismäßigkeit zu wahren. Insbesondere darf die Schwere des staatlichen Grundrechtseingriffs nicht außer Verhältnis zum Gewicht der damit verfolgten Ziele stehen.[18] Es soll mithin *nicht mit Kanonen auf Spatzen geschossen werden*. Bildaufnahmen von Versammlungen sind dabei grundsätzlich als durchaus erheblicher Grundrechtseingriff zu werten. Die Aufnahmen können eine große Zahl von Personen betreffen, darunter auch solche, die hierfür keinen Anlass gegeben haben. Hiervon können Einschüchterungseffekte ausgehen und Personen in ihrem Verhalten beeinflusst werden. Auch können die Aufnahmen Aufschluss über politische oder weltanschauliche Auffassungen geben und sind somit als sensibel einzustufen. Zusätzlich erhöht wird das Gewicht bei verdeckter[19] Durchführung und bei Aufzeichnung der Aufnahmen, verringert hingegen bei bloßer Anfertigung von Übersichtsaufnahmen.[20] Jedenfalls bedarf es – nicht zuletzt auch wegen des hohen Rangs der Versammlungsfreiheit – gewichtiger Gründe, um im Rahmen einer Versammlung polizeiliche Bildaufnahmen zu fertigen.

Überdies sind der Überwachung von Versammlungen seitens der Verfassung von vornherein Grenzen gezogen. Insbesondere sieht es das Bundesverfassungsgericht als unzulässig an, durch „exzessive Observationen und Registrierungen" den grundsätzlich staatsfreien Charakter von Versammlungen zu verändern[21],

ohne dass allerdings geklärt ist, wann genau das der Fall ist. Jedenfalls spricht dies für eine grundsätzlich restriktive Handhabung der videotechnischen Überwachung von Versammlungen. Auch darf der unantastbare Bereich privater Lebensgestaltung nicht verletzt werden[22], was bei der Überwachung öffentlicher Versammlungen allerdings eher schwer vorstellbar ist.

Gesetzliche Regelungen

Gesetzliche Ermächtigungen zur Anfertigung von Bildaufnahmen finden sich in den Versammlungsgesetzen des Bundes und der Länder Berlin, Bayern, Niedersachsen, Sachsen und Sachsen-Anhalt. Da somit in den meisten Ländern noch immer das Versammlungsgesetz des Bundes gilt und überdies die Versammlungsgesetze der Länder in der Regel an die bundesgesetzlichen Vorschriften angelehnt sind, soll hier vorrangig das Versammlungsgesetz des Bundes betrachtet werden.[23]

Gemäß §§ 12a, 19a VersammlG darf die Polizei Bild- und Tonaufnahmen von Teilnehmern bei oder im Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen. Die Maßnahmen dürfen auch durchgeführt werden, wenn unbeteiligte Dritte unvermeidbar mitbetroffen sind.

Die öffentliche Sicherheit umfasst insbesondere die Unversehrtheit der Rechtsordnung. Eine Verletzung liegt bei einem Verstoß gegen bestehende Rechtsnormen vor, etwa bei Körperverletzungen, Sachbeschädigungen oder Verstößen gegen versammlungsrechtliche Vorschriften. Öffentliche Ordnung hingegen meint die Gesamtheit ungeschriebener Regeln, deren Befolgung nach den herrschenden sozialen und ethischen Anschauungen als unerlässliche Voraussetzung eines geordneten menschlichen Zusammenlebens angesehen wird.[24] Die öffentliche Ordnung kann beispielsweise gestört sein, wenn eine Versammlung ein nationalsozialistisches Gepräge aufweist, ohne dass dabei gegen Strafnormen verstoßen wird.[25] Eine Gefahr ist bei einer Sachlage gegeben, die bei ungehindertem Ablauf des zu erwartenden Geschehens mit hinreichender Wahrscheinlichkeit zu einer Verletzung der öffentlichen Sicherheit oder Ordnung führt.[26] Die Erheblichkeit der Gefahr ergibt sich aus Bedeutung und Gewicht der bedrohten Rechtsgüter.[27] Es müssen tatsächliche Anhaltspunkte vorliegen, dass eine solche erhebliche Gefahr vorliegt – bloße Vermutungen genügen nicht.

Die Einführung der §§ 12a, 19a VersammlG im Jahr 1989 ist dabei politisch im Zusammenhang mit dem Vermummungsverbot in § 17a Abs. 2 VersammlG zu sehen. Indem Bild- und Tonaufnahmen von Versammlungsteilnehmern nur in Fällen erheblicher Gefahren zugelassen sind, soll dem Einwand, Versammlungsteilnehmer müssten sich zur Verteidigung gegen eine exzessive Überwachung von Seiten der Polizei vermummen, der Boden entzogen werden.[28]

Im Hinblick auf die Anfertigung von Bildaufnahmen bei Versammlungen stellen sich verschiedene rechtliche Probleme. Fraglich ist, ob Gefahren für die öffentliche Ordnung geeignet sind, Eingriffe in die Versammlungsfreiheit zu rechtfertigen. Bezweifelt wird zum einen, dass solche Gefahren überhaupt die geforderte Erheblichkeit erreichen können[29], zum anderen, dass die öffentliche Ordnung gegenüber der Versammlungsfreiheit ein gleichwertiges Schutzgut darstellt.[30] Das Bundesverfassungsgericht allerdings gesteht auch dem Schutz der öffentlichen Ordnung ein hohes verfassungsrechtliches Gewicht zu[31] und sieht bei Verstößen gegen die öffentliche Ordnung sogar ein Versammlungsverbot (§ 15 VersammlG) nicht als schlechthin unzulässig an.[32] Dementsprechend ist die öffentliche Ordnung grundsätzlich geeignet, die Anfertigung von Bildaufnahmen zu rechtfertigen. Hierbei ist von Seiten der Polizei allerdings große Zurückhaltung zu fordern. Auf jeden Fall ist es zu begrüßen, dass die Regelungen in Niedersachsen und Sachsen-Anhalt Bildaufnahmen von Versammlungsteilnehmern nur noch bei erheblichen Gefahren für die öffentliche Sicherheit gestatten.

Fraglich ist auch, inwieweit die Anfertigung bloßer Übersichtsaufnahmen – etwa zur Lenkung und Leitung des Polizeieinsatzes – auf die §§ 12a, 19a VersammlG gestützt werden kann. Da hierin ein Grundrechtseingriff zu sehen ist, bedarf es jedenfalls einer gesetzlichen Grundlage. Der Wortlaut der §§ 12a, 19a VersammlG ist dabei insoweit problematisch, als die Überwachung einzelner Teilnehmer, nicht aber das Filmen der Versammlung als solches gestattet wird. Trotzdem erscheint es rechtlich zulässig, die Anfertigung von Übersichtsaufnahmen hierauf zu stützen, wenn zumindest von einigen Versammlungsteilnehmern erhebliche Gefahren ausgehen; auch vor dem Hintergrund, dass gemäß §§ 12a Abs. 1 Satz 2, 19a VersammlG die Aufnahme Unbeteiligter nicht von vornherein ausgeschlossen ist.[33] Jedenfalls müssen dann aber die Voraussetzungen der §§ 12a, 19a VersammlG, also erhebliche Gefahren für die öffentliche Sicherheit und Ordnung, auch tatsächlich vorliegen. Die Länder Niedersachsen, Berlin, Sachsen und Bayern haben explizite Regelungen zur Anfertigung von Übersichtsaufnahmen erlassen, wobei zum Teil an das Bestehen einer Gefahr, zum Teil an die Größe und Unübersichtlichkeit der Versammlung angeknüpft wird.[34]

Probleme bereitet überdies die Frage, ob die §§ 12a, 19a VersammlG auch das verdeckte Anfertigen von Bildaufnahmen gestatten. Der Wortlaut der Regelungen bezieht hierzu keine Stel-

Stephan Schindler

Stephan Schindler ist wissenschaftlicher Mitarbeiter am Lehrstuhl für öffentliches Recht, Informationstechnologierecht und Rechtsinformatik von Prof. Dr. Hornung, LL.M. an der Universität Passau.

lung. Da die verdeckte Fertigung von Bildaufnahmen gegenüber einem offenen Vorgehen einen intensiveren Eingriff darstellt[35] und die Polizei grundsätzlich offen zu handeln hat[36], ist die Befugnis zur verdeckten Überwachung ausdrücklich zu regeln und daher von den §§ 12a, 19a VersammlG nicht umfasst.[37] Es ist zu befürworten, dass in Niedersachsen, Sachsen und Bayern explizit normiert ist, dass Versammlungsteilnehmer nur offen gefilmt werden dürfen.

Im Hinblick auf die Verwendung von Drohnen ergeben sich zusätzliche Probleme. Weder das Versammlungsgesetz des Bundes noch die Versammlungsgesetze der Länder nehmen ausdrücklich zum Einsatz von Drohnen Stellung. Die maßgeblichen Regelungen besagen lediglich, dass unter bestimmten Umständen Bildaufnahmen angefertigt werden dürfen. Auf die dabei einzusetzende Technik wird nicht näher eingegangen, so dass der Einsatz von Drohnen jedenfalls dann nicht von vornherein ausgeschlossen ist, solange nur Bildaufnahmen gefertigt werden. Zwar sollen nach der Rechtsprechung des Bundesverfassungsgerichts technische Eingriffsinstrumente möglichst genau bezeichnet werden. In einem gewissen Rahmen ist es aber zulässig, auch neue Techniken auf bestehende Ermächtigungsgrundlagen zu stützen.[38]

Zum Teil wird vertreten, dass der Einsatz von Drohnen im Vergleich zur herkömmlichen Videoüberwachung mit einer deutlich höheren Eingriffsintensität verbunden sei[39], so dass die bestehenden Regelungen den daraus erwachsenden erhöhten Anforderungen nicht entsprächen. Dies erscheint aber nicht zwingend. Zwar mögen Drohnen prinzipiell sowohl zur Verfolgung einzelner Personen als auch zur Anfertigung von umfassenden Aufnahmen gut geeignet sein. Jedoch ist dies mittels anderer Techniken, zum Beispiel dem Einsatz von Hubschraubern oder der Nutzung von Kamerafahrzeugen, ebenfalls möglich. Überdies ist die Erkennbarkeit von Menschen aus dem Blickwinkel einer Drohne, mithin aus vertikaler Perspektive, wohl eher gering.[40] In diesem Zusammenhang stellt sich auch die Frage, ob die Bildaufnahme mittels Drohne stets als verdeckte Maßnahme zu werten ist. Auch dies kann nicht pauschal bejaht werden[41], sondern hängt von der konkreten Einsatzsituation ab.[42] Ist die Drohne aufgrund ihrer Größe, ihrer geringen Flughöhe oder ihrer Geräuschentwicklung leicht feststellbar, wird man von einer offenen Überwachung ausgehen können. Ist die Drohne hingegen nicht ohne weiteres erkennbar, zum Beispiel wegen großer Flughöhe und geringer Größe, ist von einer verdeckten Maßnahme auszugehen. Dies muss jedenfalls dann gelten, wenn die Polizei die Drohne bewusst in einer Art und Weise einsetzt, die sie nicht wahrnehmbar werden lässt. Erkennt man an, dass die verdeckte Überwachung einer Versammlung im Regelfall unzulässig ist, muss der Drohneneinsatz daher grundsätzlich in erkennbarer Weise erfolgen.

Vor dem Hintergrund der bestehenden Rechtslage ist die Anfertigung von Bildaufnahmen mittels Drohnen dementsprechend nicht von vornherein ausgeschlossen.[43] Die Bildaufnahme durch Drohnen unterscheidet sich nicht grundlegend von anderen Aufnahmetechniken. Eine gesetzliche Klarstellung – insbesondere wenn der Einsatz von Drohnen in Zukunft zunehmen sollte – erscheint allerdings wünschenswert. Jedenfalls muss der Gesetzgeber die Entwicklung des Drohneneinsatzes bei Versammlungen beobachten, um bei Fehlentwicklungen steuernd einzugreifen.[44] Von überragender Bedeutung für die Praxis ist aber vor allem, dass die Polizei die bereits bestehenden gesetzlichen Beschränkungen beachtet und nicht standardmäßig Bildaufnahmen von Versammlungen fertigt.[45]

Ausblick

In den letzten Jahren wurden große Fortschritte bei der Entwicklung automatisierter biometrischer Erkennungssysteme erzielt, die es in der Zukunft ermöglichen könnten, einzelne Demonstranten etwa mittels Gesichtserkennung in einer Versammlung zu identifizieren.[46] Ob und unter welchen Umständen der Einsatz solcher Systeme rechtlich zulässig ist, ist noch weitestgehend ungeklärt.[47] Ausdrückliche gesetzliche Regelungen existieren bisher nicht.

Anmerkungen

1 *Zum Ausmaß der Videoüberwachung in Deutschland s. z. B. BT-Drs. 17/2750. „Spitzenreiter" bei der Überwachung des öffentlichen Raums ist wohl Großbritannien. Die genaue Zahl der dort eingesetzten Kameras ist nicht bekannt, es sind wahrscheinlich mehr als vier Millionen, s. House of Lords, Surveillance: Citizen and the State, 2009, 20.*

2 *Zu den verschiedenen in Deutschland eingesetzten Drohnentypen s. z. B. BfDI, 24. TB, 52 f. u. BT-Drs. 17/8693. Umfassend zu Technik und Anwendungsmöglichkeiten Kornmeier, Der Einsatz von Drohnen zur Bildaufnahme, 2011, 9 ff. S.a. Weichert, ZD 2012, 501, 501 f.*

3 *Siehe Weichert, ZD 2012, 501, 502.*

4 *Siehe das Gesetz zur Änderung des Grundgesetzes v. 28.8.2006 (BGBl. I S. 2034). Die Bundeskompetenz zur Regelung des Versammlungsrechts wurde aus Art. 74 Abs. 1 Nr. 3 GG gestrichen und steht somit den Ländern zu, Art. 70 Abs. 1, 30 GG. Gemäß Art. 125a Abs. 1 GG gilt das Versammlungsrecht des Bundes solange fort, wie die Länder keine eigenen versammlungsrechtlichen Regelungen treffen.*

5 *Die für die Anfertigung von Bild- und Tonaufnahmen maßgeblichen Vorschriften sind § 1 VersammlG Bln, Art. 9 BayVersG, §§ 12, 17 NVersG, §§ 12, 20 SächsVersG u. § 18 VersammlG LSA. In Schleswig-Holstein wird gegenwärtig über den Erlass eines Versammlungsgesetzes beraten, s. Gesetzesentwurf in LT-Drs. 18/119.*

6 *Drohnen kommt überdies eine luftverkehrsrechtliche Relevanz zu. Siehe hierzu z. B. BfDI, 24. TB, 53 f.; Kornmeier, Der Einsatz von Drohnen zur Bildaufnahme, 2011, 39 ff.*

7 *BVerfGE 65, 1 (43).*

8 *Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, s. § 3 Abs. 1 BDSG.*

9 *Siehe z. B. Lang, BayVBl 2006, 522, 524. Videoaufnahmen können z. B. Angaben über den Aufenthaltsort, die Kleidung oder das Verhalten einer Person enthalten. Ist die Person identifizierbar aufgenommen, können ihr diese Angaben zugeordnet werden.*

10 *Hierzu grundlegend BVerfGE 65, 1 (41 ff.). Ausführlich zum Recht auf informationelle Selbstbestimmung Albers, Informationelle Selbstbestimmung, 2005.*

11 *Zum Verhältnis dieser beiden Grundrechte zueinander s. Koranyi/Singelnstein, NJW 2011, 124, 124; Dietel/Gintzel/Kniesel, Versammlungsgesetz, 16. Aufl. 2011, § 12a, Rn. 2.*

12 *BVerfGE 104, 92 (104).*

13 *BVerfGE 65, 1 (43).*

14 *BVerfGE 69, 315 (343 ff.).*

15 *Z. B. BT-Drs. 11/4359, 17.*
16 *Zur aktuellen Rechtsprechung s. VG Münster, NWVBl 2009, 487; VG Berlin, NVwZ 2010, 1442. S.a. BVerfGE 122, 342 (368 ff.). Das OVG Münster ist hingegen wohl der Ansicht, dass bloßen Übersichtsaufnahmen zur Lenkung- und Leitung des Polizeieinsatzes keine Eingriffsqualität zukommt, OVG Münster, DVBl 2011, 175, 175.*
17 *Zum Bestimmtheitsgebot s. z. B. BVerfGE 110, 33 (53 ff.).*
18 *Zum Verhältnismäßigkeitsgebot s. z. B. BVerfGE 120, 378 (427 f.).*
19 *Hierunter sind Maßnahmen zu verstehen, die für den Betroffenen nicht erkennbar sind bzw. nicht erkennbar sein sollen, s. Petri, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, 768.*
20 *Zu den Kriterien des BVerfG zur Bestimmung des Eingriffsgewichts s. BVerfGE 122, 342 (369 ff.), BVerfGE 120, 378 (401 ff.).*
21 *BVerfGE 69, 315 (349).*
22 *Zum Kernbereich s. BVerfGE 130, 1 (22) m.w.N. Hierzu gehören z. B. Äußerungen innerster Gefühle oder Ausdrucksformen der Sexualität.*
23 *Ein Rückgriff auf die Vorschriften des allgemeinen Polizeirechts ist grundsätzlich nicht möglich. Das Versammlungsrecht ist insoweit „polizeifest". S. Kniesel/Poscher, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, 1146 f.; Koranyi/Singelnstein, NJW 2011, 124, 125. Grundsätzlich möglich ist allerdings die Fertigung von Bildaufnahmen gemäß § 100h Abs. 1 Satz 1 Nr. 1 StPO zur Strafverfolgung, s.a. § 12a Abs. 3 VersammlG.*
24 *Zu den Begriffen s. BVerfGE 69, 315 (352) u. Denninger, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, 192 ff. u. 199 ff.*
25 *BVerfG, NJW 2001, 2069, 2071; BVerfGE 111, 147 (157).*
26 *Denninger, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, 202.*
27 *Dietel/Gintzel/Kniesel, Versammlungsgesetz, 16. Aufl. 2011, § 12a, Rn. 9.*
28 *Dietel/Gintzel/Kniesel, Versammlungsgesetz, 16. Aufl. 2011, § 12a, Rn. 5; Kunert/Bernsmann, NStZ 1989, 449, 455.*
29 *Brenneisen/Wilksen, Versammlungsrecht, 2001, 238.*
30 *Koranyi/Singelnstein, NJW 2011, 124, 125.*
31 *Siehe z.B. BVerfGE 120, 378 (427).*
32 *BVerfGE 111, 147 (156 f.).*
33 *S. Brenneisen/Wilksen, Versammlungsrecht, 2001, 244. Das VG Münster, NWVBl 2009, 487 hat die Frage offengelassen.*
34 *Die Regelungen in Berlin, Bayern und Sachsen orientieren sich dabei an den Aussagen in BVerfGE 122, 342 (372 f.). Zu Zweifeln an der bayerischen Regelung s. Koranyi/Singelnstein, NJW 2011, 124, 127.*
35 *Siehe oben Die höhere Eingriffsintensität wird vor allem damit begründet, dass dem Betroffenen hierdurch vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz zumindest erschwert wird, BVerfGE 120, 378 (402 f.). Umgekehrt könnte man natürlich auch argumentieren, dass gerade von offenen Überwachungsmaßnahmen erhöhte Einschüchterungs- und Abschreckungseffekte ausgehen.*
36 *BVerfGE 133, 277 (328).*
37 *Koranyi/Singelnstein, NJW 2011, 124, 127. Für ungeklärt erachten dieses Problem Dietel/Gintzel/Kniesel, Versammlungsgesetz, 16. Aufl. 2011, § 12a, Rn. 4.*
38 *BVerfGE 112, 304 (316).*
39 *So Weichert, ZD 2012, 501, 503.*
40 *Siehe Weichert, ZD 2012, 501, 502.*
41 *So allerdings BfDI, 24. TB, 54.*
42 *Siehe auch Kornmeier, Der Einsatz von Drohnen zur Bildaufnahme, 2011, 147 f.*
43 *Kritisch BfDI, 24. TB, 52. Weichert, ZD 2012, 501, 503 fordert für den staatlichen Einsatz von Beobachtungsdrohnen eine ausdrückliche gesetzliche Regelung. Die niedersächsische Landesregierung hält die §§ 12a, 19a VersammlG für geeignet, den Einsatz von Beobachtungsdrohnen zu tragen, s. Plenarprotokoll 16/71, 8949.*
44 *Zur Beobachtungspflicht des Gesetzgebers s. BVerfGE 112, 304 (316 f. u. 320); BVerfGE 113, 29 (58).*
45 *Siehe Koranyi/Singelnstein, NJW 2011, 124, 128.*
46 *Siehe Bericht zum Forschungsprojekt des BKA, Gesichtserkennung als Fahndungshilfsmittel – Foto-Fahndung, 2007.*
47 Zur Biometrie s. z. B. Gundermann/Probst, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 9.6.

Jens Gulden

Privacy in da House

Bedrohung von Privatsphäre durch minderwertige Wohngebäude

Nicht-technische Überwachung

Die zunehmende Durchdringung des menschlichen Lebens mit Technologie und die Entwicklung sozio-technischer Infrastrukturen, die die orts- und kontextungebundene Anwendung von Technologie zu einem wesentlichen Baustein der Lebensgestaltung haben werden lassen, haben zu einer Sensibilisierung und Intensivierung des Diskurses um den Schutz von Privatsphäre und Menschenwürde vor Überwachung geführt [1, 2].

Den nachfolgenden Ausführungen liegt die Annahme zugrunde, dass durch die zunehmende Konfrontation des Einzelnen mit Verletzungen der Privatsphäre in Folge von Technologieanwendungen die Hemmschwelle für die Verletzung der Privatsphäre anderer geringer wird. Dadurch besteht die Gefahr, dass zunächst nur abstrakt erlebte Menschenrechtsverletzungen, z. B. die Verletzung des Schutzes eigener Daten, Ausgangspunkt für eine selbstverstärkende Ausweitung von Privatsphäre-Verletzungen werden und in fundamentalere Lebensbereiche sedimentieren, in denen Grundlagen der physischen und psychischen Existenz von Menschen bedroht sind.

Mit der Weiterentwicklung ethischer und juristischer Ansprüche an den Schutz von Privatsphäre und Menschenwürde dürfen daher neben den Gefahren, die aus der Anwendung neuer Technologien und sozio-technischer Infrastrukturen entstehen, auch grundlegende Schutzbedürfnisse des Menschen, die nicht erst mit der Anwendung von Technologie gegeben sind, nicht aus dem Blick geraten. Der vorliegende Text nimmt speziell das Problem fehlender Privatsphäre in Mehrparteienwohnhäusern in den Blick, das sich auf der Grundlage unzureichender bautechnischer Praktiken und Regularien [3] als ein exemplarisches Beispiel für sich zuspitzende gesellschaftliche Konflikte zeigt, die durch unzureichende Anpassungen gesellschaftlicher Normen an veränderte

technische und soziale Rahmenbedingungen entstehen. Es ist ethisch geboten, diese Konflikte zu identifizieren und Lösungsvorschläge aufzuzeigen. Beides sind Ziele des vorliegenden Texts.

Wohnen als genuin menschliche Tätigkeit

Neben der Fähigkeit zu sprechen ist Wohnen eine genuin menschliche Tätigkeit, die Menschen nicht nur von Tieren unterscheidet, sondern konstitutiv ist für weitere fundamentale Merkmale des Menschseins, wie beispielsweise die Ermöglichung von Sozialisation durch die Trennung der Lebenssphären des Privaten und des Öffentlichen [4, 5]. Auf diesen ethischen Grundpfeilern fußen im Konkreteren juristisch formulierte Ansprüche in den Verfassungen und Grundgesetzen westlicher Demokratien auf die Konstitution menschlicher Würde, die freie Entfaltung der Persönlichkeit, sowie die Realisierbarkeit weiterer Grundrechte.

Ermöglicht ein Gebäude es nicht, die fundamental notwendige Trennung von Öffentlichkeit und Privatsphäre zu realisieren, kann nach heutigem Verständnis nicht von *Wohnraum* gesprochen werden, selbst dann nicht, wenn solche Gebäude früher schon einmal legal am Markt zur Vermietung oder zum Verkauf als Wohnraum angeboten wurden.

In der Tat allerdings stellt sich heraus, dass je nach Wohnlage innerhalb Deutschlands gravierende Unterschiede in der durchschnittlichen Qualität der Wohngebäude bestehen. Um beispielsweise die Produktion von Waffen gegen Ende des Zweiten Weltkriegs zu unterbinden, wurden Industriestandorte in Nordrhein-Westfalen wie das Ruhrgebiet oder das Siegerland intensiv bombardiert und neben den militärischen Zielen auch bestehende Wohnraumsubstanz vernichtet. Nach dem Krieg wurden diese Schäden so schnell wie möglich geflickt. Die Folge ist ein in manchen Gebieten dominierender Gebäudetypus aus Plattenbauten der primitivsten Art, die ohne jeden Anspruch auf Nachhaltigkeit und langfristige Nutzbarkeit errichtet wurden, und die aus heutiger Perspektive nur noch als provisorische Gebäude bezeichnet werden können. In diesen Gebäuden sind normale Gespräche ohne Weiteres durch Wände zu hören. Geräusche von Fernsehern, das Klappern von Besteck, quietschende Betten, Toilettenspülungen, usw., werden mit Nachbarn sowohl in seitlich angrenzenden Wohnungen als auch darüber- und darunterliegenden Etagen geteilt. Dies führt zur Auflösung der Privatsphäre und zu schweren psychischen Belastungen und Verletzungen der Menschenwürde der Bewohner, weil ein ständiges Bewusstsein für die Möglichkeit, überwacht zu werden, das menschliche Verhalten einschränkt und verändert [6].

Folgen minderwertiger Wohngebäude

Die Auswirkungen auf das Leben der Bewohner von derartigen Gebäuden sind enorm. Es wird unmöglich, ein eigenständiges, selbstbestimmtes Berufs- und Privatleben in der eigenen Wohnung zu führen, weil jede Handlung potenziell mit der akustischen Anteilnahme von Nachbarn verbunden ist. Die starke Diversifizierung von Lebensmodellen in den vergangenen Jahrzehnten und eine erhöhte Intoleranz gegenüber (Anders-)Denkenden insbesondere in bildungsfernen Bevölkerungsgruppen [7] führen in derartigen Wohnkonstellationen mitunter zu gefährlichen Vernichtungskämpfen. Da nahezu jede Aktion durch Fremde sowohl passiv belauscht, wie auch aktiv beeinflusst oder kommentiert werden kann, sind der Erniedrigung Schwächerer, beispielsweise alleinstehender Berufstätiger, Tor und Tür geöffnet.

Sobald sich eine Wohnpartei dafür entscheidet, destruktiv in das Leben eines anderen Hausbewohners einzugreifen, sind diesem Verhalten auf Grund der minderwertigen Gebäudequalität keine Grenzen auferlegt. Das Leben des Betroffenen wird nicht nur punktuell beeinflusst, sondern in breitem Spektrum beschädigt: Feindselige Nachbarn können nicht nur Telefongespräche mithören, Berufsgeheimnisse erfahren oder politische Präferenzen mithören. Sie haben, wenn gewünscht, Anteilnahme an der Verdauung anderer Menschen beim Toilettenbesuch oder an sexuellen Intimitäten. Spätestens mit letzterem Punkt ist eine Grenze der Perversion überschritten, die die Verwendung von minderwertiger Gebäudesubstanz zur Wohnraumnutzung als unmenschlich und widernatürlich nachweist und damit Gegenmaßnahmen ethisch geboten macht.

In den Jahren, in denen die im Kern bis heute gültigen Regularien bezüglich Schalldämmung von Wohngebäuden erstellt wurden, gab es kein Telefonbanking mit gesprochenen Passwörtern, und es gab keine telefonisch mitgeteilten Kreditkartennummern. Die Kategorie von Schäden, die durch ungeschützte Verbreitung derartiger Informationen entstehen, und die heute unter anderem mit dem Begriff *Identitätsdiebstahl* [8] beschrieben werden, war damals nicht denkbar. Auch die Nutzung von Radio, Fernsehen, Stereoanlagen etc., die heute zur normalen Lebensgestaltung erwachsener Bürger gehören, war, wenn überhaupt, nur eingeschränkt absehbar. Ohne ausreichend schallgedämmte Wohngebäude können diese Kulturgüter allerdings nicht im vorgesehenen Ausmaß genutzt werden, weil sonst Andere ungewünscht involviert oder gestört werden. Zusammenfassend lässt sich also feststellen, dass mangelhafte Schalldämmung von Wohnraum aus heutiger Bewertung die Teilnahme am wirtschaftlichen und kulturellen Leben in unvertretbarer Weise ein-

Jens Gulden

Dr. **Jens Gulden** ist Wirtschaftsinformatiker und Philosoph. Er forscht und lehrt an der Universität Duisburg-Essen, nachdem er zuvor schon an der Freien Universität Berlin, der Technischen Universität Berlin und der Universität Siegen tätig war. Seine Forschungsthemen orientieren sich an der Untersuchung der Beziehungen zwischen menschlichem Denken und computergestützter Informationsverarbeitung, insbesondere ist er im Bereich konzeptueller und grafischer Modellierung von sozio-technischen Systemen verankert.

schränkt, und daher auch aus dieser soziologischen Perspektive grundlegende Veränderungen am Status Quo geboten sind.

Einer besonderen Gefahr sind Berufstätige mit akademischen Berufen ausgesetzt. Wer sich zur Ausübung einer kreativen Tätigkeit konzentrieren und Gedanken zu Hause ins Unreine sprechen möchte, hat wenig Chancen auf eine erfolgreiche Ausübung seiner Tätigkeit, wenn aggressiv gesinnte Nachbarn dies belauschen und kommentieren. Man stelle sich beispielsweise die Situation eines Software-Architekten vor, der sich Gedanken macht, wie ein objekt-orientieres Softwaresystem sinnvoll in Ober- und Unterklassen strukturiert werden kann, während gleichzeitig in der Nebenwohnung eine Gruppe politischer Aktivisten wilde Klassenkampfphantasien entwickelt, in Reaktion auf die als Reizworte interpretierten Begriffe *Oberklasse* und *Unterklasse*.

Baurechtliche Regularien

Die gegenwärtige Gesetzeslage und die nach wie vor gültigen baurechtlichen Regularien stehen deshalb nachvollziehbar in der Kritik. Vorliegende Arbeiten [3, 9, 10] kritisieren die fehlende Berücksichtigung der Grundbedürfnisse von Gebäudebewohnern insbesondere durch die als unzureichend bewerteten gesetzlichen Mindestanforderungen der DIN 4109 [11] sowie den in der Rechtsprechung üblicherweise vorzufindenden Rekurs auf ausschließlich baurechtliche Vorschriften, wenn versucht wird, Kompensation für entstandene Schäden in Folge von Privatheitsentzug gerichtlich einzuklagen. Einen Überblick über die Spannbreite unterschiedlicher Qualitätsstufen von Schalldämmungsverfahren gibt die nachfolgende Tabelle, die aus der VDI Richtlinie 4100 [12] stammt. Diese Richtlinie behandelt Maßnahmen zur Erreichung von Schalldämmung im Hochbau und führt dazu unter anderem eine in drei Stufen gegliederte Staffelung von Schalldämmungsgraden ein, die so genannten Schallschutzstufen (SSt). Sogar die in der Tabelle aufgeführte Schallschutzstufe II ordnet Gespräche in normaler Lautstärke lediglich als in angrenzenden Wohneinheiten „nicht verstehbar", und nicht als „nicht hörbar", ein. Die Schallschutzstufe I beschreibt das Niveau der gesetzlichen Mindestanforderungen der DIN 4109, die normal gesprochene Sprache im besten Fall als „im Allgemeinen nicht verstehbar" einordnet, alle weiteren Arten des Sprechens schon als „verstehbar" oder „im Allgemeinen verstehbar". Dies kann vor dem Hintergrund der oben identifizierten ethischen Anforderungen an menschlichen Wohnraum nicht als ausreichend hingenommen werden.

Der Rekurs auf ausschließlich baurechtliche Aspekte bei der Beurteilung eines angemessenen Schalldämmungsniveaus von Wohngebäuden, wie er bisher von Gerichten vollzogen wird [3], ist methodisch unangemessen. Das Baurecht erhebt nicht den Anspruch, die Einhaltung von Grundsätzen der Menschenwürde beim Wohnen sicherzustellen, stattdessen regelt es gemäß seiner Zielsetzung baustatische Fragen, die beim Errichten von Gebäuden zu berücksichtigen sind. Dabei handelt es sich um kategoriell andere Fragestellungen als sie bei einer umfassenderen Betrachtung des Themas vor dem Hintergrund der Realisierung einer menschenwürdigen Existenz zu stellen sind.

Lösungsvorschläge

Aus der ethischen Überlegung heraus, dass bei Gebäuden, die keine Trennung zwischen Öffentlichkeit und Privatsphäre zulassen, nach heutigem Verständnis nicht von *Wohnraum* gesprochen werden kann (siehe zweiter Abschnitt), ergibt sich zunächst die Empfehlung, ein sensibleres öffentliches Verständnis für die Existenz von Problemimmobilien der beschriebenen Art und der Nöte ihrer Bewohner zu schaffen. Dies führt in einem ersten Schritt zumindest dazu, dass Betroffene besser Gehör finden und ihre Notsituation nicht aus Unkenntnis heraus banalisiert wird. In gleicher Weise warnt das öffentliche Thematisieren diejenigen Menschen, die vor einem Wohnungswechsel stehen, in besonderer Weise auf angemessene Schalldämmung zu achten und keine Miet- oder Kaufverträge über Immobilien abzuschließen, die die Mindestanforderungen an menschenwürdiges Wohnen nicht erfüllen können. Neben den Mietervereinen sind bei der Umsetzung vor allem Menschenrechtsorganisationen und Initiativen von Privacy-Aktivisten gefragt, in deren Rahmen auch dieser Text entstanden ist.

Art der Geräuschemission	**Wahrnehmung der Geräusche aus der Nachbarwohnung, abendlicher Grundgeräuschpegel von 20 dB(A) vorausgesetzt**		
	SSt I	SSt II	SSt III
Laute Sprache	verstehbar	im Allgemeinen verstehbar	im Allgemeinen nicht verstehbar
Sprache mit angehobener Sprechweise	im Allgemeinen verstehbar	im Allgemeinen nicht verstehbar	nicht verstehbar
Sprache mit normaler Sprechweise	im Allgemeinen nicht verstehbar	nicht verstehbar	nicht hörbar
Gehgeräusche	im Allgemeinen störend	im Allgemeinen nicht mehr störend	nicht störend
Geräusche aus haustechnischen Anlagen	unzumutbare Belästigungen werden im Allgemeinen vermieden	gelegentlich störend	nicht oder nur selten störend
Hausmusik, laut eingestellte Rundfunk- und Fernsehgeräte, Parties	deutlich hörbar		im Allgemeinen hörbar

Tabelle: Wahrnehmung von Geräuschen aus Nachbarwohnungen und Zuordnung zu drei Schallschutzstufen (SSt). (VDI 4100 Tabelle 1 und E-DIN 4109-10 Tabelle A 1, wiedergegeben nach [13])

Unterstützend sollte die Gesetzeslage so angepasst werden, dass Marktmechanismen stimuliert werden, die langfristig zum Verschwinden minderwertigen Wohnraums führen. Hier ist insbesondere eine ethisch motivierte Überarbeitung baurechtlicher Regularien geboten (siehe dritter Abschnitt), die menschliche Grundbedürfnisse gemäß den Grundsätzen unserer konstitutiven Gesetzesnormen wesentlich stärker berücksichtigt. Darüber hinaus sollte ein Recht auf menschenwürdigen Wohnraum, das sich implizit aus den Menschenrechtsartikeln des Grundgesetzes ergibt, durch ein Einzelgesetz explizit einklagbar gemacht werden sowie die Idee des zivilrechtlichen Schadensersatzes für den Entzug von Privatsphäre eingeführt werden. In schweren Fällen sollte der Entzug von Privatsphäre in Wohngebäuden als Form von Folter strafrechtlich geahndet werden. Kurzfristigere Lösungsansätze scheinen nicht sinnvoll zu sein, denn ein unverzügliches Verbot minderwertigen Wohnraums z. B. in Deutschland würde in Gebieten mit hohem Anteil von Alt- und Nachkriegsbauten über Nacht einen erheblichen Prozentsatz der zur Verfügung stehenden Wohnquartiere illegalisieren, für die kurzfristig kein Ersatz bestünde. Damit wäre niemandem geholfen. Gangbar erscheint daher nur eine langsame Gesundung des Wohnungsmarktes, für deren Erreichung die oben genannten Maßnahmen realisierbar erscheinen.

Referenzen

[1] Zurawski, Nils (Hg.): Überwachungspraxen – Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle. Budrich UniPress, Leverkusen, 2011.

[2] Trojanow, Ilija; Zeh, Juli: Angriff auf die Freiheit: Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte. dtv, München, 2010.

[3] Moll, Wolfgang: Schallschutz nach DIN: Es geht auch besser. In: Beratende Ingenieure, Jg. 38, Nr. 1/2, Verband Beratender Ingenieure VBI, Berlin, 2008.

[4] Arendt, Hanna: Vita activa oder vom tätigen Leben. Piper, München Zürich, 2002.

[5] Gerhardt, Volker: Öffentlichkeit: Die politische Form des Bewusstseins. C. H. Beck, München, 2012.

[6] Gulden, Jens: Videoüberwachung in der menschlichen Lebenswelt. In: Koschke, Rainer; Herzog, Otthein; Rödiger, Karl-Heinz; Ronthaler, Marc (Hg.): INFORMATIK 2007 – Informatik trifft Logistik, Köllen Druck+Verlag, Bonn, 2007.

[7] Zick, Andreas; Küpper, Beate; Hövermann, Andreas: Die Abwertung der Anderen: Eine europäische Zustandsbeschreibung zu Intoleranz, Vorurteilen und Diskriminierung. Friedrich-Ebert-Stiftung, Berlin, 2011.

[8] Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph: Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche und technische Aspekte. Springer, Berlin, 2011.

[9] Ertel, Hanno; Moll, Wolfgang: R'w oder DnT,w? Überlegungen zur Kennzeichnung des Schallschutzes und Konsequenzen für eine Neufassung von DIN 4109. In: Bauphysik, Heft 2, Ernst & Sohn, Berlin, 2007.

[10] Deutsche Gesellschaft für Akustik e. V.: DEGA Empfehlung 103: Schallschutz im Wohnungsbau – Schallschutzausweis. März 2009, http://www.dega-akustik.de/publikationen/DEGA_Empfehlung_103.pdf

[11] Deutsches Institut für Normung: DIN 4109:1989-11, Schallschutz im Hochbau; Anforderungen und Nachweise. Beuth, Berlin, 1989.

[12] Verein Deutscher Ingenieure: VDI 4100:2012-10, Schallschutz im Hochbau – Wohnungen – Beurteilung und Vorschläge für erhöhten Schallschutz. Beuth, Berlin, 2012.

[13] Kötz, Wolf-Dietrich: Vorbeugender Schallschutz im Wohnungsbau. In: BundesBauBlatt, Heft 12/2000, Bauverlag, Gütersloh, 2000.

Stand der Web-Links März 2014.

Walter Schmidt

Videoüberwachung in Frankfurt am Main

Erfahrungen einer Bürgerrechtsgruppe im öffentlichen Straßenraum

Einer der Arbeitsschwerpunkte der Bürgerrechtsgruppe ***die*Datenschützer** *Rhein-Main*[1] *ist das Thema Videoüberwachung. Auslöser für die Auseinandersetzung mit der Thematik waren persönliche Erfahrungen einzelner Gruppenmitglieder, die feststellten, dass sie auf ihren alltäglichen Wegen durch Frankfurt teilweise von Dutzenden von Videokameras ins Visier genommen werden. Die Gruppe konzentriert sich derzeit bei der Bearbeitung der Thematik vorrangig auf die Überwachung des öffentlichen Straßenraums durch öffentliche Einrichtungen (z. B. Polizei, Verkehrsüberwachung) und private Stellen (z. B. Firmen, Grundstückseigentümer).*

Videoüberwachung ist überall…

Auf dem Territorium der Stadt Frankfurt haben Mitglieder der Bürgerrechtsgruppe *die*Datenschützer Rhein-Main im Verlauf der letzten 12 Monate mehr als 270 Grundstücke und Gebäude identifiziert, auf denen mehr als 700 Videokameras so platziert und ausgerichtet sind, dass sie sich auch dafür eignen, den benachbarten öffentlichen Straßenraum zu beobachten. Betreiber dieser Videokameras sind u. a. Apotheken, Arztpraxen, Banken (in außerordentlich hoher Zahl), Cafés, Detekteien, Handwerksbetriebe, Immobilienmakler, Industriebetriebe, Juweliere, Kleingartenvereine, Krankenhäuser, Restaurants, Speditionen, Spielhallen, Sportstätten, Tiefgaragen und die Universität.

Opernplatz – Alte Oper. Alle Fotos: Walter Schmidt

Hinzu kommen

- 78 Verkehrsüberwachungskameras der Integrierten Gesamtverkehrsleitzentrale (IGLZ) der Stadt Frankfurt, die den Verkehr auf den Haupteinfallstraßen nach Frankfurt und auf wichtigen Knotenpunkten des Individualverkehrs im Stadtgebiet aufzeichnen;

- (geschätzt) mehr als 300 Kameras, die an Kreuzungen und Fußgängerüberwegen dazu genutzt werden, Verkehrssignalanlagen zu steuern und

- mindestens 100 Kameras an oberirdischen Haltestellen des öffentlichen Nahverkehrs, die auch den öffentlichen Straßenraum außerhalb des unmittelbaren Haltestellenbereichs *im Blick* haben.

Bei vielen dieser mehr als 1.000 Kameras sind Zweifel berechtigt, ob ihre Installation den Vorgaben des Bundesdatenschutzgesetzes (BDSG) und anderer Rechtsnormen (z. B. des HSOG[2] oder des Urteils des Bundesgerichtshofs vom 24.05.2013 – Az.: V ZR 220/12[3]) entsprechen.

…und häufig rechtswidrig!

Stichprobenartige Beschwerden von Mitgliedern der Bürgerrechtsgruppe *die*Datenschützer Rhein-Main beim Hessischen Datenschutzbeauftragten machten deutlich, dass illegale Videoüberwachung des öffentlichen Straßenraums kein Einzelfall ist. Drei Beispiele:

- Bei einem Unternehmen im Industriegebiet des Frankfurter Stadtteils Seckbach waren ca. 15 von mehr als 60 Kameras auf den benachbarten öffentlichen Straßenraum gerichtet; zudem waren acht Dome-Kameras ebenfalls in der Lage, den öffentlichen Straßenraum zu überwachen. Die Beschwerde beim Hessischen Datenschutzbeauftragten hatte das erfreuliche Ergebnis, dass diese 15 Kameras neu ausgerichtet und alle acht Dome-Kameras komplett deinstalliert wurden[4].

- Ähnlich die Situation an der Alten Oper Frankfurt. Auch hier waren 16 Kameras (in der Mehrzahl Dome-Kameras) auf den Opernplatz gerichtet – eine häufig für Kundgebungen und Demonstrationen genutzte Versammlungsstätte. Nach Beschwerde beim Hessischen Datenschutzbeauftragten wurden die Kameras, die den täglich von tausenden Menschen genutzten Opernplatz beobachten, neu ausgerichtet, darüber hinaus mussten die Betreiber der Anlage weitere datenschutzrechtliche Mängel beseitigen[5].

- Im April 2014 hat der Hessische Datenschutzbeauftragte auf eine Beschwerde hinsichtlich Videoüberwachung des öffentlichen Straßenraums durch die Firma *Merz Pharma* im Frankfurter Nordend erneut deutlich gemacht, dass diese nicht zulässig ist[6].

Der Hessische Datenschutzbeauftragte Prof. Dr. Michael Ronellenfitsch bezeichnete bei der Präsentation seines Tätigkeitsberichts für 2013[7] Anfang April 2014 die Zunahme von Videoüberwachung im öffentlichen Straßenraum als „Dauerbrenner" und

Am Bornheimer Hang – Zugang zum FSV-Stadion
Stadt Frankfurt – Polizei

„Sorgenkind". In Bäckereien, Friseursalons, Kindergärten und Schulen, Sauna- und Umkleidebereichen, Stadthallen, denkmalgeschützten Einrichtungen und sogar im Wald würden immer mehr elektronische Augen installiert, stellte er fest. In den Kapiteln *3.3.5.2 Videoüberwachung an Schulen bleibt ein Dauerthema*, *3.3.7.6 Videoaufnahmen von Kindern im Kindergarten oder in einer Kindertagesstätte* und *4.2.2 Videoüberwachung nach Bundesdatenschutzgesetz* werden auf mehr als zehn Druckseiten eine Vielzahl von Beispielen dargestellt, wie öffentliche und private Stellen rechtswidrig Videoüberwachungstechnik einsetzen. Ronellenfitsch hat eine „pathologische Neigung" ausgemacht, nicht nur das persönliche Eigentum schützen, sondern auch den Nachbarn bespitzeln zu wollen. Zudem beklagte er, dass es der Landesgesetzgeber bisher versäumt habe, in das hessischen Datenschutzrecht eine Regelung aufzunehmen, wie öffentliche Stellen mit Hilfe von Videoüberwachung ihr Hausrecht ausüben können und wo Grenzen der Videoüberwachung nicht überschritten werden dürfen.

Mitglieder der Bürgerrechtsgruppe *die*Datenschützer Rhein-Main mussten häufig die Erfahrung machen, dass Betreiber von Kameras, die den öffentlichen Straßenraum beobachten, in völliger Unkenntnis der Rechtslage handeln. So teilten z. B. die Geschäftsleitungen der *Stadtwerke Frankfurt am Main Holding GmbH* und der *HFM Managementgesellschaft für Hafen und Markt mbH* nach Beschwerden mit, dass die Videoüberwachung – auch des benachbarten öffentlichen Straßenraums – durch die Zustimmung des jeweiligen Betriebsrats legitimiert sei. Eine Rechtsauffassung, der die Mitglieder der Bürgerrechtsgruppe *die*Datenschützer Rhein-Main nicht folgen mochten. Sie legten in diesen und anderen Fällen Beschwerde beim Hessischen Datenschutzbeauftragten ein. Die dazu anhängigen Verfahren sind derzeit noch nicht abgeschlossen.

Besonders hartnäckig als Auskunftsverweigerer zeigte sich der Frankfurter Feuerwehr-, Ordnungs- und Sportdezernent Markus Frank gegenüber einem Mitglied der Bürgerrechtsgruppe *die*Datenschützer Rhein-Main. Der Bürger begehrte Auskunft

Konstabler Wache

zu einer umfangreichen Videoüberwachungsanlage im Bereich Eissporthalle, Festplatz und dem Volksbankstadion im Frankfurter Stadtteil Bornheim. Auch ein Jahr nach der ersten Anfrage hat Herr Frank die Bürgeranfrage nicht beantwortet. Für diese intransparente Haltung wurde Herr Frank von den Frankfurter Datenschützern als Preisträger für die BigBrotherAwards[8] 2014 vorgeschlagen, aber nicht ausgewählt, weil es noch größere Datenkraken zu geben scheint.

Lediglich durch die Intervention des zuständigen Ortsbeirats, der eine gleichgelagerte Auskunft anforderte und durch ein Gespräch von Mitgliedern der Bürgerrechtsgruppe *die*Datenschützer Rhein-Main im Polizeipräsidium Frankfurt wurde bekannt, dass die Videoüberwachungsanlage für die Sportorte von der Stadt Frankfurt errichtet und finanziert, und durch das Polizeipräsidium Frankfurt genutzt wird. Nach Auskunft des Polizeipräsidiums fehlt auch mehrere Jahre nach Errichtung der Anlage ein aktuelles, vollständiges und von beiden verantwortlichen Stellen i. S. d. § 14 Abs. 3 HSOG bzw. § 15 HDSG gemeinsam erstelltes Verfahrensverzeichnis.

Hin und wieder führten Interventionen unmittelbar bei den Kamerabetreibern auch zum Erfolg. So veranlasste der Geschäftsführer eines Vereins, der im Frankfurter Ostpark eine Übernachtungsstätte für wohnungslose Menschen betreibt, nach Beschwerde den Abbau einer Kamera, die eine öffentlich zugängliche Fläche des Ostparks im Visier hatte[9]. Erfreulich auch die schnelle Reaktion aus der Geschäftsführung der *Eintracht Frankfurt*. Nach einer Anfrage wegen einer Videokamera auf dem Trainingsgelände im Frankfurter Stadtteil Riederwald teilte ein Mitglied des Geschäftsführenden Präsidiums der Eintracht mit: *„Ich lade Sie ein, die Videoeinstellung und Aufzeichnungen von einem von Ihnen zu bestimmenden Tag einzusehen, um Ihre Bedenken und Befürchtungen auszuräumen […]"*

Gespräche mit den Betreibern von Videoüberwachungsanlagen

Auf Grund von Nachfragen zu den von der Polizei und von der Verkehrsüberwachung der Stadt Frankfurt betriebenen Videoüberwachungsanlagen erhielten Mitglieder der Bürgerrechtsgruppe *die*Datenschützer Rhein-Main in den letzten Monaten Einladungen zu zwei informativen Gesprächen, eines in der *Integrierten Gesamtverkehrsleitzentrale (IGLZ)* der Stadt Frankfurt nach Einladung durch den Verkehrsdezernenten der Stadt Frankfurt[10], das andere im Polizeipräsidium Frankfurt nach Einladung durch den Polizeipräsidenten[11].

Ähnlich gesprächs- und informationsunwillig wie der Frankfurter Stadtrat Frank zeigten sich auch die Nahverkehrsunternehmen aus der Region Rhein-Main. Auf eine Anfrage der Bürgerrechtsgruppe *die*Datenschützer Rhein-Main zur Nutzung von Videoüberwachung an Haltestellen und in Fahrzeugen reagierten nur zwei Unternehmen, eines davon mit einer völlig nichtssagenden Antwort.

Eine Forderung an die politisch Verantwortlichen: Einrichtung eines Videokatasters!

Die Online-Ausgabe der *Süddeutschen Zeitung* präsentierte im Juli 2013 unter der Überschrift *Wie Kameras unser Verhalten verändern* eine interaktive Karte, auf der erkennbar ist, wo in Bayern von wem zu welchem Zweck wie viele Videoüberwachungsanlagen betrieben werden. Grundlage dieser Karte war eine Tabelle, die das Bayerische Staatsministerium des Innern zusammengestellt und am 1. Februar 2013 in einer Landtagsdrucksache veröffentlicht hatte. Darin sind alle der Bayerischen Staatsregierung bekannten Videoüberwachungsanlagen von öffentlichen und privaten Stellen in Bayern erfasst – mehr als 17.000 Kameras[12].

In Kenntnis dieser Veröffentlichung der Bayerischen Staatsregierung hat die Bürgerrechtsgruppe *die*Datenschützer Rhein-Main im August 2013 den Oberbürgermeister der Stadt Frankfurt und die Fraktionen in der Frankfurter Stadtverordnetenversammlung aufgefordert, ein Videoüberwachungskataster für Frankfurt zu erstellen und zu veröffentlichen. Im Februar 2014 hat die Gruppe dann auch den hessischen Innenminister aufgefordert, nach bayerischem Vorbild ein Videokataster für Hessen anzulegen und zu publizieren.

Die Reaktionen der politisch Verantwortlichen waren bislang mehr als verhalten:

- Der Frankfurter Oberbürgermeister ließ Anfang September 2013 verlauten, *„dass eine Prüfung Ihres Anliegens durch die zuständigen Dezernate erfolgt"*; eine inhaltliche Stellungnahme steht auch nach mehr als sechs Monaten noch aus.

Der hessische Innenminister reagierte etwas schneller, aber ähnlich unverbindlich. Ausgelöst durch eine Anfrage eines Landtagsabgeordneten der FDP sowie Anträge der Fraktion der Linken[13] und der FDP[14] erklärte er Anfang April im hessischen Landtag, dass das vorgeschlagene Verzeichnis *„nur mit ganz erheblichem Aufwand angelegt werden"* könne.

„Das Innenministerium müsste die dazu benötigten Daten zunächst bei den Landesbehörden, den Kommunen, den Bundesbehörden und allen privaten Unternehmen mit Sitz in Hessen erheben… Darüber hinaus könnte das Verzeichnis keine Auskunft darüber geben, ob eine bestimmte Videoüberwachung nach den datenschutzrechtlichen Vorschriften zulässig ist…"[15]

Leider erteilte auch der Datenschutzbeauftragte des Landes, Michael Ronellenfitsch, dem Vorschlag eines Videokatasters eine Absage. Die technokratische Begründung: Überwachungsanlagen von Firmen und Privatleuten müssten nicht bei den Landesdatenschutzbeauftragten gemeldet werden, da das Bundesdatenschutzgesetz eine solche Regelung nicht vorsieht. Daher könne eine Liste der Anlagen auch nicht aktuell gehalten werden.

Positiv die Reaktionen von FDP und DIE LINKE im Hessischen Landtag. Die FDP-Fraktion ließ in einer Pressemitteilung[16] verlauten:

*„Wir sind der Auffassung, dass die Bürgerinnen und Bürger genauso wie vor unverhältnismäßiger Videoüberwachung öffentlicher Stellen auch vor unzulässiger Überwachung Privater im öffentlichen Raum geschützt werden müssen. Deshalb unterstützt die FDP-Fraktion den Hessischen Datenschutzbeauftragten bei seinem Einsatz gegen unrechtmäßige Videoüberwachungsanlagen im öffentlichen Raum und begrüßen es, wenn Initiativen wie die Gruppe ‚die*Datenschützer *Rhein-Main' den Datenschutzbeauftragten auf erkennbare Missstände hinweisen … Wir … sind gespannt, ob er ein Verzeichnis der den öffentlichen Straßenraum in Hessen überwachenden Videoanlagen für sinnvoll erachtet, wie es ‚die*Datenschützer *Rhein-Main' fordern und wie es die bayerische Staatsregierung im Jahr 2013 für Bayern erstellt hat."*

Der Antrag der Fraktion DIE LINKE im Hessischen Landtag hat folgenden Tenor:

„Der Landtag begrüßt die Anregung … ein Verzeichnis aller den öffentlichen Straßenraum beobachtenden Videoüberwachungsanlagen in Hessen zu erstellen oder erstellen zu lassen … Die Erstellung eines Verzeichnisses aller Videoüberwachungsanlagen schafft die notwendige Transparenz, um die Einhaltung von Datenschutzbestimmungen überprüfen zu können."

Anmerkungen

Merz Pharma

1 *Informationen zur Bürgerrechtsgruppe die*Datenschützer Rhein-Main *auf der Homepage http://diedatenschuetzer-rheinmain.wordpress.com/*

2 *HSOG: Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (http://www.rv.hessenrecht.hessen.de/jportal/portal/t/7ucg/page/bshesprod.psml?doc.hl=1&doc.id=jlr-SOGHErahmen&documentnumber=1&numberofresults=140&showdoccase=1&doc.part=R&paramfromHL=true#focuspoint)*

3 *Siehe dazu: http://openjur.de/u/637430.html*

4 *Siehe dazu: http://diedatenschuetzerrheinmain.wordpress.com/2013/10/02/ein-erfolg-videokameras-die-den-offentlichen-strasenraums-uberwachten-wurden-abgebaut/*

5 *Siehe dazu: http://diedatenschuetzerrheinmain.wordpress.com/2014/01/31/videouberwachung-an-der-alten-oper-beschwerde-war-erfolgreich-rechtswidrige-uberwachung-des-offentlichen-raums-wurde-beendet/*

6 *Siehe dazu: http://diedatenschuetzerrheinmain.wordpress.com/2014/04/12/firma-merz-pharma-videouberwachung-des-offentlichen-strasenraums-erst-nach-beschwerde-beim-hess-datenschutzbeauftragten-beendet/*

7 *Siehe dazu: http://www.datenschutz.hessen.de/tb42inhalt.htm#entry3988*

8 *Siehe dazu: https://www.bigbrotherawards.de/*

9 *Siehe dazu: http://diedatenschuetzerrheinmain.wordpress.com/2013/11/11/ausufernde-videouberwachung-eindammen-es-ist-moglich-2/*

10 *Einzelheiten dazu unter http://diedatenschuetzerrheinmain.wordpress.com/2013/11/11/videouberwachung-des-strasenverkehrs-in-frankfurt-ein-besuch-in-der-integrierte-gesamt%C2%ADverkehrsleitzentrale-iglz-der-stadt-frankfurt/*

11 *Nähere Einzelheiten dazu unter http://diedatenschuetzerrheinmain.wordpress.com/2014/03/11/videouberwachung-durch-die-polizei-in-frankfurt/*

12 *Bayerischer Landtag; Landtagsdrucksache 16/15571, siehe http://www1.bayern.landtag.de/ElanTextAblage_WP16/Drucksachen/Schriftliche%20Anfragen/16_0015571.pdf*

13 *Landtagsdrucksache 19/225*

14 *Landtagsdrucksache 19/299*

15 *Hessischer Landtag, Vorläufiger Bericht der 8. Plenarsitzung – 19. Wahlperiode – 1. April 2014 (Seite 20 f.)*

16 *Siehe dazu http://fdpfraktion.hessen.liberale.de/Videoueberwachung-im-oeffentlichen-Raum/14047c31833i1p1788/index.html*

Walter Schmidt

Walter Schmidt wohnt in Frankfurt am Main.
Er ist Mitglied der Bürgerrechtsgruppe *die*Datenschützer Rhein-Main.

BIG BROTHER AWARDS.de — Die Oscars für Datenkraken

Stefan Hügel

BigBrotherAwards 2014

Der seit gut einem Jahr diskutierte Bruch des Menschenrechts auf Privatheit durch die umfassende nachrichtendienstliche Ausspähung der Kommunikation stellt praktisch alle zuvor bekannten Datensammlungen in den Schatten. Dennoch sollten wir uns auch weiterhin mit diesen beschäftigen: Nicht nur stellen solche Datenschutzverstöße einen Bruch der Privatheit aus eigenem Recht dar, auch können sie eine Vorstufe zur Ausspähung duch die Nachrichtendienste sein. Alle gesammelten Daten können letztlich in deren Datenbeständen landen und geheimdienstlich ausgewertet werden – sei es, dass sie bewusst, freiwillig oder unfreiwillig, den Nachrichtendiensten zur Verfügung gestellt werden, sei es, dass die Unternehmen und Behörden selbst unwissentlich angezapft werden. Im Ergebnis tragen potenziell alle Datenbestände zu der Ausspähung unserer Kommunikation und damit eines wesentlichen Teils unseres Lebens bei.

Wenn auch bei den diesjährigen BigBrotherAwards[1], die am 11. April 2014 in Bielefeld verliehen wurden, die nachrichtendienstliche Ausspähung breiten Raum einnahm, so spielten doch auch die anderen Bereiche eine Rolle, in denen personenbezogene Daten verarbeitet werden und dabei der Datenschutz nicht immer all zu genau genommen wird. Wie jedes Jahr wurden besonders prägnante Beispiele in mehreren Kategorien prämiert. Erstmals gab es in diesem Jahr auch einen Positivpreis, benannt *Julia-und-Winston-Award* nach den Hauptfiguren des Roman *Nineteen eighty-four* von *George Orwell*.

Kategorie *Politik*

Der BigBrotherAward 2014 in der Kategorie *Politik* steht in engem Zusammenhang mit der nachrichtendienstlichen Ausspähung, genauer, mit dem Umgang damit. Er wird dem **Bundeskanzleramt** – vertreten durch die Bundeskanzlerin, den Chef des Bundeskanzleramts und Beauftragten für die Nachrichtendienste, den Staatssekretär für Nachrichtendienst-Angelegenheiten und den Geheimdienst-Koordinator – verliehen, für „*Verstrickungen in den NSA-Überwachungsskandal sowie […] unterlassene Abwehr- und Schutzmaßnahmen*“, wie Laudator Rolf Gössner in seiner Laudatio betonte. Konkret geht es darum, dass:

- *„die bundesdeutschen Geheimdienste eng mit dem völker- und menschenrechtswidrig agierenden US-Geheimdienst NSA und anderen Diensten des ‚Echelon'-Geheimverbunds der ‚Five-eyes' kooperieren,*
- *[…] der dem Bundeskanzleramt unterstehende Bundesnachrichtendienst (BND) und das Bundesamt für Verfassungsschutz an Überwachungsinstrumenten, Spähprogrammen und Infrastrukturen der NSA beteiligt sind und*
- *[…] sowohl die alte als auch die neue Bundesregierung es sträflich unterlassen haben, mit Massenausforschung und Digitalspionage verbundene Straftaten, Verfassungs- und Bürgerrechtsverstöße abzuwehren und die Bundesbürger sowie von Wirtschaftsspionage betroffene Betriebe vor weiteren feindlichen Attacken zu schützen.“*

Der Laudator zeichnete den Überwachungsskandal nach, begonnen mit den ersten Enthüllungen von Edward Snowden und den daraus im weiteren Verlauf veröffentlichten Erkenntnissen, nach denen offenbar nicht nur die US-amerikanische NSA und der britische GCHQ diese Überwachung betreiben, sondern auch deutsche Geheimdienste daran beteiligt sind. Er wies auf die Gefahren dieser Datenauswertung hin – offenbar haben sie Konsequenzen, die von Einreiseverboten, wie bei dem Schriftsteller Ilja Trojanow (oder später der Campact-Aktivistin Maritta Strasser) bis hin zu Drohnenangriffen mit zahlreichen Todesopfern reichen.

Das Bundeskanzleramt ist dabei die zentrale Schaltstelle der Bundesregierungen und oberste Fachaufsicht des Auslandsgeheimdienstes BND – und zuständig für die Koordination der Zu-

Der Big Brother Award steht für die Preisträger zur Abholung bereit, Foto: Matthias Hornung, CC BY

sammenarbeit aller drei deutschen Nachrichtendienste, BND, Verfassungsschutz und MAD. Dass es auf die Enthüllungen sehr zögerlich reagiert, und den von der Ausforschung betroffenen Menschen und Unternehmen den Schutz davor verweigert, führt Gössner auf die enge deutsch-amerikanische Kooperation zurück, bei der Deutschland integraler Bestandteil des *Kriegs gegen den Terror* geworden ist.

Eine herausragende Rolle beim Verharmlosen, Beschwichtigen und Ignorieren spielte der frühere Chef des Bundeskanzleramts, Ronald Pofalla, der ungeachtet der Enthüllungen die Affäre zwischenzeitlich für beendet erklärte – erst nachdem bekannt wurde, dass auch das Mobiltelefon von Bundeskanzlerin Angela Merkel angezapft wurde, reagierte er empört.

Anfang Februar haben die Internationale Liga für Menschenrechte, der der Laudator angehört, Digitalcourage und der Chaos Computer Club Strafanzeige gegen die Verantwortlichen erstattet, die von Tausenden unterstützt wurde – ein Akt der Notwehr und der Nothilfe. Darauf folgt nun der BigBrotherAward für das Bundeskanzleramt.

Kategorie *Verkehr*

Für die Verpflichtung ihrer Online-Kunden, sich mit einem gültigen, offiziellen Ausweisdokument mit Lichtbild auszuweisen, erhält das Unternehmen **MeinFernbus GmbH** den BigBrotherAward in der Kategorie *Verkehr*. Laudator Peter Wedde begründete die Verleihung.

Bei MeinFernbus gilt die *„ausgedruckte oder in elektronischer Form (als PDF-Datei) vorzeigbare Buchungsbestätigung im Zusammenhang mit einem gültigen offiziellen Lichtbildausweis des Fahrgastes"* als Fahrausweis. Eine Ausweispflicht gibt es zwar auch bei einigen Wettbewerbern. Die MeinFernbus GmbH hat sich aber dadurch für den BigBrotherAward qualifiziert, dass in ihrer Datenschutzerklärung Möglichkeiten für die Datenweitergabe an Dritte vorgesehen sind. Bei der Zahlungsabwicklung wird – ohne Nennung eines zwingenden Grundes – auch die Telefonnummer, neben Vor- und Nachname, Straße, Hausnummer, Postleitzahl, Ort, Geburtsdatum an Dritte weiter gegeben. Zusätzlich werden laut Datenschutzerklärung „weitere" Daten übermittelt. Es kann nicht ausgeschlossen werden, so Wedde, dass dazu auch Informationen über konkrete Reiseverbindungen gehören. Für die in den AGB zu findende Ausweispflicht und die sich hiermit verbindende Datenerhebung gebe es weder eine gesetzliche Grundlage noch einen gesetzlichen Zwang. Der Datenschutz bleibe auf der Strecke; Ausweispflicht und Datenverwendungserklärung führten zur umfassenden Überwachung der Fahrgäste. Anonymes und ausweisfreies Reisen müsse für alle Fahrgäste garantiert werden.

Kategorie *Technik*

Der BigBrotherAward in der Kategorie *Technik* geht in diesem Jahr an die **Spione im Auto** – für Technologien mit der zunehmenden Aufzeichnung von Daten, die zu einer umfassenden Beobachtung von Verkehrsteilnehmern führen.

Einen Hauptverantwortlichen für die Tendenz, durch neue Technologien eine zunehmende Beobachtung von Verkehrsteilnehmern aufzubauen, nennt Laudator Frank Rosengart nicht. Die Komponenten die dazu beitragen, vom Gesetzgeber, von Herstellern und von Zulieferern, seien nicht voneinander zu trennen. Einige Technologien seien auch noch nicht serienreif – der Preis werde für das Gesamtwerk vergeben, um auf die Gesamttendenz aufmerksam zu machen.

Er nannte die Diskussion um den verpflichtenden Einbau eines Unfalldatenschreibers („*Black Box*") besorgniserregend, auch wenn er in Deutschland, gerade wegen der damit verbundenen Überwachungsmöglichkeiten, skeptisch gesehen wird. Gleichzeitig speicherten aber Airbag-Steuergeräte bereits heute genau die Parameter, die zum Auslösen des Airbags führen – nicht zuletzt zur Absicherung gegen einen möglichen Vorwurf, der Airbag wäre ohne Grund ausgelöst worden. Bei einem Unfalls oder auch einer schweren Verkehrsregelübertretung könnte die Polizei das Steuergerät beschlagnahmen und die dort gespeicherten Daten auslesen.

Doch auch weitere Geräte im Fahrzeug speichern Daten. Diese werden – zur Fehleranalyse – in den Werkstätten ausgelesen. Es ist möglich, dass damit personenbezogene Daten der Autofahrerinnen und Autofahrer auf den Servern der Autowerkstätten landen.

Ähnliches gilt für den Bordcomputer, der häufig auf dem Betriebssyste *Android* von Google basiert. Damit kann man die Dienste von Google auch im Auto nutzen – die Datenverarbeitung ist dabei Cloud-basiert, die Daten werden auf den Servern von Google oder anderen Anbietern verarbeitet. Eine Navigationsanfrage geht – üblicherweise samt Fahrzeugkennung – an den Navigationsdienstleister. Es ist also dort nachvollziehbar, wer wohin fahren wollte.

Auch Ortungsdienste, um gestohlene Fahrzeuge wiederzufinden, sammeln Daten – auch dann, wenn das Automobil nicht gestohlen ist. Einzelne Anbieter bieten ein permanentes Tracking des Fahrzeugs an.

Das europäische Notrufsystem E-Call ist dagegen – gemäß EU-Richtlinie – so gestaltet, dass die SIM-Karte, über die im Notfall ein Notruf abgesetzt wird, nicht ständig im Netz eingebucht ist. Das gilt freilich nur für die reine E-Call-Funktion. Werden auf der SIM-Karte weitere Dienste freigeschaltet, verhält sie sich wie ein normales Mobiltelefon.

Kategorie *Wirtschaft*

Im Zusammenhang mit der Ausspähaffäre ist auch ein US-amerikanisches Consulting-Unternehmen in die öffentliche Diskussion geraten. Neben einer Reihe von Bundesministerien, für die sie sicherheitskritische Projekte abwickelt, arbeitet die **Computer Sciences Corporation (CSC)** auch für US-amerikanische Nachrichtendienste und hat offenbar auch Entführungsflüge für die CIA organisiert. Rena Tangens hielt die Laudatio auf den Preisträger der Kategorie *Wirtschaft*.

Sie wies darauf hin, dass US-amerikanische Geheimdienste häufig Aufgaben an kommerzielle Dienstleister auslagern, so-

genannte *Private Intelligence Contractors*. CSC ist einer dieser Auftragnehmer. Seine Dienstleistungen erstreckten sich dabei offenbar nicht nur auf den digitalen Bereich. Über eine Tochterfirma wurden für die CIA auch Flüge für den verdeckten Transport von Terrorverdächtigen organisiert – darunter auch Khaled al-Masri, ein deutscher Staatsbürger, der monatelang in Mazedonien und Afghanistan festgehalten wurde.[2]

Gleichzeitig ist CSC in großem Umfang für deutsche Bundesministerien tätig. Seit 2009 regelt ein Rahmenvertrag IT-Dienstleistungen, z. B. beim bundesweiten Waffenregister, beim elektronischen Personalausweis (nPA) und bei De-Mail, dem Dienst für „sichere" Kommunikation mit Behörden, der bis heute keine End-zu-End-Verschlüsselung für Bürgerinnen und Bürger vorsieht.

Darüber hinaus hat die Bundesregierung CSC damit beauftragt, den Quellcode des von der *Gamma Group* entwickelten Staatstrojaners zu prüfen. CSC hat damit einen detaillierten Einblick in dessen Funktionsweise.

Rena Tangens bei ihrer Laudatio
Foto: Fabian Kurz, CC BY

Die Bundesregierung verweist auf Aussagen der *CSC Deutschland Solutions GmbH*, sie sei organisatorisch und personell vollständig vom US-amerikanischen Geschäftsbereich getrennt, der für das Geschäfts mit den dortigen Behörden zuständig ist. Sie habe keine vertraglichen Beziehungen zu NSA, CIA und FBI. Es bestünde kein wechselseitiger Einblick in Verträge und Tätigkeiten. Der Außenauftritt des Unternehmens erweckt streckenweise jedoch einen anderen Eindruck.

Kategorie *Neusprech*

Gerne wird bei der Datenausspähung und -auswertung darauf verwiesen, dass ja nicht die Kommunikationsinhalte gesammelt würden, sondern „nur" die **Metadaten**, als sei es nicht schützenswerter Abfall der Kommunikation. Dass dem nicht so ist, erläuterten Kai Biermann und Martin Haase in ihrer Laudatio der Kategorie *Neusprech*.

Metadaten geben Aufschluss darüber, wann wir welchen Nachrichten an wen schicken, und wie oft. Darüber, wo wir uns befinden und welche Geräte wir zur Kommunikation benutzen. *„Inhalte sagen, was wir sagen. Metadaten aber sagen, was wir tun, und was wir denken"*, so die Laudatoren. Deswegen müssten sie genauso wie der Inhalt geschützt werden. Für diese sprachliche Verschleierung der Überwachung gibt es den BigBrotherAward.

Kategorie *Arbeitswelt*

Stellvertretend für Unternehmen, die für die Bewertung ihrer Mitarbeiterinnen und Mitarbeiter technische Aufzeichnungsmethoden verwenden, wird die **RWE Vertrieb AG** mit dem BigBrotherAward in der Kategorie *Arbeitswelt* ausgezeichnet. Die Laudatio hielt Sönke Hilbrans.

Er verwies zunächst auf neue Informationen, die *„den Preis an einigen nicht ganz irrelevanten Stellen in einem etwas anderen Licht erscheinen"* ließen. Dennoch halte die Jury an der Preisvergabe fest.

Es geht um einen inzwischen fast alltäglichen Vorgang: Will man Services telefonisch über ein Call-Center in Anspruch nehmen, wird man zunächst gefragt, ob man mit der Aufzeichnung des Gesprächs „zur Verbesserung der Servicequalität" einverstanden sei. Widerspricht man dem nicht, kann es sein, dass das Gespräch aufgezeichnet wird. Eingesetzt wird dafür die Software eines Herstellers, der auch Geheimdienste – einschließlich der NSA – beliefert. Sie erfasst den Inhalt des Gesprächs – einschließlich Tonlage, Dauer, Stimmungen etc. – und weitere Aktivitäten: Mausklicks, gedrückte Tasten, Zeitabstände zwischen Interaktionen und weitere Parameter. So wird der Mitarbeiter im Call-Center auf Qualität und Leistung überprüft.

Der Jury kam es bei der Bewertung nicht darauf an, ob diese Überwachung legal oder illegal ist. *„Denn schon die Möglichkeit, dass die Einzelnen überwacht werden, und dass daraus denkbare Konsequenzen gezogen werden, reicht aus, um den Einzelnen unter den Druck zu setzen, sein Verhalten an reale oder an vermutete Erwartungen anzupassen. Auch gefühlter Überwachungsdruck hat reale Konsequenzen. Es gibt keine gute Überwachung und es gibt damit auch keine gute Aufzeichnung und gute Qualitätskontrolle in Callcentern"*, so der Laudator. Es sei aber möglich, die Aufzeichnung abzulehnen – was die Jury den Anruferinnen und Anrufern empfiehlt.

Kategorie *Verbraucherschutz*

Für das Ausspähen unserer Wohnzimmer erhält die **LG Electronics GmbH** den BigBrotherAward in der Kategorie *Verbraucherschutz*. padeluun zog in seiner Laudatio Parallelen zum *Teleschirm* aus dem Roman *Nineteen eighty-four.*

Zunächst gab er einen Überblick über die tatsächliche technische Entwicklung bei Fernsehgeräten. 1948, als der Roman geschrieben wurde, war ein Rückkanal noch technisch unmöglich. Doch mit dem Versuch, das Medium Fernsehen zu einem interaktiven Medium umzugestalten, kam der Bildschirmtext (BTX) und mit ihm auch dieser Rückkanal – freilich (vorerst) nicht zur Überwachung der Zuschauer, sondern um die Bestellung von Waren zu ermöglichen.

Heute „fernsehen" wir im Internet. Und damit wurden die Fernsehgeräte *smart*: flache Computer mit Internetanschluss.

Damit steht nun ein Rückkanal zur Verfügung – und er wird genutzt, wie es einem Blogger in England auffiel: Sein Fernsehgerät sendete Informationen über das angezeigte Programm, die eingelegte DVD und die gepeicherten Dateien auf angeschlossenen USB-Sticks und Festplatten. Es gab auch eine Einstellung, die diese Datenübertragung abstellen sollte – sie hatte aber offenbar keinerlei Wirkung: die Daten wurde einfach weiter gesendet.

In einer Studie der Technischen Universität Darmstadt zu dem hier genutzten Standard *HbbTV* zeigten sich die Forscherinnen und Forscher *„überrascht, wie viele Daten dort wie häufig ausgesendet wurden."* *„Adressaten der Daten seien unter anderem die Server großer Werbetreibender wie Google Analytics, Chartbeat und Webtrekk gewesen. Bei den Untersuchungen der Forscher wurden Daten zum TV-Verhalten auch bei Fernsehern übertragen, bei denen der Zuschauer gar keine smarten Inhalte abgerufen hatte"*, fasste padeluun die Ergebnisse zusammen. Fernsehen mit Internetanschluss reiche dafür aus.

Tadelnde Erwähnungen

Auch dieses Jahr gab es eine Reihe *tadelnder Erwähnungen*. Unter anderem wurden dabei erwähnt:

- Die **Kirchensteuer auf die Abgeltungssteuer**, durch die Banken verpflichtet werden, beim Bundeszentralamt für Steuern die Konfession ihrer Kunden zu erfragen, um die Kirchensteuer von Kapitalerträgen abzuführen. Dies unterhöhlt das Recht, selbst zu entscheiden, ob und wen man über seine Kirchenmitgliedschaft informiert.

- **WhatsApp** für unsichere Kommunikation. Dazu führen Sicherheitslücken, deren Schließung teilweise lange dauerte, unverschlüsselt gespeicherte Chatprotokolle und die Forderung weitreichender Zugriffsrechte für den täglichen Betrieb.

- **Telefonmitschnitte** und ihre Veröffentlichung – die mediale Verwertung vertraulicher Gespräche. Mehrfach kamen solche Gespräche an die Öffentlichkeit, indem Mitschnitte davon im Internet auftauchten. Dabei gab es kaum eine kritische Nachfrage, z. B. wie diese Gespräche aufgezeichnet wurden, welche Interessen dahinter stehen und ob es journalistisch vertretbar ist, solche Informationen zu verwenden. Nach deutschem Recht sind solche Mitschnitte verboten. Wir sollten die Vertraulichkeit des Wortes ernst nehmen – auch wenn es sich um politsche Gegner handelt.

Weitere tadelnde Erwähnungen sind auf der Web-Seite der BigBrotherAwards nachzulesen.

Julia-und-Winston-Award

Erstmals wurde in diesem Jahr ein Positivpreis verliehen: Der *Julia-und-Winston-Award* – nach den Hauptfiguren des Romans nineteen eighty-four – wurde an **Edward Snowden** verliehen. Unter großem Beifall hielt Heribert Prantl, Leiter des Ressorts Innenpolitik bei der *Süddeutschen Zeitung*, die Laudatio.

Er bezeichnete Edward Snowden als Aufklärer und Motivator. Er habe die globale US-Großinquisition aufgedeckt und musste vor dem Großinquisitor fliehen. Er habe Besseres verdient, als ein zeitlich begrenztes Asyl in Russland. Prantl forderte für Snowden einen stabilen Aufenthaltstitel für Deutschland.

„Snowdens Handeln mag in den USA strafbar sein, weil er US-Gesetze verletzt hat; wirklich kriminell sind aber die Zustände und die Machenschaften, die er anprangert", so Prantl weiter. *„Snowden hat gegen US-Geheimhaltungsvorschriften verstoßen. Ist er deswegen Landesverräter? Nein. Verräter nennen ihn die, die selbst die Grundrechte verraten haben. Snowden hat dem Rechtsstaat Nothilfe geleistet."*

Jacob Appelbaum dankte im Namen von Edward Snowden für die Preisverleihung. *Digitalcourage* verleiht der Forderung nach Asyl für Snowden mit 1.000.000 Aufklebern Nachdruck, die kostenlos im Digitalcourage-Shop[3] bestellt werden können.

Anmerkungen

1 *BigBrotherAwards, http://www.bigbrotherawards.de*
2 *Christian Fuchs, John Goetz (2013): Geheimer Krieg. Wie von Deutschland aus der Kampf gegen den Terror gesteuert wird. Reinbek bei Hamburg: Rowohlt*
3 *Digitalcourage-Shop, https://shop/digitalcourage.de/thema/snowden*

Lichtjonglage von Jens Neumann
Foto: Matthias Hornung, CC BY

Rolf Gössner

Kategorie *Politik* – Laudatio

Der BigBrotherAward 2014 in der Kategorie Politik geht an das Bundeskanzleramt,

vertreten durch die Hausherrin, Bundeskanzlerin Dr. Angela Merkel (CDU), den Bundeskanzleramtschef und Beauftragten für die Nachrichtendienste, Peter Altmaier (CDU), den Staatssekretär für Nachrichtendienst-Angelegenheiten, Klaus-Dieter Fritsche (CSU) sowie den Geheimdienstkoordinator Günter Heiß,

dafür, dass

1. die bundesdeutschen Geheimdienste eng mit dem völker- und menschenrechtswidrig agierenden US-Geheimdienst NSA und anderen Diensten des *Echelon*-Geheimverbunds der *Five-eyes* kooperieren,

2. dafür, dass der dem Bundeskanzleramt unterstehende Bundesnachrichtendienst (BND) und das Bundesamt für Verfassungsschutz an Überwachungsinstrumenten, Spähprogrammen und Infrastrukturen der NSA beteiligt sind und

3. dafür, dass sowohl die alte als auch die neue Bundesregierung es sträflich unterlassen haben, mit Massenausforschung und Digitalspionage verbundene Straftaten, Verfassungs- und Bürgerrechtsverstöße abzuwehren und die Bundesbürger sowie von Wirtschaftsspionage betroffene Betriebe vor weiteren feindlichen Attacken zu schützen.

Im Kern geht es also um bundesdeutsche Verstrickungen in den NSA-Überwachungsskandal sowie um unterlassene Abwehr- und Schutzmaßnahmen. Mitte 2013 ist die flächendeckende verdachtsunabhängige Ausforschung der globalen Telekommunikation durch den US-Geheimdienst NSA (*National Security Agency*) und den britischen Geheimdienst GCHQ (*Government Communications Headquarters*) bekannt geworden. Die historisch einmaligen Enthüllungen basieren auf Geheimdokumenten, die der Ex-NSA-Mitarbeiter und Whistleblower Edward Snowden öffentlich machen ließ. Snowden spricht von der „größten verdachtsunabhängigen Überwachung in der Geschichte der Menschheit". Diese digitale Durchleuchtung der Privatsphäre ganzer Gesellschaften stellt alle Menschen, die auf irgendeine Art elektronisch kommunizieren, unter Generalverdacht, unterhöhlt die Unschuldsvermutung, führt zur Verletzung von Persönlichkeitsrechten und stellt verbriefte Grundrechte, ja die Demokratie insgesamt in Frage.

Nach und nach stellte sich heraus, dass nicht allein US- und britische Geheimdienste in den globalen Überwachungsskandal involviert sind, sondern dass auch bundesdeutsche Geheimdienste – BND, Verfassungsschutz, Militärischer Abschirmdienst – an diesem transatlantischen Geheimverbund partizipieren. Sie profitieren von überlieferten Daten und übermitteln selbst Millionen von Telekommunikationsdaten aus Deutschland – etwa personenbezogene Verbindungs- und Verdachtsdaten, die bei der pauschalen Überwachung und Kontrolle des Fernmeldeverkehrs ins und vom Ausland anfallen.

„Na und?" fragen sich noch immer viele Menschen: „Wer soll denn diese Massen belangloser Daten überhaupt auswerten? Was kann mir schon passieren?" Leider zu kurz gedacht, denn die dokumentierbaren Folgen können heftig sein: Am Ende solcher Datenerfassungen und -auswertungen kann etwa eine verweigerte Einreise in die USA stehen, wie im Fall des bundesdeutschen Schriftstellers Ilija Trojanow, der die US-Überwachungsorgie öffentlich kritisiert hatte. Oder aber im Extremfall ein US-Drohnenbeschuss auf „Terrorverdächtige", wie etwa im Dezember 2013 im Jemen, bei dem 17 Mitglieder eines Hochzeitskonvois ums Leben kamen. Dazwischen ist so manche Unannehmlichkeit, Schikane oder Tortur möglich – von verschärften Grenzverhören, Nachforschungen bei Nachbarn oder Arbeitgebern, über Staatstrojaner im PC, die Aufnahme in US-No-Fly- oder Terrorlisten bis hin zu Verhaftungen oder Folter in Spezialgefängnissen. Selbst wer treuherzig glaubt, er habe eigentlich „nichts zu verbergen", kann plötzlich zum Opfer einer fatalen Verwechslung werden – wie Khaled El Masri, der mit einem „Terroristen" verwechselt, von CIA-Agenten nach Afghanistan verschleppt und monatelang gefoltert wurde. Oder man ist zur falschen Zeit am falschen Ort wie Murat Kurnaz, der aufgrund von „Verfassungsschutz"-Informationen als angeblicher „Terrorverdächtiger" für viereinhalb Jahre im US-Foltercamp Guantánamo verschwand.

Spektakuläre Einzelfälle? Sicher, aber es gibt auch viele „kleinere" Beispiele für üble Folgen des Überwachungswahns. So forschen Geheimagenten deutscher und alliierter Dienste über die BND-Tarnbehörde „Hauptstelle für Befragungswesen" jährlich Hunderte Flüchtlinge aus oder werben sie als „Quellen" oder Spitzel an – hier werden schutzsuchende Menschen in akuten Notlagen skrupellos abgeschöpft und für staatliche Zwecke missbraucht.

Nach Informationen von Edward Snowden tauschen deutsche und US-Geheimdienste nicht nur massenhaft Informationen aus, sondern teilen auch Instrumente, gemeinsame Datenbanken (z. B. „Projekt 6"), Spähsoftware wie das XKeyscore-Überwachungsprogramm und Infrastrukturen – kurzum: Sie gehen „miteinander ins Bett", so Snowdens bildhafte Worte in seinem ARD-Interview (26. Januar 2014).

Diese enge Kooperation und intensive Datenübermittlungspraxis, die weitgehend ohne Datenschutzkontrolle abläuft, basiert auch auf Geheimverträgen mit den Westalliierten. Diese Verträge räumen den Vertragspartnern Sonderrechte ein, die weite Handlungsfelder eröffnen und stark in Grundrechte der Bundesbürger eingreifen – ohne jede parlamentarisch-demokratische Beteiligung oder Kontrolle. Und sie beschränken die Souveränität Deutschlands bis heute.

Seit Jahren und Jahrzehnten sind die verantwortlichen Bundesregierungen und ihre Nachrichtendienste also Komplizen, Gehilfen, ja Mittäter im großen aggressiven Spiel westlicher Geheimdienste – oder anders formuliert: willfährige Partner. Dabei

kommt dem Bundeskanzleramt eine ganz entscheidende Rolle zu, die es heute zu „würdigen“ und negativ auszuzeichnen gilt. Denn dieses Amt ist zentrale Schaltstelle der Bundesregierungen, ist zuständig für die oberste Fachaufsicht über den Auslandsgeheimdienst BND sowie für Koordination und Intensivierung der Zusammenarbeit aller drei Bundesgeheimdienste untereinander und mit anderen Dienststellen im In- und Ausland.

Wer sich in den vergangenen Monaten verzweifelt die Frage stellte, warum die Bundesregierung den Bürgern und Unternehmen, die von der massenhaften Ausforschung betroffen sind, bis heute jeglichen Schutz verweigert, findet hier eine plausible Antwort: Das auffallend zögerliche Verhalten nach Snowdens Enthüllungen und die geradezu unterwürfige Zurückhaltung gegenüber den USA dürfte mit der engen deutsch-amerikanischen Kooperation zu erklären sein; und vor allem damit, dass Deutschland längst integraler Bestandteil der US-Sicherheitsarchitektur und des US-„Kriegs gegen den Terror“ geworden ist. Angesichts bilateraler Geheimabkommen, Partizipation und Duldung völker- und menschenrechtswidriger Strukturen und Aktionen der USA in der Bundesrepublik hält man sich seitens der Bundesregierung offenbar lieber bedeckt, verharmlost und beschwichtigt – zumal man, frei nach Constanze Kurz (CCC), künftig „beim großen Datenroulette“ nicht länger „am Katzentisch sitzen“ will. So plant die aktuelle Große Koalition tatsächlich eine stärkere Zentralisierung und Vernetzung der deutschen Geheimdienste untereinander und auch mit der Polizei – und damit eine Stärkung demokratiewidriger Geheim-Institutionen, die weder transparent noch demokratisch kontrollierbar sind. Und diese „GroKo“ ist auch noch wild entschlossen, mit der erneuten Legalisierung der verdachtslosen Vorratsspeicherung sämtlicher Telekommunikationsdaten der Bevölkerung den Überwachungskosmos hierzulande noch gehörig zu erweitern – anstatt ihn, wie vor dem Hintergrund der NSA-Massenausforschung dringend geboten, endlich wirksam einzuschränken.

Verharmlosen, beschwichtigen und ignorieren – diese regierungsamtliche Scheinreaktion auf die beunruhigende NSA-Affäre hat einen Namen: Pofalla, Ronald (CDU) – bis Ende 2013 amtierender Chef des Bundeskanzleramts, zugleich Beauftragter für die Nachrichtendienste und oberster Aufseher des BND.

Als die NSA-Affäre im Juni 2013 für Aufsehen sorgte, da duckte sich der unmittelbar zuständige Pofalla erstmal weg und schwieg. Niemand hat von ihm je einen erhellenden Beitrag zur Rechtmäßigkeit der millionenfachen Auswertung von Telekommunikationsdaten durch die US-Geheimdienste und zur Rolle des BND vernommen. Im Gegenteil: Er bezifferte die Weitergabe von Informationen über deutsche Staatsbürger an US-Geheimdienste auf ganze zwei Datensätze, obwohl es nachweislich Hunderte waren. Später erklärte er ungeachtet weiterer Enthüllungen die NSA-Affäre für beendet: Alle gegen die Geheimdienste erhobenen Vorwürfe seien „vom Tisch“ und millionenfache Grundrechtsverletzung habe es in Deutschland nie gegeben. Vielmehr hätten ihm die beteiligten Dienste schriftlich versichert, sich an deutsches Recht zu halten. Für diese herausragenden „Vermauschel-Dienste“ verlieh die NDR-Satiresendung Extra3 Pofalla den Negativpreis „Silberner Hilfssheriff-Stern“, den er allerdings vor laufender Kamera verweigerte – womöglich hatte er ja insgeheim einen goldenen Hilfsagenten-Orden erwartet. Oder gleich den BigBrotherAward. Solche Männer braucht … die Deutsche Bahn … bekanntlich ihrerseits Trägerin eines BigBrotherAwards …

Und Pofallas Chefin, die Hausherrin des Bundeskanzleramts? Was unternahm eigentlich Frau Merkel angesichts der eskalierenden Überwachungsaffäre? Kurze Antwort: so gut wie nichts! Und dabei hat sie doch schon dreimal Stein und Bein geschworen, ihre „Kraft dem Wohle des deutschen Volkes“ zu widmen, seinen Nutzen zu mehren, Schaden von ihm zu wenden, das Grundgesetz und die Gesetze des Bundes zu wahren und zu verteidigen und ihre Pflichten gewissenhaft zu erfüllen.

Dr. Rolf Gössner hält die Laudatio für den Big Brother Award in der Kategorie Politik für das Bundeskanzleramt
Foto: Matthias Hornung, CC BY

Stattdessen zog Frau Merkel den Kopf zwischen die Schultern und verwies auf ihren profunden Pofalla, der die Affäre Mitte August 2013 für beendet erklärte; danach verwies sie auf ihren damaligen CSU-Innenminister Hans-Peter Friedrich, der die Affäre wenige Tage später ebenfalls für beendet erklärte. O-Ton Friedrich: „Alle Verdächtigungen, die erhoben wurden, sind ausgeräumt.“ Auch er sah keinen Grund, daran zu zweifeln, dass sich die USA an Recht und Gesetz hielten. Von einem Kurztrip in die USA zur Aufklärung der NSA-Affäre kehrte er zufrieden mit der Mär zurück, er habe die Vorgänge geklärt. Bei der Snowden-Affäre handele es sich ohnehin um „falsche Behauptungen und Verdächtigungen, die sich in Luft aufgelöst haben (…) Wir können sehr zufrieden und auch sehr stolz darauf sein, dass unsere Nachrichtendienste bei unseren Verbündeten als leistungsfähige, bewährte und vertrauenswürdige Partner gelten“ (16.08.13). Und zum Abschluss bescheinigt Friedrich NSA-Kritikern eine „Mischung aus Antiamerikanismus und Naivität“, die ihm „gewaltig auf den Senkel“ gehe. Was durchaus auf Gegenseitigkeit beruht, haben wir ihn doch schon 2012 mit dem BigBrotherAward bedacht. Leider ohne Erfolg: Zur Rechtfertigung der NSA-Massenüberwachung hat dieser Bundesinnenminister, der zugleich Verfassungsminister war, ein so genanntes „Supergrundrecht auf Sicherheit“ frei erfunden, dem er verbriefte Grund- und Freiheitsrechte kurzerhand unterordnen zu können glaubt.

Erst als im Oktober 2013 bekannt wurde, dass die NSA schon jahrelang ein Mobiltelefon der Kanzlerin gezielt abhört, da äußerte sich Ronald Pofalla plötzlich wieder und diesmal empört – jetzt sprach er von einem „schweren Vertrauensbruch“ sei-

tens der USA. Ihren Regierungssprecher ließ die Kanzlerin erbost von einer „völlig neuen Qualität“ faseln, denn: „Abhören von Freunden, das geht gar nicht“. Also: Nicht die massenhafte Ausspähung der Bevölkerung, nicht die Sorge um deren Schutz, sondern erst dieser unfreundliche Angriff auf das Handy der Kanzlerin führte endlich zu schärferen Reaktionen gegenüber den Auftraggebern im Weißen Haus. Und, ganz nebenbei, geriet mal wieder unser Inlandsgeheimdienst „Verfassungsschutz“ unter Druck, zu dessen Kernaufgaben die Spionageabwehr gehört: Denn von den Spionageaktionen gegen die Kanzlerin hatte er offenbar nichts mitbekommen, geschweige denn, diese Lauschangriffe verhindert.

Und sage noch eine oder einer, die Bundesregierung hätte doch gar nichts gegen die feindlichen Attacken auf Privat-, Betriebs- und Regierungssphäre unternehmen können, nachdem doch schon das öffentlichkeitswirksam zelebrierte No-Spy-Abkommen mit den USA von Anfang an zum Scheitern verurteilt war. Doch, die Regierung könnte vom Verfassungsschutz enttarnte Abhör-Agenten in US- und anderen Botschaften, von deren Gelände aus politische Institutionen ausgeforscht werden, zu unerwünschten Personen erklären und des Landes verweisen. Sie könnte im Fall möglicher Grundrechtsverletzungen zu Lasten von Bundesbürgern militärische US-Liegenschaften durch deutsche Sicherheitsbehörden kontrollieren lassen – etwa den weiteren Bau eines NSA-Abhörzentrums auf dem US-Stützpunkt in Wiesbaden oder das Africom-Regionalkommando der US-Streitkräfte in Stuttgart, das Luftangriffe, Kampfdrohnen-Einsätze, Verschleppungen und extralegale Hinrichtungen von Terrorverdächtigen in Afrika plant(e). Und die Bundesregierung könnte Geheimverträge offen legen und revidieren. Weshalb sie und die Ermittlungsbehörden insoweit untätig geblieben sind, ist nicht nachvollziehbar und dürfte an Verfassungsbruch grenzen.

Deshalb sahen sich Internationale Liga für Menschenrechte, Digitalcourage und ChaosComputerClub Anfang Februar 2014 gezwungen, beim Generalbundesanwalt Strafanzeige gegen die involvierten Geheimdienste und die Bundesregierung zu erstatten, um die politisch und strafrechtlich Mitverantwortlichen endlich zur Rechenschaft zu ziehen. Es war ein Akt der Notwehr und Nothilfe, der wie ein Ventil wirkte, das plötzlich geöffnet wird: Tausende haben uns geschrieben und die Strafanzeige unterstützt. Ja, und heute öffnen wir ein weiteres Ventil …

Herzlichen Glückwunsch zum BigBrotherAward 2014, Bundeskanzleramt.

Kai Biermann und Martin Haase

Kategorie *Neusprech* – Laudatio

Den BigBrotherAward 2014 in der Kategorie Neusprech erhält der Begriff *Metadaten*

Geheimdienste und Regierungen beteuern immer wieder, dass sie sich nicht für die Daten der Bürger interessieren, sondern „nur“ für die Metadaten, als ginge es dabei um völlig Irrelevantes, nachgerade um Datenabfall, der sowieso bei jeder Datenübertragung anfällt und im Gegensatz zu den „richtigen“ Daten nicht besonders schützenswert sei. „Niemand hört mit“, sagte US-Präsident Barack Obama nach Bekanntwerden der Snowden-Dokumente und wollte damit alle beruhigen. Was für eine Lüge.

Das griechische Präfix μετά- bedeutet „nach“ oder „jenseits“, wörtlich sind also Metadaten „Nachdaten“ oder „jenseitige Daten“. Im Deutschen wird das Präfix jedoch meistens verwendet, um anzuzeigen, dass es sich um etwas handelt, das auf einer höheren Abstraktionsebene anzusiedeln ist, in diesem Fall also: Daten über Daten.

Es sind eben jene Daten, die benötigt werden, um Informationen zu übermitteln: Wer schickt was und wie viel wie oft wohin, wo befindet er sich dabei, welche Geräte benutzt er dazu, wie lange dauert das alles. Die Metadaten sind für die Kommunikation essenziell, ohne sie könnten wir uns nicht digital unterhalten.

Spätestens seit Edward Snowden wissen wir, dass Geheimdienste Metadaten abschnorcheln, speichern und auswerten, wo sie nur können. Denn Inhalte sagen, was wir sagen. Metadaten aber sagen, war wir tun, und was wir denken. Sie enttarnen uns und unsere Pläne, ohne dass wir es merken. Metadaten erlauben es, soziale Netzwerke aufzudecken, die Standorte von Menschen zu ermitteln und Bewegungsprofile zu erstellen.

Prof. Dr. Martin Haase hält die Laudatio
Foto: Bernd Sieker, CC BY

Statt sie wie Abfall zu behandeln, den jedermann aufsammeln kann, müssten sie mindestens ebenso gut geschützt werden, wie der Inhalt unserer Kommunikation. Denn sie sind ganz und gar nicht so „jenseitig“, wie das Präfix andeutet.

Außer den Überwachten scheint daran aber niemand Interesse zu haben. Was sich unter anderem daran zeigt, dass die große Lüge von den harmlosen Metadaten auch sprachlich aufrecht erhalten werden soll. Das Synonym „Verbindungsdaten" macht nicht im Ansatz klar, wie umfangreich und aussagekräftig unsere Metadaten sind. Als Verschleierung genügt das offensichtlich nicht, inzwischen ist „Rahmendaten" das neue Ersatzwort *(http://www.tagesschau.de/ausland/obama3660.html).*

Für den Versuch, diese flächendeckende Überwachung sprachlich zu verheimlichen, erhält der Begriff **Metadaten** einen Big Brother Award 2014.

Heribert Prantl

Julia-und-Winston-Award (Positivpreis)

In diesem Jahr verleihen wir zum ersten Mal einen Positivpreis. Der „Julia-und-Winston-Award" wurde benannt nach den „rebellischen" Hauptcharakteren aus George Orwells dystopischem Roman „1984", aus dem auch der „Große Bruder" stammt. Der Award soll Personen auszeichnen, die sich in besonderem Maße gegen Überwachung und Datensammelwut eingesetzt haben. Der Preis ist auf eine Million dotiert – allerdings nicht eine Million Euro.

Die Laudatio für den ersten Julia-und-Winston-Award hält Heribert Prantl, Mitglied der Chefredaktion der Süddeutschen Zeitung.

Der Preisträger des ersten *Julia-und-Winston-Award* ist

Edward Snowden.

In Berlin hat der Bundestag einen Untersuchungsausschuss eingesetzt, der den NSA-Skandal aufklären soll. Das Seltsame dabei ist, dass die Mehrheit im Ausschuß den nicht hören will, der den Skandal aufgedeckt hat. Die CDU/CSU redet über Snowden, als habe er eine ansteckende Krankheit. Und die SPD widerspricht kaum. Das ist grober Undank.

Der Mann habe doch schon alles gesagt, was er wisse, heißt es; man brauche ihn doch daher gar nicht mehr zu vernehmen. Das ist vorweggenommene Beweiswürdigung. Die ist im gesamten Recht verboten; im Deutschen Bundestag auch. Snowden ist ein zentrales Beweismittel, das weiß jeder. Der wahre Grund dafür, warum man Snowden nicht einmal einladen will, ist der: die Kanzlerin Angela Merkel fürchtet, dass dann die Amerikaner pikiert und unwirsch reagieren, wenn sie im Mai in die USA reist. Das ist nicht nur hasenherzig. In ihrem Amseid hat die Kanzlerin geschworen, Schaden vom deutschen Volk zu wenden. Schaden wenden – das heißt: etwas gegen den Schaden zu tun, den die NSA anrichtet. Stattdessen tut die Bundesregierung so, als sei Snowden und nicht die USA der Schädiger.

Edward Snowden ist ein Aufklärer. Er hat die globale US-Großinquisition aufgedeckt und musste fliehen vor dem Großinquisitor. Er hat persönlich keinerlei Vorteile von seiner Whistlerblowerei, er hat nur Nachteile. Den Gewinn hat die Rechtsstaatlichkeit der westlichen Demokratien, sie könnte ihn haben, wenn diese den globalen Skandal zum Anlass nehmen, ihren Geheimdiensten Grenzen zu setzen.

Snowden ist also nicht nur Aufklärer, er ist auch Motivator. Er hat etwas Besseres verdient als ein wackeliges, zeitlich begrenztes Asyl in Russland. Die Amerikaner verfolgen ihn, als handele es sich bei Snowden um die Reinkarnation von Bin Laden. Dabei ist er nur ein einzelner Flüchtling; er ist ein Flüchtling, wie er im Buche steht. Wie soll, wie muss Deutschland mit Edward Snowden umgehen? Vor allem dankbar! Snowden hat Schutz und Hilfe verdient. Er ist ein klassischer Flüchtling.

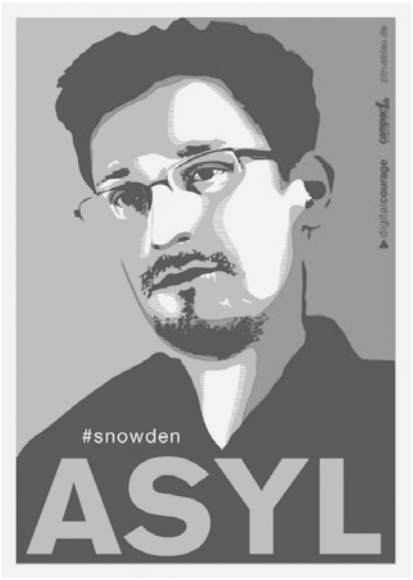
Man soll, man muss Edward Snowden einen stabilen Aufenthaltstitel für Deutschland geben. Man soll, man muss Edward Snowden freies Geleit gewähren. Das alles ist rechtlich möglich. Stattdessen tun die Politiker der großen Koalition so, als sei die Macht Amerikas in Deutschland rechtssetzend. Deutschland braucht Aufklärung über die umfassenden Lauschangriffe der USA. Aufklärung ist der Ausgang aus selbstverschuldeter Unmündigkeit.

Heribert Prantl hält die Laudatio für den Julia-und-Winston-Award für Edward Snowden, Foto: Bernd Sieker, CC BY

Snowdens Handeln mag in den USA strafbar sein, weil er US-Gesetze verletzt hat; wirklich kriminell sind aber die Zustände und die Machenschaften, die er anprangert. Snowden hat gegen US-Geheimhaltungsvorschriften verstoßen. Ist er deswegen Landesverräter? Nein. Verräter nennen ihn die, die selbst die Grundrechte verraten haben. Snowden hat dem Rechtsstaat Nothilfe geleistet.

Das verdient Anerkennung durch Justiz und Staat, in Deutschland und in Amerika. Snowden hat sich verdient gemacht um die rechtsstaatliche Demokratie. Er hat eine Diskussion in Gang

gesetzt, die hoffentlich dazu führt, dass sich der Rechtsstaat schützt vor den NSA-Angriffen, die ihn gefährden. Einen deutschen Orden braucht er nicht unbedingt; davon kann er nicht abbeißen. Aber er braucht Schutz und Hilfe.



Der Aufkleber „Asyl für Snowden" kann bei digitalcourage (kostenlos) bestellt werden.

„Unglücklich das Land, das keine Helden hat", sagt Galileo Galileis Schüler Andrea Sarti im Theaterstück von Bert Brecht. Amerika kann sich also eigentlich glücklich schätzen, dass es einen Snowden hat. Galilei erwidert seinem Schüler Sarti wie folgt: „Nein. Unglücklich das Land, das Helden nötig hat". Das stimmt auch.

Snowden ist ein Symbol für den zivilcouragierten Widerstand eines Einzelnen gegen ein mächtiges staatliches System. Er ist ein Winzlings-David, der gegen einen Super-Goliath aufgestanden ist. Snowden hat Widerstand geleistet und er tut das immer noch.

Widerstand ist ein Wort, das man mit dem Aufbegehren gegen ein diktatorisches Regime verbindet. Widerstand ist aber auch in der Demokratie, auch im Rechtsstaat notwendig. Widerstand heißt in der Demokratie nur anders: Er heißt Widerspruch, Zivilcourage, aufrechter Gang oder auch einfach – Edward Snowden.

Wenn Widerstand strafbar ist: Widerständler nehmen das in Kauf. Sie nehmen die Strafe oder die Mühen der Flucht in Kauf, um die Verhältnisse zu ändern, um Mißstände und Unrecht zu beseitigen.

Der verstorbene Rechtsphilosoph Arthur Kaufmann hat einmal vom Widerstand in der Demokratie als dem „kleinen Widerstand" gesprochen. Dieser kleine Widerstand müsse geleistet werden „damit der große Widerstand entbehrlich bleibt". Manchmal ist dieser angeblich kleine Widerstand aber ein ganz großer. So ist es bei Snowden. Sein Widerstand erfasst seine ganze physische und psychische Existenz.

Danke, Edward Snowden.

Frank Rosengart

Kategorie *Technik* – Laudatio

Der BigBrotherAward 2014 in der Kategorie *Technik* geht an Die Spione im Auto.

Üblicherweise nennen wir die Schuldigen für Verletzungen der Privatsphäre gerne beim Namen – das ist in diesem Fall allerdings nicht so einfach, weil Hersteller von Kraftfahrzeugen, Zulieferer von Teilen und auch der Gesetzgeber derzeit eine so umfassende Beobachtung von Verkehrsteilnehmern aufbauen, dass die Teile nicht losgelöst voneinander zu betrachten sind. Und nicht zuletzt sind einige der hier beschriebenen Technologien noch nicht serienreif – wir vergeben den Preis darum für das geplante Gesamtwerk, um auf die bedenklichen Tendenzen hinzuweisen.

Fangen wir mit der halbwegs guten Nachricht an: Das auch unter Datenschutzaspekten viel kritisierte europäische Notrufsystem e-Call, das über eine fest ins Auto eingesetzte SIM-Karte im Falle eines Crashs eigenständig einen Notruf absetzen kann, soll – zumindest nach EU-Richtline – keine Datenkrake werden. Denn diese SIM-Karten sollen nicht ständig im Netz eingebucht sein und Datenspuren hinterlassen. Allerdings ist es den Autoherstellern freigestellt, ob sie auf der SIM-Karte nur die reine „e-Call"-Funktion aktivieren, oder auch bereits weitere Dienste freischalten. Dann verhält sich das „e-Call"-Gerät nämlich wie ein normales Mobiltelefon. Der Autofahrer sollte also beim Kauf sehr genau nachfragen.

Es gibt aber andere Entwicklungen rund ums Auto, die uns aus Datenschutz-Sicht große Sorgen machen: Aus den USA herübergeschwappt ist die Diskussion um den verpflichtenden Einbau eines Unfalldatenschreibers (Blackbox), der im Falle eines Unfalls die relevanten Fahrzeugdaten (Geschwindigkeit, Beschleunigung/Verzögerung, Blinker) etc. aufzeichnet. Hierzulande wird der verpflichtende Einbau skeptisch gesehen, nicht zuletzt wegen der Überwachungsmöglichkeiten (Stichwort: Gläserner Autofahrer).

Kaum jemand weiß jedoch, dass in jedem modernen Auto bereits eine solche Blackbox vorhanden ist: Zum Beispiel speichern die Airbag-Steuergeräte fast aller Hersteller bei der Auslösung eben jene Parameter, die für die Auslösung relevant sind. Der Hersteller möchte sich damit dagegen absichern, dass ihm möglicherweise vorgeworfen wird, der Airbag wäre grundlos ausgelöst worden.

Problematisch ist ein solcher Datenspeicher für den Autofahrer: Im Falle eines Unfalls (oder möglicherweise auch schon bei einer schweren Verkehrsregelübertretung) kann die Polizei das Fahrzeug und damit das Steuergerät beschlagnahmen und die dort gespeicherten Daten auslesen. Damit wäre das Aussagever-

weigerungsrecht ausgehebelt. Der Fahrer sollte zumindest über diese „Black Box“ informiert sein.

Neben dem Airbag-Computer speichern noch weitere Geräte im Fahrzeug umfangreiche Daten, die Aufschluss über das Fahrverhalten geben können: Vom Motorsteuergerät bis hin zur Zentralverriegelung. Wenn das Auto in der Vertragswerkstatt an den Service-Computer angeschlossen wird, zieht der Autohersteller wie mit einem großen Datenstaubsauger alle möglichen technischen Daten aus den Bordsystemen. Der Eigentümer des Autos wird darüber nicht aufgeklärt, geschweige denn um ausdrückliche Erlaubnis gebeten. Im Gegenteil: Moderne Autos sind ohne diese Fehleranalyse-Geräte gar nicht mehr zu reparieren, selbst das Service-Scheckheft wird bei einigen Herstellern mittlerweile als Datenbank auf einem zentralen Server geführt. Dabei besteht die Gefahr, dass auch Daten mit Personenbezug das Auto in Richtung Werkstatt verlassen. Die Autohersteller sehen diese Daten ganz selbstverständlich als „ihre“ an, wie VW-Chef Winterkorn bekräftigt.

Als Autofahrer bin ich da allerdings anderer Meinung. Das gibt wohl eine Diskussion beim nächsten Werkstattbesuch.

Frank Rosengart hält die Laudatio
Foto: Fabian Kurz, CC BY

Ein unter Datenschutzaspekten gefährliches Konglomerat sind neue Komponenten von Bord-Entertainment und -Navigationssystemen. Das klassische Autoradio hat ausgedient, vor allem bei teureren Fahrzeugen:

Anstelle eigener Entwicklungen bevorzugen die Hersteller Googles Betriebssystem Android. Mit dem Bordcomputer kann man dann nicht nur Radio hören und sich die schnellste Route anzeigen lassen, sondern über zusätzliche Apps auch sämtliche Google-Dienste und Webbrowser benutzen und sogar E-Mails und Twitter direkt auf dem Bildschirm im Armaturenbrett ablesen oder durch die Autolautsprecher vorlesen lassen. Wenn ich also die Vorzüge eines modernen Bordcomputers nutzen will, werde ich häufig zwangsweise an die Google-Datenkrake verfüttert.

Wie auch bei Mobiltelefonen ist die Google-Software für Android oftmals hochgradig Cloud-basiert: Die Daten werden nicht mehr auf dem Gerät verarbeitet, sondern auf den Servern von Google oder anderen Anbietern. Wenn sich also zum Beispiel der Autofahrer die kürzeste Fahrtroute von A nach B berechnen lässt, wird dies nicht vom Bordcomputer erledigt, sondern die Anfrage geht zum Navigationsdienstleister, wird dort berechnet und wieder zum Auto gesendet. Dabei wird üblicherweise eine persönliche oder zumindest Fahrzeug-Kennung mitgeschickt, über die sich später sehr genau verfolgen lässt, wer wohin fahren wollte.

Als Autofahrer sollte ich mir die Datenschutzbestimmungen der Dienste sehr genau durchlesen, um zu wissen, was mit meinen Daten passiert – Wenn es denn überhaupt eine entsprechende Information gibt:

Audi zum Beispiel leitet bei seinem Premium-Dienst *Audi Connect* sämtliche private Kommunikation via Twitter etc. durch ihre eigenen Server, angeblich aus Sicherheitsgründen. Auf Nachfrage war Audi nicht in der Lage, für diesen Dienst eine in Deutschland gültige Datenschutzerklärung zur Verfügung zu stellen.

Nicht ganz neu sind Ortungsdienste, die seit Jahren in Premiumautos eingebaut sind und im Falle eines Diebstahls das Auto wiederfinden lassen sollen. Sie laufen immer mit und sammeln auch Daten, wenn das Auto nicht gestohlen ist. Einige Hersteller bieten als kostenpflichtigen Zusatzdienst ein permanentes Tracking des Autos an: neugierige Eltern können damit ihre Kinder überwachen oder eifersüchtige Partner dem anderen hinterher spionieren.

Die Technik dafür wird sich – dank e-Call – zukünftig nicht nur in Premiumautos finden, sondern in jedem Personenwagen.

Und besonders spannend sind diese Daten für die Versicherungen – aber spezielle Versicherungstarife, die auf eine Überwachung des Fahrverhaltens setzen, haben wir bereits im Jahr 2007 mit einem BigBrotherAward bedacht.

Liebe Autohersteller, auch wenn ihr euch nicht direkt angesprochen fühlt, weil die Daten ja „von jemand anderem“ gespeichert werden oder die Speicherung gar „gesetzlich vorgeschrieben“ ist – mit diesem BigBrotherAward seid Ihr gemeint. Aber natürlich auch der Gesetzgeber, der zum Beispiel mit Systemen wie e-Call eine technische Basis für Datenschutz-heikle Zusatzdienste schafft.

Herzlichen Glückwunsch zum BigBrotherAward 2014!

BIG BROTHER AWARDS.de

Die Oscars für Datenkraken

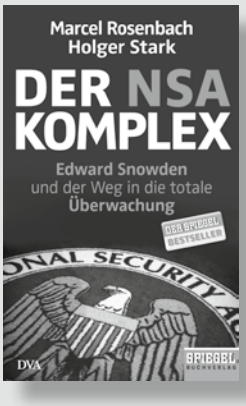
Dietrich Meyer-Ebrecht

Marcel Rosenbach und Holger Stark – „Der NSA–Komplex. Edward Snowden und der Weg in die totale Überwachung"

Nicht viel Phantasie brauche es, so die Autoren Marcel Rosenbach und Holger Stark, sich auszumalen, mit welchem Eifer – und mit welchen gesellschaftlichen Konsequenzen! – die Staatsorgane der ehemaligen DDR die Ausspähtechniken genutzt hätten, über die Geheimdienste heute verfügen. Müssen wir nicht nur auf repressive Regimes wie den Iran schauen, um eine Vorstellung von der Bedrohung für Dissidenten und Regimekritiker, ja selbst für lediglich Nichtlinientreue zu gewinnen? Und können wir sicher sein, dass nicht auch in Staaten, die sich heute auf demokratische Spielregeln berufen und uns die Kontrolle ihrer Geheimdienste zusichern, die politische Situation kippen könnte, vermutlich sogar mit tatkräftiger Unterstützung der Überwachungsapparate? So treffen die Autoren mit ihrem Untertitel dann auch den Kern ihres Anliegens: Sie wollen ihre Leserschaft sensibilisieren für die Brisanz des Themas, für die zwar latente, aber dennoch höchst reale persönliche Bedrohung, für die potenzielle Gefährdung unseres Gesellschaftssystems.

Wie ein Agentenkrimi lesen sich die ersten beiden Kapitel, die Edward Snowdens Geschichte nachzeichnen. Aufwachsen und Schulzeit im regierungsnahen, anonymen Kleinstadtmilieu der Ostküste, Undercoverjob für die CIA in Genf, Wartungsarbeiten im Auftrag der Firma Dell an NSA-Servern in Tokio. Zweifel an der Rechtmäßigkeit der NSA-Operationen kommen ihm mit zunehmenden Einblick in deren Aktivitäten. Sein Wechsel zu *Booz Allen Hamilton* mit Einsatz in einer NSA-Außenstelle in Honolulu verschafft ihm den gesuchten, tiefer reichenden Zugang zu den NSA-Datenbanken. Der Plan für seinen Ausstieg reift. Mit seinem Wissen fühlt er sich moralisch verpflichtet, die Weltöffentlichkeit über den schier unfasslichen Umfang der Erfassung von Kommunikationsdaten und personenbezogenen Informationen, über die Mächtigkeit der Analysewerkzeuge, über illegale Praktiken der NSA und kooperierender Geheimdienste zu informieren – jedoch nicht ohne umfassendes Material, das ihm Glaubwürdigkeit schaffen soll. Und nicht ohne mit seiner Person für seine Enthüllungen einzustehen, mit allen Risiken, um seinem moralischen Anspruch Nachdruck zu verleihen. Am 20. Mai 2013 die gut vorbereitete Flucht über Hongkong, komplizierte konspirative Treffen mit Journalisten[1], Übergabe des Materials, vorläufiges Ende der Flucht in Moskau.

Der mächtigste Geheimdienst der Welt – so betitelt beschreibt das dritte Kapitel, wie Informatik und Kommunikationstechnik der NSA dieses Attribut verschaffen. Erste Ideen einer automatischen Datenanalyse bereits in den 1970ern, Beginn der Entwicklung eines ersten vollautomatischen Überwachungssystems *Thin Thread* Ende der 1980er, erster Online-Einsatz 1998 mit drei Anzapfstellen des internationalen Telefonverkehrs – eine davon in Bad Aibling … Die mit diesen ersten Ansätzen demonstrierten Möglichkeiten wecken den Appetit der Geheimdienstler, stimulieren die Systementwickler und lassen die staatlichen Budgets fließen. Die Digitalisierung der Telefonnetze und das Zusammenwachsen mit dem Internet zu einem globalen und universellen Kommunikationssystem beschert den Geheimdiensten einen fundamentalen Synergieeffekt: das *Goldene Zeitalter der Überwachung* (Kapitel 4) ist gekommen. Wunderbar gebündelt bieten die Glasfaserkabel der Internet-Backbones die Erfassung eines repräsentativen Teils der globalen Kommunikation an – nicht ohne erhebliche technische Hürden natürlich, aber die werden genommen, im Wettlauf zwischen den Geheimdiensten. Mit dem Tempora-Projekt macht sich das britische GCHQ einen Namen. Beiläufig sei bemerkt, dass die NSA die Kollegen vom BND ob ihrer besonderen Expertise im Anzapfen rühmt. (Wie verträgt sich eigentlich der Auftrag zur Spionageabwehr mit der Rolle des NSA-Kooperationspartners?) Interessant ist in diesem Zusammenhang auch die Situation der Industrie. Obschon sie vielfältiges Ziel der Ausspähung ist, dient sie sich den Geheimdiensten mit speziellen Produktentwicklungen und Dienstleistungen an. Internet-Dienstleister lassen den Zugriff auf die Daten ihrer Kunden zu – in vorauseilendem Gehorsam, von Behörden genötigt oder sogar durch Gesetze zur Kooperation gezwungen.



Marcel Rosenbach und Holger Stark (2013): Der NSA–Komplex. Edward Snowden und der Weg in die totale Überwachung. München und Hamburg: Deutsche Verlags-Anstalt und Spiegel-Buchverlag, 383 S., 19,90 €

Dem Ausspähdrang der Geheimdienste kann keine Schranke Halt gebieten, nicht der Respekt vor Persönlichkeiten (das Kanzlerinnen-Telefon) oder internationalen Institutionen (die UN und ihre internationalen Delegationen), nicht die Regeln eines fairen partnerschaftlichen Miteinanders politischer ‚Freunde' (Botschaften, Politiker), nicht legale Grenzen (G10-Gesetz), nicht technische Schutzmaßnahmen (Einbruch in Computer und Netze mit einem Arsenal raffinierter Softwaretools) und selbst physikalische Barrieren nicht (Zugang zu offline-betriebenen Systemen mit strafbaren Mitteln wie Einbruch oder Erpressung). Auffallend – und nachvollziehbar! – ist das Interesse der Ausspäher auch an Finanztransaktionen, über die nicht nur illegale Geschäfte aufgespürt sondern auch Wirtschaftsprozesse ausspioniert werden. Kaum nötig, aber ausgesprochen hilfreich arbeiten wir den Geheimdiensten auch noch durch einen leichtfertigen Umgang mit unseren Daten und Datengeräten zu, indem wir ein Fülle intimer Informationen über unsere Bewegung, Kontakte, Ansichten und Absichten arglos und ahnungslos preisgeben – das Smartphone als Taschenwanze. „Aber bedeutet das Speichern schon Überwachung?" fragt Hans-Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz in seiner SPIEGEL-Rezension dieses Buches suggestiv, und er wiegelt ab, „Ich bin der Überzeugung, dass selbst ein Nachrichtendienst wie die NSA überfordert wäre,

wollte sie den gesamten Telekommunikationsverkehr der Deutschen mitlesen und mithören."[2] Auch ohne Rosenbach und Stark gelesen zu haben, sollte Maaßen wissen, dass längst nicht mehr Analysten anhand von gegebenen Verdachtsmomenten ermitteln, sondern Big-Data-Tools mit hoch entwickelten Statistikmethoden und Mustererkennungsverfahren den Verdacht gleichsam erzeugen – und wehe dem, der unbescholten ins Visier dieser Automaten gerät …

Ein weiteres Kapitel widmen die Autoren der Rolle, die die digitale Ausspähung im Kontext der aktuellen Kriegsführungsdoktrin spielt. Die Szenarien beschreiben den Einsatz von Cyberoperationen in Phasen: Phase 0 *Shaping* dient dem Erkennen der Absichten des Gegners mittels geheimer Zugänge zu dessen Netzwerken. In Phase 1 *Abschreckung* werden dem Gegner mit spürbaren Operationen ‚die digitalen Muskeln gezeigt'. In Phase 2 *Dominieren* werden den Gegner schwächende Operationen eingeleitet, wie Sabotageakte oder die Übernahme der Kontrolle über kritische Systeme über die in Phase 0 implementierten Zugänge. Unter besonderer Geheimhaltung steht eine Spezialeinheit der NSA für *Tailored Access Operations* (TAO), deren Aufgabe es ist, für diese Zwecke Schwachstellen in Computersystemen zu finden, um sie unbemerkt ausbeuten zu können. An einer Reihe aktueller Beispiele wird die erfolgreiche Arbeit der TAO-Truppe der ca. 1000 im Staatsdienst arbeitenden Hackern beschrieben.

In einer schizophrenen Situation befindet sich unsere Deutsche Regierung, wenn sie zugeben muss, dass ihr Geheimdienst bestens und mannigfaltig mit der NSA zusammen arbeitet, und zugleich eingestehen muss, dass auch ihre Bürger, ihre Institutionen, ihre Industrie Opfer einer Ausspähung durch NSA und GCHQ sind, die selbst vor der Kanzlerin nicht halt macht. Der NSA-Chef General Alexander bestreitet dies auch gar nicht, und er beruft sicht dabei auf die Rechtsprechung eines geheimen nationalen Sondergerichtes, dessen elf Richter auf der Basis des *Foreign Intelligence Surveillance Act* (FISA) über die Ausspähungsanträge der NSA entscheiden. *Unter Freunden lautet* die Überschrift dieses Kapitels, in dem die Autoren unter anderem beschreiben, wie sie zur Aufdeckung und Verifizierung der Überwachung des Kanzlerinnen-Telefons beigetragen haben und in dem auch die Naivität und Scheinheiligkeit unserer Politiker gebrandmarkt wird.

Das Resümee ziehen die Autoren in ihrem abschließenden Kapitel *Wir Überwachten*. Dieses Kapitel ist ein Plädoyer an die Regierenden, ihre Verpflichtung zum Schutz ihrer Bürger wahrzunehmen, ihnen ihr verbrieftes Recht auf Unverletzlichkeit der Privatsphäre zuteil werden zu lassen. Es ist ein Plädoyer an die Bürger, Eigenverantwortlichkeit zu übernehmen, dem Abbau ihrer Freiheit nicht apathisch und tatenlos zuzusehen – unter Medienkompetenz müssen endlich auch die Fähigkeiten verstanden werden, Kommunikationsverhalten im Bewusstsein des für einen scheinbar kostenlosen Komfort zu zahlenden Preises zu steuern und aktiven informativen Selbstschutz zu betreiben. Dieses Kapitel ist auch eine Warnung vor dem Hineinschliddern in eine total überwachte Gesellschaft. Es ist eine Warnung vor dem *Deep State*, vor einem parlamentarisch nicht mehr kontrollierbaren Einwirken der Geheimdienste auf politische Entscheidungen.

Mit umfassend recherchierten Fakten und Zahlen machen Rosenbach und Stark das gigantische Ausmaß des Überwachungskomplexes begreifbar. Auf der Grundlage fundierten Sachwissens legen sie seine Entstehung, seine Mechanismen und sein Potenzial dar. Auf gut 300 Textseiten geben die Autoren eine detaillierte Übersicht über die im zurückliegenden Jahr in einer Vielzahl von Einzelaspekten veröffentlichten Fakten, decken interessante Zusammenhänge auf und schaffen ein gesamtheitliches Verständnis. Dabei konnten sie sich als SPIEGEL-Autoren auf die Auswertung von Edward Snowden offen gelegter Geheimdokumente der NSA und des britischen GCHQ stützen, soweit diese dem SPIEGEL zugänglich waren. Das macht ihr Buch besonders authentisch. Eine themenbezogene Chronik der Ereignisse vom Zeitpunkt von Snowdens Untertauchen bis zum Abschluss der Arbeiten an ihrem Buch (Februar 2014), ein Glossar der technischen Sachbegriffe und Abkürzungen, ein detailliertes Register und – für diese beiden Autoren selbstverständlich – ein umfassendes Quellenverzeichnis machen dieses flüssig zu lesende Werk zu einem wertvollen Sachbuch. Es erscheint zu einem für die politische Debatte günstigen Zeitpunkt – eine *wichtige Hilfe* für die Opposition im NSA-Untersuchungsausschuss, so Christian Ströbele.

Anmerkungen

1 *Spannend wird die Darstellung des Journalisten sein, der eine zentrale Rolle für die Übergabe und Ausbreitung des Materials spielt, Glenn Greenwald. Gerade ist sein Buch erschienen „Die Globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen", Droemer Verlag, München 2014*

2 *DER SPIEGEL 14/2014, http://www.spiegel.de/spiegel/print/d-126267966.html*

Bildnachweis Titelseite

von links nach rechts und von oben nach unten:

Arbeitsplatz der Zugansage im Bielefelder Hbf; Foto: ACBahn, CC BY
Kritisches Graffiti des Street-Art Künstlers Banksy in London; Foto: oogiboig, CC BY-SA 2.0
Weihnachtsmarkt in Stuttgart; Foto: Stefan Hügel, CC BY
Mobile Videoüberwachungsanlage in einem Kleinbus der Polizei; Foto: Daniel Arnold, CC BY-SA 3.0
Piktogramm Videoüberwachung nach DIN 33450
Hinweis auf Video-Überwachung in der Dresdner Innenstadt; Foto: N-Lange.de, CC BY-SA 3.0
Kamera am Gebäude der Commerzbank Hamburg-Altstadt; Foto: GeorgHH
Logo „The day we fight back"; Photo Credit: alecperkins, CC BY
Split Screen einer Videoüberwachungsanlage im MVG Muesum in München; Foto: Mattes, CC BY-SA 3.0

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.

FIfF-Mailinglisten

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 Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

FIfF online

Das ganze FIfF
www.fiff.de

Twitter-Accounts
@FIfF_de und
@FaireComputer
@FIfF_AK_RUIN

FIfF-Blog
http://blog.faire-computer.de/

FIfF-Beirat

Michael Ahlmann (Bremen); **Peter Bittner** (Bad Homburg); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); 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); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (München); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr**. Klaus-Peter Löhr** (Berlin); **Werner Mühlmann** (Oppung); 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); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Prof. Dr. **Dietrich Meyer-Ebrecht** (stellv. Vorsitzender) – Aachen
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Rainer Rehak – Berlin
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Sara Stadler – Bremen

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	1 100 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck, Sara Stadler
Schwerpunktredaktion	Stefan Hügel, Peter Bittner
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de.* Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	Fotomontage zur Überwachung/Videoüberwachung, Bildnachweis Seite 65
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.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

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

FrOSCon 2014 – Free and Open Source Software Conference
23. und 24. August 2014 in St. Augustin

MRMCD14 – MetaRheinMainConstructionDays
5. bis 7. September 2014, Hochschule Darmstadt

Datenspuren 2014
13. bis 14. September in Dresden

Freedom not Fear 2014
26. bis 29. September in Brüssel

FIfF-Jahrestagung
7. bis 9. November 2014 in Berlin
„Der Fall des Geheimen – Blick unter den eigenen Teppich"

FIfF-Kommunikation
3/2014 »Gender«
Britta Schinzel, Sara Stadler
Redaktionsschluss 1.8.2014

W&F – Wissenschaft & Frieden
1/14 – Konfliktdynamik im »Globalen Norden«
2/14 – Gewalt(tät)ige Entwicklung
3/14 – Künste, Krieg und Frieden
4/14 - Soldat

vorgänge - Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#203 (3/13) – Religiöse Sonderrechte auf dem Prüfstand
#204 (4/13) – Polizei
#205 (1/14) – Sicherungsverwahrung
#206 (2/14) – Überwachung

DANA – Datenschutz-Nachrichten
1/14 – Konzerndatenschutz
2/14 – Internet der Dinge

Das FIfF-Büro

Geschäftsstelle FIfF e.V.
Ingrid Schlagheck (Geschäftsführung) und Sara Stadler
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*

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

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

Ask Zelda!

Seit einem Jahr erfahren wir immer mehr darüber, wie wir durch Nachrichtendienste ausgespäht werden. Die Menschen dahinter bleiben – abgesehen von einzelnen Führungspersönlichkeiten, wie General Keith Alexander – im Dunkeln. Klar, das liegt in der Natur der Sache.

Doch es gibt offenbar auch Dokumente, die ein kleines Schlaglicht auf die Menschen hinter der Überwachung werfen: Menschen wie Du und ich, Menschen, die die gleichen kleinen täglichen Probleme am Arbeitsplatz haben, und sich auf ihren Feierabend freuen.

Für all diese kleinen Probleme gibt es Hilfe: „Ask Zelda!", eine Kolumne im Intranet der NSA hilft offenbar bei allen täglichen Problemen. Bei Fragen der angemessenen Kleidung am Arbeitsplatz, wenn Mineralwasser aus dem gemeinsamen Kühlschrank verschwindet, wenn Vorgesetzte nicht auf E-Mails antworten – Zelda weiß Rat. Sogar, wenn der Chef seine Mitarbeiterinnen und Mitarbeiter bespitzelt, kann Zelda die richtigen Hinweise geben: „*Wow, that takes ‚intelligence collection' in a whole new – and inappropriate – direction.*" Man möchte zustimmen und kann sich dennoch des Gefühls nicht erwehren, einer Satire aufzusitzen.

Die Geschichte gibt der Überwachung eine „menschliche" Seite – und macht gleichzeitig eines deutlich: Letztendlich ist es nicht die anonyme Organisation, sondern es sind die Menschen die in ihr arbeiten. Menschen, die Werte haben, nach denen sie leben.

Spione, die sich darüber beklagen, ausspioniert zu werden: Sind sie sich dessen bewusst, was sie den ganzen Tag tun?

Und damit wären wir wieder bei der alten Frage nach der Verantwortung für das individuelle Handeln.

Referenzen

The Intercept, Peter Maass (2014): The NSA Has An Advice Columnist. Seroiusly. https://firstlook.org/theintercept/article/2014/03/07/nsa-advice-columnist-seriously/

Plakat zum Film: „Spion für Deutschland", Quelle: Familienarchiv Ellgaard, CC BY-SA 3.0

Stefan Hügel