14. Buckower Mediengespräche 2010: Mein Avatar und Ich. Die Interaktion von Realität und Virtualität in der Mediengesellschaft

Ralf Lankau

# Das Ich ist eine Datenspur.
## Identität als Realität im digitalen Kokon

Vorspann (Folie 1: Robin Sage):

Robin Sage ist 25 Jahre alt und Absolventin der Elite-Universität MIT (Massachusetts Institute of Technology, Cambridge). Sie arbeitet als Analystin für Cybersicherheit der US-Marine. Ihre eMail-Adresse weist sie als Mitarbeiterin von Blackwater aus, einer US-Söldnerfirma. So steht es in ihrem Facebook- und Twitter-Profil. Robin Sage kommuniziert mit US-Militärs, Nachrichtendiensten und Sicherheitsunternehmen aus der IT-Branche. Sie hat innerhalb weniger Wochen Kontakt zu über 300 zum Teil hochrangigen Militärs, Geheimdienst-Agenten, Politikern und Mitarbeitern von Rüstungsunternehmen. Man schickt ihr vertrauliche Informationen, auch aus aktuellen Einsätzen. Sie bekommt interne Dokumente zum Gegenlesen. Die Kollegen, mit denen Sie via Facebook und Twitter kommuniziert, sitzen zum Teil im gleichen Gebäude. Sie bekommt Einladungen zu Konferenzen, auch von extern, und Job-Angebote renommierter Rüstungsbetriebe. Um die berufliche Zukunft von Robin Sage muss man sich keine Gedanken machen , wäre da nicht eine Kleinigkeit ...*[1]

## 0 Die Welt ist eine (Matt)Scheibe: Monitor und Display

Was würden Sie normalerweise tun, wenn Sie den Namen Robin Sage hören und wissen wollen, wer das ist? Die meisten Menschen würden „ins Internet“ gehen, über 90 Prozent davon den Namen „googeln“. Das ist mittlerweile so selbstverständlich geworden, dass man leicht vergisst, dass es diese ganzen Techniken erst seit kurzem gibt. Seit gerade Mal 15 Jahren gibt es das World Wide Web (seit 1995). Google selbst wird nach offizieller Zählweise zwölf Jahre alt (als offizieller Geburtstag gilt der 27. September 1998). Das ist nicht gerade alt für ein „unverzichtbares Medium“.

[1] *Siehe Nachsatz zu Robin Sage am Ende des Dokuments

Gleichwohl sind Internet und World Wide Web mittlerweile als Begriffe ebenso Allgemeingut wie Chatroom, Blog oder Online-Foren. Mobilkommunikation und Web 2.0 („das Mitmach-Web) sind gleichermaßen selbstverständlich geworden wie die euphemistisch „social media" genannten Plattformen wie Facebook oder StudiVZ. Nicht mehr nur „Nerds" und „Geeks"[2] diskutieren stetig über neue Geräte, Techniken und Dienste (neudeutsch „App")[3]. Und das olympische „schneller, höher, weiter" als Grundprämisse scheint gleichermaßen für die Unterhaltungs- und IT-Industrie bzw. deren Produkte zu gelten. Doch der zur Verstetigung der Umsätze notwendige Update-Zwang für Hard- und Software wird von den Nutzern ja willig akzeptiert. Jeden aktuellen Medienhype toppt allenfalls der nächste, schon angekündigte, noch größere Hype. Wahlweise steht man sich für neue Software oder ein neues Smartphone die ganze Nacht die Beine in den Bauch und ist glücklich, wenn man als eine(r) der ersten das Gerät besitzt und in die Kameras der TV-Stationen halten darf. Neu ist gut, digital ist besser, der Fortschritt stetig. Das ist das Geschäft. „The show must go on."

## 1 Digitale Identität: Ariadne-Faden des Web

Niemand macht diese Show aus Altruismus. Der ganze (Marketing-)Zirkus ist Teil des Business. Wie bei jeder Show und jedem Zirkus zahlt das Publikum. Denn wer glaubt, das sei alles „umsonst", ist bestenfalls naiv oder beruft sich auf das vermeintliche „Bürgerrecht, überhaupt nichts zu denken", wie es Max Frisch in seiner Parabel von Biedermann und den Brandstiftern niederschrieb.[4] Biedermann reicht den Brandstiftern sogar die Streichhölzer („Wenn die wirklich Brandstifter wären, du meinst, die hätten keine Streichhölzer?"), mit denen Schmitz und Eisenring die Benzinfässer auf dem Dachboden anzünden und die

2 Nerd: technik- und computeraffiner Streber mit emotionalen und kommunikativen Defiziten; gleiches gilt für den „Geek", der durch intensive Internetnutzung auffällt. Neben negativen Konnotationen im sozialen Kontext werden dem Nerd bzw. Geek oft eine analytische Intelligenz und technische Kompetenz nachgesagt.

3 app: engl: Abkürzung für application, dt.: Applikation, Anwendung

4 Max Frisch: Biedermann und die Brandstifter. Ein Lehrstück ohne Lehre (Uraufführung 1958, Schauspielhaus Zürich). „Biedermann weiß, dass die Welt voller Brandstifter ist: er erkennt sie sogar. Aber er unterdrückt seine Erkenntnis, bis es zu spät ist und auch das eigene Haus brennt." (Hensel, Spielplan, 1966, Bd. 2, S. 939)

ganze Stadt niederbrennen – so wie Internet-Nutzer immer mehr Daten über sich und andere ins Netz stellen, unbemerkt als Datenspur oder freiwillig in Web-2.0-Anwendungen und „social media"-Plattformen.

Daten werden zu Identitäten. Nicht immer im Sinne einer personalisierten Identität, immer aber im Sinne der Mustererkennung und Profilierung. Eine Studie des MIT und der Harvard-University belegt, dass sich aus den Verbindungsdaten der Mobiltelephone einer Versuchsgruppe von 94 Probanden deutlich mehr und bessere Rückschlüsse über Freundschaften und Cliquenbildung generieren ließen als über direkte Interviews. Die in wenigen Wochen mit rein technischen Mitteln analysierten Kontaktdaten waren nicht nur wirtschaftlicher – sie entsprachen dem Aufwand von 330 Tausend Arbeitsstunden oder 38 Jahren klassischer Feldforschung – sondern auch treffsicherer[5]. Lediglich acht Prozent der Kommunikationsdaten einer Gruppe genügen, um eine gesamte Gruppe zu überwachen.[6] Es entsehe eine neue Form der Identifizierung aus Kommunikationsspuren, Ortsangaben und Konsumnachweisen. Es entstehen neue Identitäten:

> „Man erkennt uns, weil wir leben. Die neue Form digitaler Identifizierung weiß zwar nicht, wer wir sind, aber alles über das Mosaik unserer Existenz." (Graff, Man erkennt uns, 2010, S. 9)

Aber bleibt man im Netz nicht anonym, wenn man will? Man kann doch „Nicknames" (frei wählbarer Nutzername) benutzen und auch bei der eMail-Adresse diesen Phanatsienamen einsetzen? Wie sollte jemand wissen, wer ich bin, wenn ich nur als „Klaus-die-Maus@gmx.de" oder „Peter.Pan@gmail.de" auftrete? Die Antwort ist erschreckend einfach: Beim Vertragsabschluss mit Telekommunikationsdienstleistern gibt man notwendig Realnamen mit Adresse, Bankverbindungen etc. an. Diese Realdaten sind für alle Vertragsabschlüsse oder Bestellungen im Netz zwingend. Zum zweiten hat jeder Rechner eine weltweit eindeutige IP-Adresse. Andernfalls wüssten die Maschinen ja nicht, wohin sie die angeforderten Daten schicken sollen. Jede Aktion im Netz kann zu diesem Rechner zurückverfolgt werden. Das ist der Aridane-Faden des Net-

5 Schulzki-Haddouti, Rasterfahndung,, 2010, S. 30

6 Studie der Universität Leuven und der Erasmus Universität Rotterdam; siehe Schulzki-Haddouti, Rasterfahndung, 2010, S. 30

zes: eine eindeutige Rechner-Adresse. Die dazugehörige Verbindung in die Realwelt hat der Provider. Zum dritten ist es ein Leichtes, durch die oben angesprochenen Mustererkennungen jeden Einzelnen durch sein Kommunikationsverhalten und seine Kommunikationspartner selbst dann zu identifizieren, wenn er (oder sie) sich für jeden Internetkontakt konsequent eine neue Identität (neuer Nickname, Passwort und eMail-Adresse) zulegen und jedes mal einen anderen Rechner nutzen würde, etwa in Internet-Cafes. Es dauert nur länger, um das Muster zu identifizieren …

Die Währung des Netzes sind nun mal Daten. Ob diese anonymisiert oder personalisierte gesammelt, gespeichert und benutzt werden, entscheiden die Datensammler anhand ihrer (wirtschaftlichen, politischen) Interessen. Eine Kontrolle über die erhobenen Daten und deren Anwendung durch Dritte oder eine juristische Verfolgung bei Missbrauch ist schwierig. Im Zweifelsfall gelten die Gesetze des Landes, in dem die Webadresse registriert ist oder die Webserver stehen. Wie hieß es schon in den 1980er bei CompuServe und AOL? Es gilt das Gesetz des Staates Ohio. Ein paar Beispiele …

## 2 Facebook-Service: Ungefragte Partnervermittlung

Ohne je Kontakt zu einer Agentur für Partnervermittlung aufgenommen zu haben, kann es Ihnen passieren, dass Ihr Foto, Name, Geburtsdatum und z. B. Hobbys auf einer Kontaktbörse auftauchen. So erging es Facebook-Mitgliedern dieses Jahr. Daten und Bilder erschienen auf der Website von „Smartdate.com“.[7] Legal, weil Facebook die Daten seiner Nutzer laut Allgemeinen Geschäftsbedingungen (AGB) an Unternehmen weitergibt, die zusätzliche Programme entwickeln. Smartdate bietet eine „App“ an, mit der sich die Dating-Funktion direkt aus Facebook heraus nutzen lässt.[8] Dabei übermittelt man nicht nur die eigenen Daten, sondern auch die seiner „Freunde“. Es genügt daher, von einem Facebook-Nutzer als „Freund“ markiert zu sein, um mit Bild

7 o.A., Dating-Seite, 2010, S. 15

8 Siehe www.smartdate.com; Ziel von Facebook ist, Nutzer möglichst lange auf der eigenen Website zu halten, weil nur hier die eingeblendete Werbung abgerechnet werden kann. Daher werden Zusatzfunktionen in die Facebook-Oberfläche integriert.

und Daten in einer Partnervermittlung zu landen.[9] Die Facebook-Betreiber sehen darin kein Problem, gehe es doch darum, möglichst viele Leute zu finden.[10] Einfacher geht es ohne externe Kooperationen. Mit der Funktion „Friendfinder“ übermittelt man seine ganzen Adressbücher an Facebook und bekommt eine Liste mit Namen der bei Facebook aktiven Nutzer zurück (und Facebook eine Liste mit Namen auch nicht aktiver Personen, die gezielt beworben werden können). Eine andere App erlaubt, Personen auf Fotografien zu „taggen“, das heißt, sie mit ihrem Namen und ggf. Profil zu verknüpfen und die persönlichen Daten so zugänglich zu machen, für jeden. Was ist schon dabei? Facebook selbst nutzt ungefragt Bilder seiner Mitglieder für Werbung, laut AGB auch das legal. Und hat nicht Facebook-Gründer Marc Zuckerberg gleich generell das „Ende der Privatsphäre“ verkündet? Das hat er zwar nicht wörtlich gesagt.[11] Aber sind Privatsphäre und Datenschutz nicht ohnehin überbewertet?

> „Was Facebook mächtig gemacht hat, war nicht der laxe Umgang mit Kundendaten. Es war vielmehr die von Beginn an massenhaft vorhandene Bereitschaft der Nutzer, sich digital preiszugeben.“ (Kittlitz, Traum, 2010, S. 33)

## 3 Spieglein, Spieglein an der Wand: Narziss und Echo

Zur Preisgabe privater Informationen, zur Aufgabe der Privat- oder sogar Intimsphäre gehören schließlich beide Seiten: der Anbieter solcher Dienste und die Nutzer.[12] „Wir spiegeln uns doch alle in den Blicken und Gesten der anderen“ intoniert Konstantin Wecker in einer seiner Balladen, nur dass man bei

9 Wenn Sie Glück haben, entdecken Sie diesen Eintrag selbst und können reagieren. Andernfalls müssen Sie möglicherweise ihrer Partnerin/ihrem Partner erklären, wie Ihre Daten auf diese Website kommen. Haben Sie sch schon mal überlegt, wie schwer es ist, nachzuweisen, dass man etwas nicht getan hat?

10 Ethan Beard, bei Facebook zuständig für die Zusammenarbeit mit anderen Websites; zit. n. o.A., Dating-Seite, 2010, S. 15

11 Das Originalzitat von Marc Zuckerberg im Interview mit Michael Arrington (TechCrunch) vom 8. Januar 2010 in San Francisco lautet: “Menschen sind einverstanden damit, Informationen über sich mit anderen zu teilen und werden immer offener zu immer mehr Menschen. Die sozialen Normen hier haben sich in der Zeit entwickelt”. Dazu titelte ein Redakteur im Weblog "ReadWriteWeb": "Facebook's Zuckerberg says the age of Privacy is over". Das ist zugespitzt, passt inhaltlich aber zu den Einstellungen zur Privatsphäre bei Facebook.

12 In den USA ist es unter Jugendlichen üblich, den Beziehungsstatus oder das Ende von Beziehungen über Facebook zu veröffentlichen.

Personenverzeichnissen im Web kein direktes Gegenüber mehr hat und als perfekter Narziss agiert. Als Spiegel dient der Monitor und das phantasierte, eigene Profil. Als Echo dient Feedback der wohlmeinenden „Freunde“. Denn Reaktionen auf die Selbststilisierung im Netz lassen sich viel leichter steuern als in der analogen, oft so mühsamen „Realität“ mit tatsächlichen Individuen.

Kontakte und „Freundschaften“ im Netz steuert man per Mausklick. „Sozialkontakte“ lassen sich ebenso spielend einrichten wie beenden.

> „Das 21. Jahrhundert hat also nicht mehr das Problem des Massenkonformismus durch Massenmedien, sondern das Problem der Gleichgesinntheit in digitalen Echokammern.“ (Bolz, Clickes Schmied, 2010, S. V2/3)

Wer hingegen bedenkt, dass „Identität“ immer (auch) ein Ergebnis von Konflikten ist, wird erahnen, was dem digitalen Narziss fehlt: Ein im positiven Sinn streitbares Gegenüber. Das „Ich“ formt sich (auch) durch Widerspruch und Dissens. So ist die gern als Argument benutzte These der „Horizonterweiterung“ durch die Kontakte im „globalen Dorf“ eine Fiktion, wie Ethan Zuckerman, Informationssoziologe am Berkman Center für Internet and Society der Harvard Law Schoul feststellt:

> „Der vermeintlich offene, aktive Austausch mit der Welt im Netz ist in Wahrheit nur die einseitige Suche nach Unterhaltungsprodukten, Meinungen und Gesprächspartnern, die sich mit den eigenen, längst vorgefassten Geschmacksmustern decken. Der Horizont wird enger.“ (Zuckerman, zit. n. Kreye, 2010, Bluesschema, S. 11)

Aber vielleicht ist der immer enger werdende Horizont der sich selbst bespiegelnden Narzisse mit den „Internet-Freunden“ als Echo das Ziel des Individuums in einer, wie es stereotyp vorgetragen wird, „komplexer werdenden Welt“? Vielleicht sind die medial rundum eingespeichelten, mit Jederzeit- und Überallangeboten gut unterhaltenen Konsumisten genau die Menschen, die am besten zurecht kommen im digitalen Wunderland des 21. Jahrhunderts? Vielleicht sind digitale Identitäten sogar die Rettung für das „erschöpfte Selbst“, so die These von Alain Ehrenberg[13]: Von allen sozialen, religiösen und politischen Zwängen und Funktionen befreit, muss sich das Individuum ständig selbst

13 Alain, Ehrenberg [Selbst, 2008]: Das erschöpfte Selbst. Frankfurt. Suhrkamp, 2008

konstruieren und konstituieren. Während man im realen Leben ob der Komplexität scheitert, erlauben digitale Plattformen und virtuelle Identitäten zumindest zeitweise die Fiktion einer gelingenden und sich selbst genügenden Existenz. Das nach positiver Zustimmung selektierte …

> „… Zeugnis der „Freunde“ nährt die Hoffnung, dass der Facebook-Avatar seinem Original entsprechen könnte. Dessen Zusammengesetztheit einzig nach den eigenen Bedürfnissen mehrt zwar die Gefahr einer nachhaltigen Spaltung der Nutzer in digitales und real verbliebenes Selbst. Der Verzicht auf Privatsphäre scheint jedoch ein geringer Preis für eine gefundene Identität …“ (Kittllitz, Traum, 2010, S. 33)

## 4 Pfadfinders Traum: Mein Smartphone weiß, wo ich bin

Wie unbedarft darf man gegenüber den Anbietern von Hard- und Software, wie vertrauensselig gegenüber IT- und Kommunikationsdienstleistern sein? Anders gefragt: Wie genau haben Sie die Allgemeinen Geschäftsbedingungen (AGB) Ihres Internetproviders oder Mobilfunkanbieters studiert (diese seitenlange, kleingedruckte, in Juristendeutsch verklausulierte Zumutung)? Sie haben immerhin zugestimmt. Sie bestätigen, den Vertrag gelesen zu haben, auch wenn Sie das Häkchen nur setzen, weil sonst Gerät oder Dienst nicht funktionieren oder man Software nicht installieren kann. In diesen AGB steht, was der Provider mit Ihren Daten machen darf. Smartphones etwa senden permanent Positionsdaten, scannen nebenbei aktive WLAN-Netze und übermitteln deren Stärke an Datenbanken. Daraus lässt sich die Position und Reichweite der Netze, der jeweilige Standort des Smartphone-Trägers und dessen Bewegungsprofile berechnen.[14] Schließlich …

> „… ist es praktisch, wenn die Hardware automatisch erkennt, wo man gerade ist (…). Auch wenn die Daten anonymisiert gespeichert werden, sollte einem schon bewusst sein, dass man sich hier als Versuchskaninchen an einer Art Vorratsdatenspeicherung beteiligt. Wer mit seinem Smartphone immer nebenbei online ist, sendet damit auch die Standortdaten seines Lebens unbemerkt im

[14] Ziel der „location based services“ ist die Verbindung von „sozialen Netzwerken“ und ortsabhängigen Diensten bzw. Werbung. Bei Facebook heißt der Dienst „Facebook Places“

> Hintergrund an den jeweiligen Hersteller. Was das Bundesverfassungsgericht bei der Vorratsdatenspeicherung als verfassungswidrig erkannte, wird hier zum Feature erklärt.“ (Beckedahl, Apple, 2010, S. 40)

Man kann diese Funktion abschalten. Standardmäßig ist sie aktiviert. Die wenigsten Nutzer wissen (die wenigsten Nutzer wollen wissen), welche Daten sie permanent weiterleiten. Denn ist es nicht ein schönes Feature, wenn ich auf meinem Smartphone nur Googlemaps aufrufen muss, um zu wissen, wo ich gerade bin? Der kleine rote Punkt da auf dem Display – schau, da(s) bin ich! Und gleich angezeigt bekomme, wo ich essen, trinken, shoppen kann?

## 5 007 Blogger Bond: Wikileaks und Project Vigilant

Was ist schon dabei, wenn Apple, Google oder ein Provider wissen, wo man gerade ist oder war. Oder dass der Provider weiß, mit wem man telefoniert oder zusammensitzt, welche Websites man angeschaut, welche Downloads man abgerufen oder an wen man Dateien geschickt hat? Es kommt darauf an.

Beispiel Wikileaks. [15] Wikis sind Internetseiten, bei denen viele Einzelpersonen an einem gemeinsamen Projekt arbeiten wie z.B. bei Wikipedia, der Online-Enzyklopädie. Leak bedeutet „Leck, undichte Stellen“. Wikileaks definiert und versteht sich als weltweite Internetplattform, auf der geheime Dokumente veröffentlicht werden. Entscheidend ist, dass publizierte Dokumente nicht zum Absender zurückverfolgt werden können. Informantenschutz ist ein konstituierender Aspekt des investigativen Journalismus.[16]

Im April 2010 veröffentlichte Wikileaks ein US-Militär-Video über den Beschuss und die Tötung von irakischen Zivilisten.[17] Am 25 Juli 2010 publizierte Wikileaks US-Kriegstagebücher aus Afghanistan – selbstredend ohne Zustim-

15 Zum Selbstverständnis von Wikileaks siehe http:(//wikileaks/org/wikileaks/de

16 Ob Wikileaks diesem Anspruch gerecht werden, wird kontrovers diskutiert. Kritik wird von mehreren Seiten laut: Es seien, so ein Vorwurf, keine neuen Informationen zu Irak oder Afghanistan, sondern nur die Bestätigung des bereits Bekannten, wenn auch durch amtliche Dokumente. „Reporter ohne Grenzen“ kritisiert die Veröffentlichung von Klarnamen afghanischer Informanten, die damit den Taliban ausgeliefert würden. Dazu kamen Vorwürfe angeblicher sexueller Übergriffe des Wikileaks-Gründers Assange gegenüber zwei Frauen in Schweden. Die Klagen wurden allerdings von der schwedischen Staatsanwältin innerhalb von 24 Stunden zurückgezogen. Assange spricht von einer „Sexfalle“ der US-Geheimdienste, vor der man ihn gewarnt habe. Es gibt wohl mehrere „Wahrheiten“.

mung des Militärs. [18] Die Folge waren (und sind) massive Drohungen gegen die Betreiber dieser Plattform in der nationalen Presse. Selbst das aus der McCarthy-Ära bekannte Reizwort der „unamerikanischen Umtriebe“ wird bemüht. Wikileaks-Mitarbeiter wie der amerikanische Hacker und Internetaktivist Jacob Applebaum wurden bei der Rückkehr in die USA verhaftet. [19] Julian Assange, der australische Gründer von Wikileaks, meidet seither die USA. Die Daten wurden auf Server in Schweden transferiert, wo ein weit gefasstes Presserecht gilt. Als zusätzlichen Schutz publizierten die Betreiber von Wikileaks ein mit Passwort verschlüsseltes Archiv mit weiteren Dokumenten.[20] Wird einer der Betreiber von Wikileaks verhaftet, gibt es genug Kopien dieser Archivdatei und des Passworts, um das Archiv trotzdem zu veröffentlichen. Über die Inhalte des Archivs lässt sich trefflich spekulieren – und so „nebenbei“ die zweite Währung des Netzes (außer Daten) einstreichen: Aufmerksamkeit.

Der Schutz der Wikileaks-Betreiber mag so funktionieren. Aber hier geht es um eine andere Form von „leak“. Der Soldat Bradley Manning wurde inhaftiert. Manning arbeitete bei einem amerikanischen Kommando in Bagdad und hatte Zugang zu besonders geschützten Daten im SIRPnet des Militärs. Angeblich hat er die bei Wikileaks publizierten Dateien kopiert und an den Hacker Adrian Lamo weitergegeben. Dieser informierte das FBI. Ein Soldat begeht Geheimnisverrat und wird interniert. So lautet die offizielle Version.

---

17 Collateral Murder, 5. April 2010, http://wikileaks.org/wiki/collateral_murder.5_Apr_2010; Download als *.mp4 und Flash-Datei; Zugriff: 17. August 2010

18 Afghan War Diary, 2004-2010; http://wikileaks.org/wiki/Afghan_War_Diary._2004-2010, Zugriff am 20. August 2010

19 Der US-Bürger Jacob Applebaum wurde im Juli 2010 bei der Rückkehr aus Amsterdam auf dem Flughafen Newark, New York verhaftet und drei Stunden verhört. Laptpop und seine drei mobile phones musste er abgeben, nur das Laptop bekam er zurück. Ob Daten kopiert wurden, ließ sich nicht feststellen. taz vom 2. August 2010; http://www.taz.de/1/netz/netzpolitik/ artikel1/wikileaks-publiziert-lebensversicherung/; Zugriff am 19.8.2010

20 Dateiname: „ insurance.aes256“; Größe: 1,4 GB (Gigabyte). Die 90.000 Dokumente des Afghan War Diary waren als gepacktes Archiv knapp 75 MB (Megabyte) groß. Die Archivgröße sagt allerdings nichts über die Inhalte oder die Anzahl der Dateien aus. Videos etwa sind „Speicherfresser“. AES ist ein Verschlüsselungsstandard (Advanced Encryption Standard) mit einer Schlüssellänge von 128, 192 oder 256 Bits. AES ist in den Vereinigten Staaten für staatliche Dokumente der höchsten Sicherheitsstufe zugelassen.

Und inoffiziell? Adrian Lamo, so die Version eines Forbes-Redakteurs, sei ein Sicherheitsspezialist des geheimen „Project Vigilant“[21]. Das sei ein bereits 1994 von der Privatwirtschaft finanziertes Projekt zur Intersicherheit, bei dem 600 Freiwillige mit dem FBI (Federal Bureau of Intelligence) und der NSA (National Security Agency) zusammenarbeiten. Gespeichert werde der gesamte Netzverkehr von zwölf überregionalen Providern mit mehr als 250 Millionen Rechnern (IP-Adressen). (Die Nutzer haben über die AGB selbstredend zugestimmt.) Manning war demnach nicht naiv, sondern benutzte nur eine der 250 Millionen IP-Adressen.[22] Damit wäre Manning lediglich einer der vielen Amerikaner, deren Aktivitäten im Internet auch nachträglich lückenlos rekonstruiert werden können. Aus Kommunikationsdaten wird eine reale Anklage.

Oder war vielleicht doch alles ganz anders? Vigilanten sind Menschen, die Selbstjustiz üben (aus dem lateinischen vigilans: wachsam) und das „Gesetz in die eigenen Hände“ nehmen. Sie sind konservativ, mit einem Hang zu Militarismus, Waffen und geheimen Bünden. So verwundert es nicht, dass die Existenz des Geheimprojekts ebenso geleugnet wird (no such project) wie die NSA (interner Spott: no such agency).[23] Amerika ist auch das El Dorado der Verschwörungstheorien und -theoretiker.

## 6 Auf-(!)gezeichnete Zukunft: Google und CIA

Existent hingegen ist Google, das die Nutzer nicht nur mit ständig neuen Anwendungen (Google Books, Google Maps, Google Streetview) beglückt – und quasi nebenbei die europäischen Vorstellungen von Urheberrechts- oder Datenschutzbestimmungen aushebelt.[24] Existent sind auch die Geheimdienstler der

21 Nichts zu sehen gibt es unter der URL www.projectvigilant.us. Wie so oft wird man auf einer inhaltsleeren Seite dazu aufgefordert, einen eigenen Account anzulegen (Username, Passwort, und natürlich eMail-Adresse). Ist das ganze Projekt ein „fraud (Betrug)“ oder ein „hoax (Jux) oder das Fehlen von Inhalten Teil der Strategie? Man könnte sich amüsieren bei diesem Versteckspiel, wären nicht die zivilen Opfer im Irak ebenso real wie der Inhaftierte Manning.

22 Borchers, Wikileaks, 2010, S. 31

23 Siehe z.B Wired.: www.wired.com/Threatlevel/2010/08/lamo-classified-documents/; Examiner, San Francisco: www.examiner.com/technology-in-san-francisco/secret-goup-aids-fight-against-terror; Die Zeit: www.zeit.de/digital/internet/2010-08/wikileaks-manning-geheimnprojekt ; Zugriffe 20.8.2010

24 Das Procedere ist immer gleich: Google schafft Fakten durch z.B. das Scannen von Büchern oder das Fotografieren ganzer Straßenzüge und „erlaubt“ den Betroffenen

CIA (Central Intelligence Agency). Bei dem Projekt mit dem sprechenden Namen „Recorded Future“ (aufgezeichnete Zukunft; sic) investieren Google und CIA (über das Unternehmen In-Q-Tel) gemeinsam und kooperieren direkt. Aufgabe von „Recorded Future“ ist die Vorhersage von Trends (perspective analysiys) und Ereignissen, die durch die Auswertung von öffentlichen und veröffentlichten Daten (und ein paar zusätzlichen Quellen, s.u.) gewonnen werden.[25]

Die Kooperation zwischen einem öffentlichen Datensammler wie Google mit militärischen Geheimdiensten erweist sich als ausgesprochen hilfreich. Können so doch neben der „OSint (Open Source Intelligence)“ – der Auswertung öffentlich zugänglicher Quellen wie Nachrichtensendungen, Tageszeitungen und Internetbeiträgen – auch die sonst eher nicht öffentlichen Daten des „SigInt“ (Signal Intelligence: das Abhören der Signale des Feindes) und des „HumInt“ (Human Intelligence: durch Spione zusammengetragene Informationen) zusammengeführt und mit entsprechender Software ausgewertet werden. Hilfreich ist zudem, wenn ergänzend Verzeichnisse und Exportdaten von Handelsgütern, Finanztransaktionen oder Kommunikationsdaten der Telekommunikation hinzugezogen werden. Dabei werden Daten zusammengeführt und verdichtet. Je nach Fragestellung und Ziel variieren die Methoden der Mustererkennung. Daraus werden, je nach Bedarf, Identitäten, Bewegungsprofile, Finanztransaktionen und personalisierte Handlungsmuster.

Man mag das für den militärischen Bereich als notwendig in Kauf nehmen. Da die Entwicklung dieser aufwendigen Analyse-Tools nur für militärische Aufgaben allerdings zu teuer wäre, suchen und propagieren die Entwickler Einsatzgebiete in der Privatwirtschaft. Aufgaben sind etwa die Beobachtung der Konkurrenz, das Erkennen von Wirtschaftsspionage oder das Erstellen von typischen Nutzerprofilen zu Kommunikations- oder Konsumverhalten definierter

nachträglich, Einspruch zu erheben. De facto werden die Daten jedoch jeglicher Kontrolle oder Nachvollziehbarkeit entzogen (die Server stehen in den USA). Bei Forderung auf Unterlassung muss man, etwa bei Einsprüchen gegen StreetView, selbstredend die eigenen Daten preisgeben. So erreicht Google sein Ziel (verifizierte Daten bzw. Zuordnung von Gebäuden und Bewohnern) sogar bei denen, die juristisch gegen das Unternehmen vorgehen. Google-Gegner verifizieren Ihre Daten selbst, innerhalb der von Google gesetzten Frist. Praktisch.

25 Siehe dazu die Selbstdarstellung unter www.analysisintelligence.com, die mit dem Slogan „Smart open source intelligence alalysis & government analytics“ werben.

Zielgruppen. Das „Scannen des Netzes“ und das Zusammentragen von Daten aus verschiedenen Quellen wird zur Dienstleistung.[26]

Privatfirmen werden (hoffentlich) nicht auf alle Datenquellen zugreifen können, die den Geheim- und Nachrichtendiensten zur Verfügung stehen. Wie mächtig diese Mustererkennung trotzdem bereits ist, um Persönlichkeits-, Kommunikations- und Bewegungsprofile Einzelner zu erstellen, hat Frank Rieger[27] in einem Gutachten für das Bundesverfassungsgericht ausgeführt.[28] Dieses Gutachten war einer der Gründe für das Verbot der Vorratsdatenspeicherung in Deutschland.

## 7 Tyrannei der Transparenz: Küss meinen Avatar

Der Datenberg wächst, die internen Verknüpfungen ebenfalls. Personenbezogene Daten sind eine Ware, die jeder zwangsläufig generiert, der digital kommuniziert. Selbst die komplette Verweigerung technischer Kommunikation hilft nicht, da genug Nutzer die Namen ehemaliger Klassenkameraden, von Freunden oder Kollegen „googeln“ und damit den Grundstein für ein neues Profil legen. Andere stellen ungefragt Bilder von Bekannten ins Netz und „taggen“ sie (ordnen Namen und Profile zu). Ergänzt wird die Personalisierung durch immer bessere Software zur Gesichtserkennung.

Das ergibt ganz neue Fragestellungen, etwa wenn man auf Bildern „identifiziert“ wurde, aber gar nicht die abgelichtete Person ist? Oder wenn aus frei vagabundierenden Daten ein Profil und eine (virtuelle) Identität generiert wird, die man weder erstellt noch inhaltlich beeinflusst hat, die aber als digitale Identität durchs Netz geistert – und für wahr genommen wird, etwa bei der Arbeits- oder Wohnungssuche? Wie weist man ggf. nach, dass man jemand nicht ist, ohne dadurch genötigt zu werden, ein korrektes Profil mit dann gleich verifizierten Daten anzulegen?[29]

---

26 Borchers, Raketen, 2010, S. 29

27 Frank Rieger ist Geschäftsführer eines Kommunikationsunternehmens und Sprecher des Chaos Computer Club, Hamburg. In der FAZ publiziert er regelmäßig zu Themen der IT-Sicherheit.

28 Rieger, Nicht verstecken, 2010, S. 33. Die Bildunterschrift lautet: „Sie wissen alles über jeden: Unsere Verbindungsdaten genügen, um unser Leben zu durchschauen.“

29 Einer meiner Namensvetter ist der „Stalker“ von Celle“, dem gerichtlich untersagt wurde, sich dem gemeinsamen Kind einer Exfreundin zu nähern.

Die Empfehlung eines Kollegen aus der IT-Sicherheit auf die Frage, wie man auf diese ganzen automatisch generierten Profile reagiere, lautet: Lege eigene Profile an, viele, mit dem echten Namen, aber fiktiven Daten und Viten und mit im Internet geklauten Bildern. Lege Profile an mit falschen Namen, aber ein paar echten Bildern. Die einzige Chance gegen die Profilierung sei die Vervielfachung der eigenen Person. Was bei Richard D. Precht noch als Frage formuliert ist „Wer bin ich und wenn ja wie viele?“[30], dient als direkte Handlungsanweisung: Werde viele! Nur Identitäten im Plural stellen sicher, dass aus digitalen Identitäten nicht auf die reale geschlossen werden kann.

Doch vielleicht hilft Versteckspielen nicht und das „Netz“ wird zur ultimativen Kontrollinstanz, auch des eigenen Handelns? So zumindest hat es Eric Schmidt – neben den beiden Gründern Sergey Brin und Larry Page der dritte Chef von Google – 2009 im US-Fernsehen formuliert:

> „Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es nicht tun.“ (Bernau, Schmidt, 2010, S. 4)

Andernfalls findet jeder es bei Google. Schmidt weiß, was er sagt. Schmidt weiß, was Google entwickelt und was technisch möglich ist. In Frage steht, ob er realisiert, was er als Subtext und „Google’sches Imperativ“ intoniert:

> Bei allem, was Du tust, frage Dich: Willst Du, dass es bei Google im Internet steht? Tue nur, was bei Google veröffentlicht werden kann.

Lesen Sie den Satz ruhig noch einmal. Google gibt konkrete Handlungsanweisungen. Das Firmenmotto von Google „Don’t be evil“ (Tue nichts böses) bekommt so eine ganz andere Reichweite und Bedeutung.

## 8 Negation der Tyrannei: Transparenz als Bürgerrecht

Gibt es kein Entkommen? Doch. Es gibt sogar einen erfreulich knappen und präzisen Vorschlag zur Umkehrung der derzeitigen Verhältnisse, den Norbert Schneider, Direktor der Landesanstalt für Medien NRW (LfM) in Düsseldorf, formuliert hat, um aus der derzeit praktizierten Transparenz des „gläsernen

[30] Richard David Precht: Wer bin ich und wenn ja wie viele? München: Goldmann, 2007

Bürgers“ eine Transparenz der Datensammler und ihrer Datensammlungen zu machen:

> „Für diese Regulierung [die gesellschaftliche Kontrolle der Datensammlungen und Datensammler; rl] genügen im Grunde zwei Paragraphen. Paragraph 1: „Die Daten eines Menschen sind sein Eigentum. Wenn sie jemand nutzen möchte, dann zu den Bedingungen, die dafür allgemein festgelegt werden. Wer sie zur Kontrolle eines Menschen nutzt, verletzt seine Würde. Paragraph 2 könnte lauten: „Der gesamte Datenverkehr muss für den Datengeber jederzeit transparent sein.“(Schneider, Menschenleser, 2010, S. 33)

Es muss zur Pflicht für die Datensammler werden, die erhobenen und generierten Daten offen zu legen. Es muss Bürgerrecht werden, diese Daten einsehen und ggf. löschen zu können. Dabei bleibt es allen Digitaljüngern und Fortschritts-Euphorikern unbenommen, ihre Daten auf Websites oder „social media“-Plattformen in beliebiger Zahl und Menge zu streuen und sich in allen nur erdenklichen Foren und Formen zu entblößen.[31]. Aber es darf niemand zur Preisgabe von persönlichen Daten genötigt werden. Bei der Vermittlung von „Medienkompetenz“ wird man daher auch die vermeintlich „sozialen“ Netzwerke thematisieren und Schülerinnen und Schülern vermitteln, dass es weder Notwendigkeiten noch Zwänge gibt, sich digital zu prostituieren. Medienkompetenz heißt, eigene Grenzen zu ziehen und „Nein“ zu sagen. Denn:

> „Das Erzeugen von Gruppendruck ist die Kernkompetenz sozialer Netzwerke. (...) Einige wenige betreiben zur kurzfristigen Gewinnmaximierung den Umbau der sozialen Normen, mit unabsehbaren Folgen.“ (Rieger, Datensatz, 2010, S. 33)

## 9 Zum Diktat: Diktatur des digital Möglichen

Die Pflicht zur Transparenz der gespeicherten Daten und die Möglichkeit zur kostenlosen Einsicht durch jeden Bürger (wie bei Schufa-Einträgen) ist der erste, das Recht, zumindest die privatwirtschaftlich gespeicherten Daten löschen zu lassen der zweite Schritt, der für den mittel- und langfristigen Erhalt unserer demokratischen Gesellschaft zwingend erforderlich ist. Man muss die „Tyran-

[31] „Facebook ist Selbstprostitution auf der Basis von Informationsgier.“, Prof. Dr. Ernst Pöppel, Professor für Medizinische Psychologie München, zit. n. Haupt, 2010, S. 35

nei der Transparenz“ – Oder haben Sie etwas zu verbergen? – gegen die Datensammler richten. Es muss unattraktiv werden, mehr als nur die absolut notwendigen Daten zu speichern. Das „Jederzeit und Überall“ der digitalen Medien muss sich umkehren in eine „Jederzeit und Überall-Kontrolle der Kontrolleure“ durch die Bürger. Wer personenbezogene Daten speichern will, hat gegenüber dem Bürger eine Bringschuld über Umfang, Notwendigkeit und Dauer. Der Verkauf dieser Daten wird untersagt. Aus der Ware „personenbezogene Daten“ wird ein (wieder) geschütztes Gut, die informationelle Selbstbestimmung als Gut und Recht wieder eingesetzt.

Ziel ist, den Datensammel- und Kontroll-Wahn zu unterbrechen, der alle Bürger nur noch als Datenquellen definiert, die möglichst genau zu erfassen und zu kontrollieren seien. Der Weg in den Kontrollstaat:

> „Der Weg von analog zu digital ist auch der Weg von einer Disziplinar- in eine Kontrollgesellschaft (Deleuze). (…) Der Mensch als Datenträger wird, indem er lesbar gemacht wird, auch steuerbar, vorhersehbar, kontrollierbar. Er wird, ohne davon irgendetwas zu wissen, um Objekt einer auf Dauer gestellten Rasterfahndung …“ (Schneider, Menschenleser, 2010, S. 33)

Rasterfahndung für alle 82 Millionen deutschen Terroristen.[32] Noch deutlicher formuliert der kanadische Software-Entwickler und Bürgerrechtler Brad Templeton[33] die Gefahren des „cloud computing“, bei dem alle, auch persönliche Daten nicht mehr lokal auf dem eigenen Rechner, sondern auf irgend einer „Server-Farm“ im Netz gespeichert werden – im direkten Zugriff der Provider und (Geheim-) Dienste. Die menschliche Geschichte sei eine Geschichte von Polizeistaaten. Wer seine Daten im Netz speichere wie bei Facebook, Gmail oder Twitter, sei bereits funktionierendes Element eines autoritären Systems:

> „Wenn wir im Namen der Bequemlichkeit heute die Infrastruktur eines Überwachungsregimes auf unseren Computern installieren, ist dessen Realisierung später nur noch eine politische, keine technologische Frage mehr.“ (Templeton, zit. n. Häntzschel, Notarzt, 2010, S. 14)

---

32 „In Deutschland leben 82 Millionen Terrorristen. Du bist einer davon.“ parodiert ein Videospot die Vorratsdatenspeicherung (www.du-bist-terrorist.de)

33 Website von Brad Templeton mit Beiträgen und Interviews: www.templetons.com

Der Aufbau einer technischen Infrastruktur zur vollständigen Überwachung der Bevölkerung: Biedermann reicht den Brandstiftern nicht nur Lunte und Streichhölzer, sondern trägt selbst die Benzinfässer auf den Speicher und zündelt selbst? Oder was wird wohl aus der „Diktatur des digital Möglichen“[34] in Verbindung mit dem willigen, das Denken verweigernden Bürger?

> „Was mit der Unterscheidung von privat und öffentlich auf dem Spiel steht, ist die Idee der bürgerlichen Freiheit. (...) Und vielleicht wird man über die bürgerliche Identität im Zeitalter des Internet bald sagen können: Jeder bemerkenswerte Mensch arbeitet gegen sein eigenes Profil.“ (Bolz, Clickes Schmied, 2010, S. V2/3)

## Nachsatz zu Robin Sage

Robin Sage hat nie existiert. Robin Sage ist ein weiblicher Avatar, den der IT-Experte Thomas Ryan erfand und bei einer Hackerkonferenz vorstellte.[35] Hinter den Bildern und dem Profil einer „attraktiven Kollegin“ (die recht freizügigen Fotos stammen von einer Pornoseite) gelang es ihm, vertrauliche Informationen und Dokumente von Soldaten im Einsatz, amerikanischen Geheimdiensten und Rüstungsfirmen zu erhalten. Ziel des Projekts war es, deutlich zu machen, wie unbedarft und vertrauensselig selbst Geheimnisträger sind, die sich in der „direkten“ Kommunikation über sogenannte soziale Netzwerke vor einer Kollegin produzieren.

## Nachsatz zu Google

Sergej Brin stellte im August 2010 in San Francisco neue Funktionen der Suchmaschine vor. Google Instant z.B. liefere „Antworten“, bevor überhaupt die Frage gestellt werden kann. Dazu blendet „Instant“ verkaufte (!) Suchbegriffe schon beim Eintippen einzelner Buchstaben und Silben ein. Viele Nutzer folgen den Links. „Wir wollen aus Google die dritte Hälfte Ihres Gehirns machen“ verkündet Brin[36]. Man darf das als Drohung verstehen.

---

34 o.A, (ward): Briefszene, in: FAZ vom 1. Juli 2010, S. 35

35 Thomas Ryan: Getting in bed with Robin Sage, Black Hat Conference, uly 28-29 2010, Cesars Palace Las vegas

36 Bernau, Finden, 2010, S. 1

*Literatur*

Zeitungskürzel: BaZ: Badische Zeitung; FAZ: Frankfurter Allgemeine Zeitung; SZ: Süddeutsche Zeitung)

o.A.[Dating-Seite, 2010, S. 15]: Facebook-Fotos auf Dating-Seite. „Smartdate“ zieht Nutzer in eigene Datenbank – ohne Wissen der Betroffenen, in: FAZ vom 20. Juli 2010, S.15

Beckedahl, Markus [Apple, 2010]: Digitale Gesellschaft: Apple speichert die Daten unseres Lebens, in: FAZ vom 24. Juli 2010, S. 40

Bernau, Varina [Schmitt]: Profil. Eric Schmitt. Chef des umstrittenen Datensammel-Konzerns Google, in: SZ vom 20. August 2010, S. 4

Bernau, Varina [Finden, 2010]: Finden, was man gar nicht sucht. Googles neue Funktion erfreut auch die Werbewirtschaft, in: SZ vom 10.9.2010, S. 1

Bolz, Norbert [Clickes Schmied, 2010]: Jeder ist seines Clickes Schmied. Warum uns mit der Privatheit in der Internet-Gesellschaft auch die bürgerliche Freiheit abhanden kommt, in: SZ vom28./29. August 2010, S. V2/3

Borchers, Detlef [Wikileaks, 2010]: Erstaunliche Wendung in Sachen Wikileaks. Stammt das Irak-Video doch vom Soldaten Manning?, in: FAZ vom 4. August 2010, S. 31

Borchers, Detlev [Raketen, 2010]: Raketen vorhersagen. Wieso Google und CIA eine gemeinsam Firma haben, in SZ vom 30. Juli 2010, S. 29

Ehrenberg, Alain [Selbst, 2008]: Das erschöpfte Selbst. Depression und Gesellschaft in der Gegenwart, Frankfurt: Suhrkamp, 2008

Erd, Rainer [Deutsche Daten, 2010]: Deutsche Daten auf Geheimservern der USA. Google und viele andere Internetunternehmen missachten Internationale Abkommen, (Außenansicht), in: SZ vom 23. August 2010, S. 2

Graff, Bernd [Man erkennt uns, 2010]: Man erkennt uns, weil wir leben. Die neue Form digitaler Identifizierung weiß zwar nicht, wer wir sind, aber alles über das Mosaik unserer Existenz, in SZ vom 25. Januar 2010, S. 9

Hamann, Götz [Listen, 2010]: Facebooks unsichtbare Listen. Der Internetkonzern speichert und nutzt auch viele Daten von Nichtkunden. Kann man ihm das zukünftig verbieten?, in; Die Zeit, Nr. 35 vom 26. August 2010, S. 22

Haupt, Frederike [Selbstprostitution, 2010]: Facebook ist Selbstprostition auf der Basis von Informationsgier. Ein Gespräch mit Ernst Pöppel, Professor für Medizinische Psychologie in München, in: FAZ vom 11. Mai 2010, S. 35

Hensel, Georg [Spielplan, 1966]: Spielplan. Schauspielführer von der Antike bis zur Gegenwart, 2 Bde, Darmstadt, Wien: Dt. Buchgemeinschaft, 1966

Kittlitz, Alard von [Traum, 2010]: Der Traum vom idealen Leben. Als der Facebook-Gründer Marc Zuckerberg verkündete, das Zeitalter der Privatsphäre sei vorbei, war die Empörung groß. Das heißt allerdings nicht, dass er mit der These daneben lag, in: FAZ vom 6. August 2010, S. 33

Kreye, Andrian [Bluesschema, 2010]: Das Bluesschema für Vorlesungen. Ted in Oxford: Quantenphysik, Comedy und das regionale Internet, in: SZ vom 15. Juli 2010, S. 11

Meckel, Miriam [Informationsmüll, 2010]: Abfuhrtermine für Informationsmüll, in: FAZ vom 5. August 2010, S. 33

Precht, Richard David [Wer bin ich, 2007]: Wer bin ich und wenn ja, wie viele? München, Goldmann, 2007

Rieger, Frank [Krieg, 2010]: Krieg nach Zahlen, in FAZ vom 7. August 2010, S. 29

Rieger, Frank [Nicht verstecken, 2010]: Du kannst Dich nicht mehr verstecken, in: FAZ vom 20. Februar 2010, S, 33f

Rieger, Frank [Datensatz, 2010]: Der Mensch wird zum Datensatz, in: FAZ vom 15. Januar 2010, S. 33

Schneider, Norbert [Menschenleser, 2010]: Die digitalen Menschenleser. Wer sich im Netz preisgibt, wird zu einem Menschen zweiter Schöpfung: Er gibt den digitalen Göttern Gelegenheit, jede Kontrollmöglichkeit auszunutzen. In: FAZ vom 10. August 2010, S. 33

Schulzki-Haddouti, Christiane [Rasterfahndung, 2010]: Alltägliche Rasterfahndung, in: c’t, Heft Nr. 2, 2010, S. 30-31

Stämpfli, Regula [Macht,2007]: Die Macht des richtigen Friseurs. Über Bilder, Medien und Frauen, Brüssel: Bartleby& Co., 2007

Wefing, Heinrich [Welt, 2010]: Die neue Welt ist nackt. Vielleicht ist die Privatsphäre tatsächlich eine Idee von gestern. Aber wir brauchen sie dringender denn je, in: Die Zeit, Nr. 34, vom 19. August 2010, S. 4

Weizenbaum, Joseph, [Computer, 1977]: Die Macht der Computer ist die Ohnmacht der Vernunft, Frankfurt am Main: Suhrkamp, 1977