

1. Man erkennt uns, weil wir leben

Süddeutsche Zeitung, 25.01.2010, 10:43 2010-01-25T10:43:00 CEST+0100,
<http://www.sueddeutsche.de/computer/912/501171/text/>

[Von Bernd Graff](#)

Wir erleben gerade das Entstehen der digitalen Identifizierung. Sie weiß zwar nicht, wer wir sind, aber alles über das Mosaik unserer Existenz.

Unsere Vorstellungen von Datensicherheit und unsere Forderungen zum Schutz der Privatsphäre [...] [definieren] sich über klassische Merkmale: Name, Geburtsdatum, Wohnort, Signatur und unveränderliche 5 biometrische Kennzeichen wie Narben, Gebiss, Augenfarbe und Fingerabdrücke. Diese Parameter beschreiben den Menschen anhand von Personalien, die [...] genau einem Individuum zugeschrieben werden können. Es sind also gewissermaßen Zuschreibungen von außen: Der zu identifizierende Mensch wird - das Passiv steckt schon im Begriff - erkennungsdienstlich behandelt. Er muss nichts tun, kann passiv bleiben bei seiner Identifizierung. [...]

10 Wir erleben jedoch gerade das Entstehen einer neuen Form der Identifizierung und damit das Entstehen neuer Identität. Dieser Identifizierung ist die alte statische Identität der Merkmale einer Person herzlich egal. Nicht einmal mehr das. Denn die Instanzen dieser neuen Identifizierung haben kein Herz. Es sind Maschinen: Computer, gefüttert mit gewaltigen Datenbeständen, die von Typisierungsalgorithmen durchkämmt werden. Ihr Wissen, ihre Potentiale und vermutlich auch ihre Macht stecken in Datenbanken, die sie durchforsten. Wir 15 selber sind es, die diese Datenbanken kontinuierlich füllen. Denn wir hinterlassen digitale Spuren: Kommunikationsspuren, Ortsangaben, Konsumnachweise. Je länger wir die Speicher füllen, desto feiner und detaillierter wird das Mosaik unserer Existenz. Diese neue Form der Identifikation also ist dynamisch, prozessual. Man erkennt uns, weil wir leben.

Erste Ergebnisse solcher Typisierung liefert der Internethändler Amazon bereits: "Menschen, die dieses Buch 20 gekauft haben, interessieren sich auch für diese Bücher." Inzwischen ist es in einem Experiment gelungen, allein aufgrund der Twitter-Verbindungen von Mitgliedern des US-Kongresses deren Parteizugehörigkeit nachzuweisen. Dazu wurden die Tweets, die Twitter-Texte, nicht gelesen, und es wurden auch keine Namen offen gelegt. Es wurde einzig analysiert, welche Teilnehmer miteinander und wie oft sie miteinander kommunizierten. Analysiert wurde wie in der Äsop-Fabel, in welcher ein Esel daran erkannt wird, in welcher 25 Gesellschaft er sich befindet. Mat Morrison, der Mann, der diese Twitter-Analyse durchgeführt, hält übrigens die Frage, ob man Parteizugehörigkeit errechnen könne, für beantwortet.

Wissenschaftler des Massachusetts Institute of Technology und der Harvard University untersuchten in einer Studie über 94 Personen, ob man deren Freundschaften und Cliquesbildung besser aus Interviews der Beteiligten oder aus deren Handy-Verbindungsdaten ermitteln könne. Die Forschergruppe fand heraus, dass 30 die Verbindungsdaten aufschlussreicher waren als die Befragungen. Wie Christiane Schulzki-Haddouti in der Fachzeitschrift c't dazu weiter ausführt, entsprachen die für diese Studie in wenigen Wochen mit technischen Mitteln erhobenen und analysierten Daten dem Aufwand von 330.000 Wissenschaftler-Arbeitsstunden - oder einer klassischen Feldforschung von fast 38 Jahren.

Die neuen Techniken der Identifizierung von Menschen verlangen geradezu nach derartig großer Zahl und 35 langer Dauer der Aufzeichnungen. Je mehr Daten von Menschen die Maschinen verarbeiten können (und sie können es immer schneller), je unterschiedlicher diese Datentypen tatsächlich sind und je länger der Zeitraum ist, über den sie erfasst werden, umso feiner wird das Raster zur Erkennung von Stereotypen. Umso genauer können sie Muster im Verhalten der Menschen erkennen und prognostizieren. [...]

Letztlich geht es dabei gar nicht mehr um Informationen über einzelne Personen und deren Verhalten. Es geht 40 um Trends, Neigungen, Tendenzen, Wahrscheinlichkeiten, Muster, die sich eben aus den Spuren Vieler ableiten

lassen. Menschen mittleren Alters, die zweimal täglich zu kaum variierenden Zeiten dieselben Wegstrecken mit dem Auto zurücklegen, dürften aller Voraussicht nach einer geregelten Arbeit nachgehen. Wenn sich diese Menschen im Internet plötzlich für Wickeltische und Babywindeln interessieren, ist es nicht unwahrscheinlich, ihnen bald Autositze für Kleinkinder verkaufen zu können.

45 Wenn man will, kann man diese Datenwölzer schon "Bewusstseinsmaschinen" (Jaron Lanier in der SZ vom 23./24. Januar) nennen. Und es stimmt: Sie arbeiten wie Profiler, wie Ermittler, die Schlüsse für künftiges Handeln ziehen aus einer Welt der hinterlassenen Spuren und Indizien. Doch ihre mutmaßliche Intelligenz steckt im Code, der auch nur so schlau ist wie die Programmierer, die ihn geschrieben haben. Was signifikant an uns sein soll, muss man den Maschinen schon sagen, da sie lediglich dumpfe Schürfarbeit leisten.

50 Doch je mehr Telekommunikationsdaten und Internet-Verkehrsdaten mit den dazu gehörenden Ortsangaben verknüpft werden können und je langfristiger solche Daten erhoben und -vor allem - zusammengeführt werden, umso besser lassen sie sich analysieren und umso auskunftsfreudiger sind sie. Selbst dann, wenn sie anonyme Massen rastern. Darum können die "big player" unter den Datensammlern, Facebook etwa und Google, ohne mit der Wimper zu zucken behaupten, dass sie selbstverständlich die personenbezogenen Daten
55 (unsere alte Identität) für schützenswert erachten, während sie andererseits jede Form menschlicher Verkehrsdaten abgreifen, (berechnen, aufbereiten), speichern, um passgenaue Konsumenten-Profile daraus zu extrahieren.

Die kürzeste Definition von Privatsphäre stammt von Samuel D. Warren und Louis D. Brandeis aus dem Jahr 1890. Sie lautet: "Privacy is the right to be let alone." Das Recht, in Ruhe gelassen zu werden. Diese

60 Privatsphäre korrumpieren wir gerade beständig selber, weil wir es sind, die das Datenmaterial liefern, auf das die Maschinen warten. Nein, das muss man nicht per se schlimm finden. Man sollte nur wissen, dass nahezu alle unsere Lebensartikulationen inzwischen von einer Technik registriert werden, die diese nach einprogrammierten Kriterien in ihre Matrix sortiert. Data-Mining ist Human-Mining. Das vermögen wir (und die guten alten Datenschützer) indes noch kaum zu begreifen. [...]

65 Eines nicht allzu fernen Tages könnte es daher passieren, dass uns ein Vertreter dieser Firma [23AndMe, GD] über eine personalisierte Werbung angeht: "Wir wissen zwar nicht, wer Sie sind, aber wir wissen, dass Sie mit sehr hoher Wahrscheinlichkeit an Alzheimer erkranken werden. Andere Patienten mit diesem Befund haben sich in dieser Situation für diese Medikamente interessiert."

Arbeitsauftrag:

1. Erläutere den Unterschied zwischen "statischer" und die "prozessual dynamischer" Merkmalerfassung in Bezug auf Effizienz und Erkenntnisinteresse.
2. Berücksichtige die Ergebnisse aus dem Tracker Manual: welche Fragestellungen erlaubt das Tracking im Internet, wenn man Data Mining-Methoden zur Auswertung heranzieht?
3. Was meint demnach der Begriff "Human Mining" und worauf will der Autor mit dem Ausdruck "die guten alten Datenschützer" hinaus?

2. Der gläserne Bürger 2.0 – Das neue Profil des Menschen

Artikel aus der Süddeutschen Zeitung Nr 126, 05./06.06.2010. Von Bernd Graff

Um das zum Teil aggressive Geschäftsgebaren von Firmen wie Google und Facebook und ihren oft kritisierten laxen Umgang mit den persönlichen Daten ihrer Kunden (uns allen!) zu verstehen, muss man bereit sein, die beiden Seiten eines Paradoxons gleichzeitig zu denken. Die beiden Seiten des Paradoxons sind:

Es ist nicht der Einzelne interessant, sondern die möglichst große Masse

5 Die Masse an sich ist nicht wichtig, sondern nur die Bewegungen, Artikulationen, Interessen und Kommunikationen der Einzelnen in dieser Masse

[...] Man könnte es auf den Nenner bringen: Firmen wie Google und Facebook wollen alles von allen wissen, um mit größtmöglicher Wahrscheinlichkeit Aussagen über einen Einzelnen machen zu können und sein Verhalten zu prognostizieren. Die Aggressivität dieser Firmen resultiert daraus, dass ihr Erfolg eben daran geknüpft ist, 10 möglichst viel von möglichst vielen erfassen und speichern zu müssen. In der Sprache von Facebook, hier in einer Aussage von Sheryl Sandberg, der Wirtschaftsverantwortlichen des Unternehmens (COO), klingt das so: „400 Millionen Nutzer sind nett. Aber wir wollen die ganze Welt vernetzen.“ Der Sound von Hybris! Hier ist sie Geschäftsmodell. Man kapiert es ja zuerst gar nicht: Bislang – in der guten alten Analogwelt – musste eine Person erkannt und identifiziert werden, um sie aufspüren und gegebenenfalls ergreifen zu können. Der Staat, 15 seine Ordnungsdienste, das Militär, die Medizin und die Arbeitswelt, und vielleicht auch noch Briefzusteller hatten Interesse daran, einen Einzelnen in der Masse ausfindig zu machen. [...]

So funktionieren Facebook und Google aber nicht – sie kehren die Verfahren der Identifizierung (und ihr Interesse daran!) gerade um. Sie wollen die Masse, sie wollen das Rauschen, ja sie benötigen es sogar. Je größer und disparater, je lieber! Das aber ist nur sinnvoll ausbeutbar und seine Ausbeutung ist nur möglich, weil 20 Computer (tatsächlich sind es Rechenplantagen mit dem Stromverbrauch von Kleinstädten) in Tausenderpotenzen schneller durch gigantische Datensätze wühlen können als Menschen – und weil sie unbeaufsichtigt, unangeleitet und un gelenkt lernen können.

„Unsupervised learning“, so heißen die neuen Verfahren des Profilings tatsächlich. Während die alten deduktiven Profiling-Methoden immer nur so schlau waren wie die Hypothesen, die ihnen zugrunde gelegt 25 waren („Lass uns nach Wurstessern mit karierten Mützen suchen!“), überlassen die neuen, induktiven Verfahren des Data-Minings die einlaufenden Datensätze völlig den Computern. Sollen die doch erst mal machen! Sollen die doch möglichst große Zahlen durchkämmen und anschließend ausspucken, was sie so gefunden haben, sprich: welche Muster sie in den Sätzen erkannt haben! Gesucht wird nach nichts, gefunden wird aber immer etwas. Und es werden Korrelationen sichtbar, die man nicht einmal ahnen kann. Etwa: 30 Menschen, die X ihre Liebesspeise nennen, den Sport Y niemals betrieben haben und nichts gegen weiße Socken einzuwenden haben, wählen Z. Die so geschürften Ergebnis-Muster werden jetzt als Hypothesen für Prognosen verwandt, also wieder zurückgespeist, um sie nach klassischen Profiling-Verfahren zu validieren – oder eben zu verwerfen. Dann beginnt alles wieder von vorne – in der Zwischenzeit sind ja auch immer neue Terabyte an Daten (immer bereitwillig eingepflegt von uns Nutzern!) dazugekommen, welche die von 35 Maschinen induktiv gewonnenen, synthetischen Hypothesen stützen oder kippen können.

Dieses zweite Verfahren gebiert völlig neue Formen des Wissens und der Erkenntnis. Ihm liegt nicht mehr eine menschengemachte Hypothese zugrunde, gewonnen aus Kenntnis, Kausalannahmen, Absicht und Erfahrung, die dann einer Prüfung standhalten muss. Die stochastischen Verfahren des maschinellen Profilings finden gerade Zusammenhänge, die man nicht erwartet oder zu finden gehofft hat, an die man nicht einmal denken 40 konnte. Und genauso funktionieren Google und Facebook: Ihr Erfolg ist der Algorithmus, mit dem disparate Daten analysiert werden, ist die im Nebel der großen Zahl stochernde Statistik. Doch niemals zuvor in der

Geschichte des Wissens wurde danach so exakt gewusst. Der Informatiker Jaron Lanier hat in der SZ darum von „Bewusstseinsmaschinen“ gesprochen.

„Das ist die Welt“, so hat es Chris Anderson, der Chefredakteur und -denker von Wired, in einem 45 bemerkenswerten Essay einmal formuliert, „in der ungeheuren Menge von Daten und angewandte Mathematik jedes andere Werkzeug menschlicher Hypothesenbildung ersetzen. Vorbei sind Soziologie und Linguistik und jede Theorie des menschlichen Verhaltens. Vergesst Taxonomie [Klassifikationsschema, GD], Ontologie [Lehre vom Seienden] und Psychologie! Wer weiß schon, warum Menschen Dinge tun? Der Punkt ist doch nur, dass sie sie tun und dass wir sie erfassen und messen können – mit einer nie da gewesenen Akkuratheit. Ist die 50 Datenmenge nur groß genug, dann sprechen die Zahlen für sich selber.“ Der Statistiker George Box hat Ende des letzten Jahrhunderts erklärt: „Alle unsere Modelle sind falsch, aber einige sind ganz nützlich!“ Peter Norvig, der Direktor der Forschungsabteilung von Google, hat diese Maxime bereits umformuliert: „Alle unsere Modelle sind falsch, aber wir haben sowieso immer mehr Erfolg damit, ganz ohne sie auszukommen.“

Darum also schicken sich Google und Facebook an, zu sogenannten Infrastrukturseiten des Internets zu werden 55 und immer mehr und immer unterschiedlichere Dienste anzubieten, bzw. wie bei Facebook: immer mehr externen Anbietern zu ermöglichen, ihre Dienste mit dem Stammangebot zu verknüpfen. Es geht nicht in erster Linie um Services für die Nutzer-Kunden, die diese an das Unternehmen binden sollen. Es geht um die Details, die Diversität und Verästelung ihrer Daten und Kommunikationen: Wohin gehen sie in Web und Welt, was hören und was essen sie, wie finden sie es, was mögen sie nicht – und was sagen sie darüber zu anderen (deren 60 Reaktionen auch wieder relevant sind, weil auch sie erfasst und jeweils profiliert wurden).

Etwa: Natürlich ist es „nett“ und relativ aufschlussreich, dass Nutzer auf Facebookseiten über einen Geo-Tagging-Dienst irgendein Restaurant empfehlen. Aber ist eine solche Empfehlung nicht ungleich wertvoller (sprich: vermarktbarer), wenn man dazu noch weiß, dass sie häufig von Alkoholikern, aber nie von Nichttrinkern kommt, oder selten von Fettleibigen, aber oft von Leptosomen? [...]

65 Googles und Facebooks Maschinen lernen gerade, Korrelationen herzustellen, keine Kausalzusammenhänge. Sie erkennen keine Bedeutung. Sie verfeinern Muster. [...] Diesseits dieser Welt aber muss ich die Bedeutung, meine Bedeutung, behaupten und unvermindert verteidigen. Andernfalls wird das Ich zur bewusstlosen Ware. [...].

Keine Sorge, das tun wir schon. Eines nicht allzu fernen Tages könnte es daher passieren, dass uns ein Vertreter 70 dieser Firma über eine personalisierte Werbung angeht: "Wir wissen zwar nicht, wer Sie sind, aber wir wissen, dass Sie mit sehr hoher Wahrscheinlichkeit an Alzheimer erkranken werden. Andere Patienten mit diesem Befund haben sich in dieser Situation für diese Medikamente interessiert."

Arbeitsauftrag:

1. Erkläre den im Text beschriebenen Gegensatz von Masse und Einzelnen: Welche Rolle spielt die Masse? Beziehe dabei die Ergebnisse aus letzter Stunde bzgl. statischer vs. dynamischer Merkmalerfassung ein
2. Erläutere die Rolle der Kausalität bei den "herkömmlichen" Wissenschaften und beim "unsupervised learning" (maschinelles Lernen)

3.eCommerce

aus: Gebhard Dettmar, *Knowledge Discovery in Databases, Teil I - Methodik und Anwendungsbereiche*, <http://www.community-of-knowledge.de/beitrag/knowledge-discovery-in-databases-teil-i-methodik-und-anwendungsbereiche/>

Im eCommerce und eBusiness machte man, schneller als manchen Beteiligten lieb sein konnte, die Erfahrung, dass steigender Web-Traffic nicht automatisch wachsende Käuferzahlen nach sich zieht. Erfolgsentscheidend auf diesem Gebiet sind vielmehr zuverlässige Konzepte zur Kundenbindung. Man geht derzeit von einem durchschnittlichen Kostenaufwand zwischen 150 - 300 Dollar pro gewonnenem Neukunden im eCommerce aus. Es ist also aus ökonomischer Sicht zwingend erforderlich, dass ein überwiegender Teil eines so aufwändig rekrutierten Kreises auch Wiederholungskäufe tätigt. Diese Konzepte zu entwickeln ist das primäre Aufgabenfeld des electronic Customer Relationship Managements (i. f. eCRM), das eine datengetriebene Informationsgewinnung über die Personen zum Inhalt hat, die man seinem Kundenstamm anzufügen beabsichtigt. Es klingt bereits an, dass hier Selektion im Spiel ist: bevor man Datenmaterial mit dem Ziel der Informationsgewinnung für eine beabsichtigte Kundenbindung erhebt, muss man wissen, wen man binden möchte - und wen nicht.

Arbeitsauftrag: Welchen Zweck verfolgt die "Kundensegmentierung"?

3.1. [Data Use Policy](#) → How advertising and Sponsored Stories work

We do not share any of [your information](#) with advertisers (unless, of course, you give us permission). As described in this policy, we may share your information when we have removed from it anything that personally identifies you or combined it with other information so that it no longer personally identifies you.

We use the [information we receive](#), including the information you provide at registration or add to your account or timeline, to deliver ads and to make them more relevant to you. This includes all of the things you share and do on Facebook, such as the Pages you like or key words from your stories, and the things we infer from your use of Facebook.

When an advertiser creates an ad, they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other [information we receive](#) or can tell about you and other users. For example, an advertiser can choose to target 18 to 35 year-old women who live in the United States and like basketball. An advertiser could also choose to target certain topics or keywords, like "music" or even people who like a particular song or artist.

[...] If the advertiser chooses to run the ad (also known as placing the order), we serve the ad to people who meet the criteria the advertiser selected, but we do not tell the advertiser who any of those people are.

Arbeitsauftrag:

1. Lies den Text und überlege, welche Gefahren dem Facebook-User entstehen, wenn FB seine Profile maschinell gesteuert, also nicht kausalitätsbasiert erstellt?
2. Wäge gegeneinander auf: a) We use [...] the things we infer from your use of Facebook. und b) "[...] but we do not tell the advertiser who any of those people are." und setze das in Beziehung zu dem bereits erarbeiteten Gegensatz von statischer und dynamischer Merkmalerfassung.

4. Auswertung persönlicher Informationen. Wie die Datensammel-Industrie hinter Facebook und Co. funktioniert. <http://www.sueddeutsche.de/digital/auswertung-persoenlicher-informationen-wie-die-datensammel-industrie-hinter-facebook-und-co-funktioniert-1.1280573>

Nicht nur die IT-Giganten profitieren von Nutzerdaten: In den USA bieten Unternehmen wie LexisNexis an, die im Netz hinterlassenen Informationen zu verknüpfen. Anwälte, Behörden und die Werbebranche nutzen die neuen Möglichkeiten - und Menschen werden aufgrund ihrer digitalen Existenz ausgegrenzt.

Ein Gastbeitrag von Lori Andrews

In der vergangenen Woche hat [Facebook Unterlagen bei der US-Börsenaufsicht eingereicht](#). Ihr Wert wird auf mindestens 75 Milliarden Dollar geschätzt. Doch alles, was [Facebook](#) zu bieten hat, sind persönliche Daten - die Daten von uns allen. Facebook verdient Geld, indem es Werbeflächen für Firmen zur Verfügung stellt, die uns möglichst zielgenau ansprechen wollen.

Die Werbekunden entscheiden sich für bestimmte Schlüsselbegriffe oder persönliche Informationen wie Beziehungsstatus, Wohnort, Freizeitaktivitäten, Lieblingsbücher oder Arbeitgeber. Facebook macht die Anzeigen dann für genau jene Nutzer sichtbar, die diesen Vorgaben entsprechen. Wer online seine Vorliebe für Kuchen kundtut, in einer bestimmten Gegend wohnt und gerade seine Freunde zu sich nach Hause eingeladen hat, der sollte sich nicht wundern, wenn er auf seiner Seite die Anzeige der Bäckerei um die Ecke vorgesetzt bekommt.

Facebook hat im vergangenen Jahr allein durch Werbung einen Umsatz von 3,2 Milliarden Dollar generiert - das sind 85 Prozent seines Gesamtumsatzes. Und doch sind Facebooks Datenvorräte und Werbeumsätze ein Klacks. [Google](#) etwa hat zehnmal so viel eingenommen: Mithilfe der Analyse von Suchanfragen und E-Mails, die über den Dienst G-Mail verschickt wurden, erreichte Google im Jahr 2011 einen Werbeumsatz von 36,5 Milliarden Dollar.

Nützlich, im schlimmsten Falle lästig

Hunderte weiterer Unternehmen greifen gierig nach Nutzerdaten, indem sie Cookies und andere technische Hilfsmittel zur Nachverfolgung auf den Computern und in den Browsern platzieren. Wenn in einer E-Mail von Angst die Rede ist und man noch dazu "Stress" auf Google gesucht hat, sollte man sich auf Anzeigen gefasst machen, die die entsprechenden Medikamente und Dienste zur Behandlung von Beklemmungen anbieten.

Solche Anzeigen können durchaus nützlich, im schlimmsten Falle lästig sein. Doch die Bits und Bytes, die Informationen über ein Leben enthalten, können auch ohne weiteres gegen jemanden verwendet werden. Die Entscheidung, ob man eine Arbeitsstelle, einen Kredit oder eine Versicherung bekommt, könnte von einem digitalen Doppelgänger abhängig gemacht werden. Bekommt man dann eine Absage, erfährt man vielleicht nie den wirklichen Grund.

Beweismittel im Sorgerechtsstreit

Es ist in den USA durchaus schon vorgekommen, dass online verfügbares Material gegen Personen verwendet wurde, die um das Sorgerecht für ihre Kinder kämpften oder in Strafprozessen angeklagt waren. Der Datenbankdienst LexisNexis bietet ein Produkt namens ["Accurint for Law Enforcement"](#) an, das Behörden mit Informationen darüber versorgt, was Bürger in den sozialen Netzwerken tun.

Das amerikanische Finanzamt durchkämmt Facebook und MySpace zum Beispiel regelmäßig auf der Suche nach Anhaltspunkten für das Einkommen und den Aufenthaltsort von Steuerhinterziehern. Von der Einwanderungsbehörde hört man, dass sie Fotos und Blogposts benutzt, um Verwandtschaftsbeziehungen nachzuvollziehen und Scheinehen aufzuspüren.

Es kommt aber auch vor, dass Arbeitgeber die Entscheidung, welchen Bewerber sie einstellen, von dessen Online-Profilen abhängig machen. Eine Studie hat ergeben, dass 70 Prozent der Personalchefs in den USA schon einmal einen Bewerber aufgrund von Informationen abgelehnt haben, die im Internet abrufbar sind. Solche Daten werden von Firmen wie Spokeo gesammelt und den Arbeitgebern (und allen anderen, die sich dafür interessieren) zur Verfügung gestellt. Spokeo schaltet sogar Werbung mit dem Spruch "Personalchefs - Hier klicken!".

Die Datensammler stellen eigene Regeln auf

Wo massenweise Daten analysiert werden, ist Stereotypisierung unvermeidbar. So könnte es sein, dass ein Kreditantrag nicht aufgrund einer momentanen finanziellen Lage oder vergangener Kredite abgelehnt wird, sondern weil die Daten einen in eine Personengruppe einordnet, deren Vorlieben und Abneigungen den eigenen ähnlich sind.

Aus dem Verhalten dieser Gruppe wird auf das individuelle Verhalten geschlossen. Wenn dann zum Beispiel statistisch nachweisbar ist, dass Gitarristen oder Leute in Scheidungsverfahren ihre Kreditkartenrechnungen mit hoher Wahrscheinlichkeit seltener begleichen, könnte die Tatsache, dass man sich kürzlich Gitarrenwerbungen angesehen oder eine E-Mail an einen Scheidungsanwalt geschickt hat, dazu führen, dass die Kreditwürdigkeit herabgestuft wird.

Das ist einem Mann aus Atlanta passiert. Der musste nach seinen Flitterwochen feststellen, dass sein Kreditrahmen von 10.800 auf 3800 Dollar herabgesetzt worden war. In einem Brief ließ die Kreditkartenfirma ihn wissen: "Andere Kunden, die ihre Karte in den Geschäften benutzt haben, in denen Sie kürzlich eingekauft haben, wiesen in der Vergangenheit American Express gegenüber eine geringe Rückzahlungsmoral auf."

Keine Transparenz über Datensammlungen

Es gibt in den USA zwar Gesetze, die es erlauben, unzutreffende Informationen in Kreditauskünften anzufechten. Es gibt jedoch keine Gesetze, die Firmen, die Daten sammeln, dazu verpflichten offenzulegen, was sie über einzelne Personen wissen. Wenn ich für einen Freund auf [Google](#) Informationen über Diabetes einhole oder den Suchbegriff "Date-Rape-Mittel" (K.-o.-Tropfen für Vergewaltigungen) eingebe, weil ich die entsprechenden Informationen für den Roman benötige, den ich gerade schreibe, gehen die Datensammler davon aus, dass diese Suchanfragen etwas über meinen eigenen Gesundheitszustand oder meine Neigungen aussagen. Und weil nicht gesetzlich festgelegt ist, welche Informationen die Datensammler anhäufen dürfen, stellen sie ihre eigenen Regeln auf.

In den Jahren 2007 und 2008 einigte sich die Werbeagentur NebuAd mit sechs Internet Providern darauf, Programme in deren Netzwerke einzubauen, mit denen die Aktivitäten der Internetnutzer überwacht werden konnten. Diese Informationen wurden auf die Server von NebuAd übertragen, wo sie analysiert und zu Werbezwecken genutzt wurden.

Über einen Zeitraum von im Schnitt sechs Monaten hinweg speicherte NebuAd jede E-Mail, jede Suchmaschinenanfrage, jeden Einkauf, den etwa 400 000 Menschen über das Internet tätigten. Andere Firmen wie Healthline Networks haben sich zwar intern Beschränkungen auferlegt. So nutzt Healthline keine Informationen aus Suchanfragen zu HIV, Impotenz oder Essstörungen. Allerdings

werden sehr wohl Informationen über manische Depressionen, überaktive Blasen oder Angstzustände genutzt - Krankheiten, die ähnlich stigmatisierend sein können.

Die Karte zeigt Streifzüge durch das Web

Der Kommunikationswissenschaftler John McKnight prägte in den siebziger Jahren den Begriff "Redlining", der die Weigerung von Banken, Versicherungen und ähnlichen Institutionen beschreibt, ihre Dienste in Problemvierteln anzubieten. Der Begriff hat seinen Ursprung in der Praxis von Bankern, auf Karten rote Linien einzuzichnen, um zu markieren, in welchen Gegenden man besser keine Investitionen tätigen sollte. Im Laufe der Zeit aber hat sich die Bedeutung des Begriffes ausgeweitet. Er bezeichnet heute alle möglichen Formen von Diskriminierung, beispielsweise die Ablehnung von Immobilienkrediten an Afroamerikaner, selbst wenn diese wohlhabend oder Angehörige der Mittelschicht sind.

Die Karte, auf der heute "Redlining" betrieben wird, ist keine geographische mehr, sondern jene fiktive Karte, die unsere Streifzüge durch das Web abbildet. So beschreibt der Begriff "Weblining" nun die Praxis, Menschen aufgrund ihrer digitalen Existenzen abzulehnen. Es könnte beispielsweise passieren, dass man keine Krankenversicherung bekommt, weil man bei Google nach Informationen über eine bestimmte Krankheit gesucht hat. Oder dass der Kreditrahmen wegen Rasse, Geschlecht, der heimischen Postleitzahl oder häufig besuchten Internetseiten niedriger ausfällt.

Die massenhafte, systematische Ansammlung von individuellen Daten hat gesellschaftliche Folgen. Wenn man junge Leute in den ärmeren Vierteln mit Werbung für Berufsschulen bombardiert, ist die Wahrscheinlichkeit dann nicht größer, dass sie ihr Studium abbrechen? Und liegt es nicht nahe, dass Frauen, denen man nur Artikel über Prominente zu lesen gibt, keinen Sachverstand in Finanzfragen entwickeln können? Die Werbeindustrie zieht eifrig neue rote Linien - und trägt so dazu bei, dass Menschen auf eben die Rollen beschränkt werden, die den gesellschaftlichen Erwartungen entsprechen.

Es muss Gesetze geben

Die amerikanische Gesellschaft ist mit dieser Entwicklung keineswegs einverstanden. 93 Prozent von 2000 befragten Amerikanern waren der Meinung, dass Internetfirmen um Erlaubnis fragen sollten, wenn sie persönliche Informationen nutzen. 72 Prozent sprachen sich dafür aus, dass man das Recht haben sollte, aus der Speicherung der eigenen Onlineaktivitäten auszusteigen. Bei einer anderen Befragung waren 69 Prozent der 1000 Befragten dafür, dass es in den USA ein Gesetz geben sollte, das jedem Bürger das Recht auf Einsicht in das gibt, was eine bestimmte Internetseite über ihn weiß.

Die schiere Menge der Informationen, die [Facebook](#) von uns allen gesammelt hat und für zielgruppenorientiertes Marketing verwendet, ist atemberaubend. In Europa gibt es Gesetze, die es den Menschen ermöglichen, in Erfahrung zu bringen, welche Informationen einzelne Firmen über sie gespeichert haben. In den USA ist das nicht der Fall.

Doch es muss Gesetze geben, welche die Online-Profilierung unterbinden, ähnlich wie das Gesetz, das Werbeanrufe einschränkt. Mit dem Unterschied, dass es jetzt nicht nur darum geht, ob man beim Abendessen gestört wird. Nein, es geht hier um die Frage, ob Träume von Bits und Bytes zerstört werden, über die man selbst keine Kontrolle hat und mit denen Internetfirmen im Moment nach Gutdünken verfahren können, ohne jemals dafür zur Rechenschaft gezogen zu werden.

Die Autorin ist Direktorin des Institute for Science, Law and Technology am Chicago-Kent College of Law.

Arbeitsauftrag:

- I. Lies den Text, erfasse die Kernaussagen und vollziehe nach, wie der Übergang von Red- zu Weblining von statten geht. Beziehe dazu deine Hintergrundkenntnisse zum Thema Tracking mit ein.
- II. Es werden 3 Gruppen a 8 Leuten gebildet, die sich wie folgt aufteilen: 3 Anbieter (z.B. Facebook, Google, NebuAD); 3 Kunden (z.B. Versicherung, Bank, Immobilienfirmen); Produkt (Facebook -/ Google User) = 3 Anbieter, 3 Kunden, 2 User (1 FB, 1 Google-User) = 8 in einer Gruppe
- III. Die User posten ihre Interessen auf FB, FB und Google werten aus und führen Verkaufsgespräche mit ihren Kunden (Versicherungen etc.). Bereite diesen Vorgang so auf, dass ihr ihn szenisch vor dem Kurs darstellen könnt.

Rollenkarten

Facebook: Du bist Facebook-CEO und bekommst Druck von Mark Zuckerberg, weil der FB-Börsengang alles andere als erfolgreich war. Das Geschäft mit Werbekunden verläuft schleppend, da die User immer häufiger mit Smartphones im Netz surfen, auf denen wenig Platz für Werbung zur Verfügung steht. Du musst neue Einnahmequellen erschließen (außerhalb von personalisierter Werbung), die auf der Auswertung von Userdaten basiert. Überlege ausgehend vom Lori Andrews-Artikel, welche Kunden sich für welche Fragestellungen und Segmentierungen ihrer Kunden interessieren könnten und biete deinen Kunden an, exakt auf ihre Fragestellungen zugeschnittene Profile aus den Userdaten zu erstellen.

Kunde: Du vertrittst eine Bank, eine Versicherung, eine Immobilienfirma (such dir was aus), kurz: ein Unternehmen, das auf Wissen über seine Kunden angewiesen ist. Eine Bank will grundsätzlich Kredite vergeben, da sie dafür Zinsen bekommt, natürlich will sie die Kreditsumme auch zurück. Eine (Kranken)-Versicherung will möglichst gesunde Kunden ohne Hobby Risikosportart etc., weil sie möglichst wenig Verletzungen, Krankenhausaufenthalte, chronische Krankheiten etc. bezahlen will. Eine Immobilienfirma braucht Mieter, die sich die Miete leisten können und pünktlich überweisen etc. Du hast von neuen Auswertungsmöglichkeiten wie LexisNexis gehört und trittst an facebook heran, um deren Möglichkeiten auszuloten, dir Wissen über potentielle Kunden zu verschaffen. Dieses Wissen beabsichtigst du zur Selektion zu benutzen (den will ich als Kunden, den nicht)

Facebook-User: Du bist äußerst „Neue Medien“-affin und hältst Facebook für das Tool des www, um mit deinen Freunde und Mitmenschen in Kontakt und über sie auf dem Laufenden zu bleiben. Mittlerweile nutzt du es anstelle eines eMail-Clients und als Portal für alles und jedes – Blogs, Foren, Mails sind für dich Schnee von gestern, der durch Facebook komplett ersetzt werden kann. Was immer du gerade tust, liest, hörst – dein Freundeskreis erfährt es sofort. Meldungen über problematische Handhabung von Sicherheit und Privatsphäre hältst du grundsätzlich für Probleme von Usern, die ihre Profileinstellungen nicht überblicken.

Im Moment bist du im Urlaub und gehst irgendeiner Sportart nach – Mountainbiken auf dem Tibi Dabo in Barcelona, Snowboarden in Les Arc, Surfen an der Atlantikküste – whatever floats your boat. Deine Timeline verlangt nach neuen Statusmeldungen, Kommentaren und Fotos – schieß los.

Ablauf: Die Kunden treten an FB heran, um sich das neue Geschäftsmodell erklären zu lassen (Austausch FB – Kunden)

Die User chatten, posten Statusupdates etc., die sie auf einem Share-Laufwerk speic hern. Im Laufe des Gesprächs öffnen die FB-CEOs diese Datei „zur Anschauung“ für ihre Kunden.

5. Assoziationsregelentdeckung mit dem Apriori-Algorithmus

SNS können aus den Nutzerprofilen extrahieren:

- Interessen
- Interessenprofile. Diese werden verwendet zur
- Assoziationsregelentdeckung (Apriori-Algorithmus)
- Eine Assoziationsregel (Beispiel L. Andrews): Antecedens: In Scheidung begriffen, Einkäufe in Gitarrengeschäften → geringere Kreditrückzahlungsmoral (Konsequens)

Beispiel Warenkorbanalyse aus: Daniel Delic, [Mining association rules with rough sets and large itemsets - a comparative study](#)

Mining Association Rules with Rough Sets and Large Itemsets - A Comparative Study

Transaction ID	Attributes
1	spaghetti, tomato sauce
2	spaghetti, bread
3	spaghetti, tomato sauce, bread
4	bread, butter
5	bread, tomato sauce

Step 3 **Large 2-Itemsets**

- {Spaghetti, Tomato Sauce}
- {Spaghetti, Bread}
- {Tomato Sauce, Bread}

Candidate 3-Itemsets

- {Spaghetti, Tomato Sauce, Bread} → support = 1 $\hat{=}$ 20%

Large 3-Itemsets

- { }

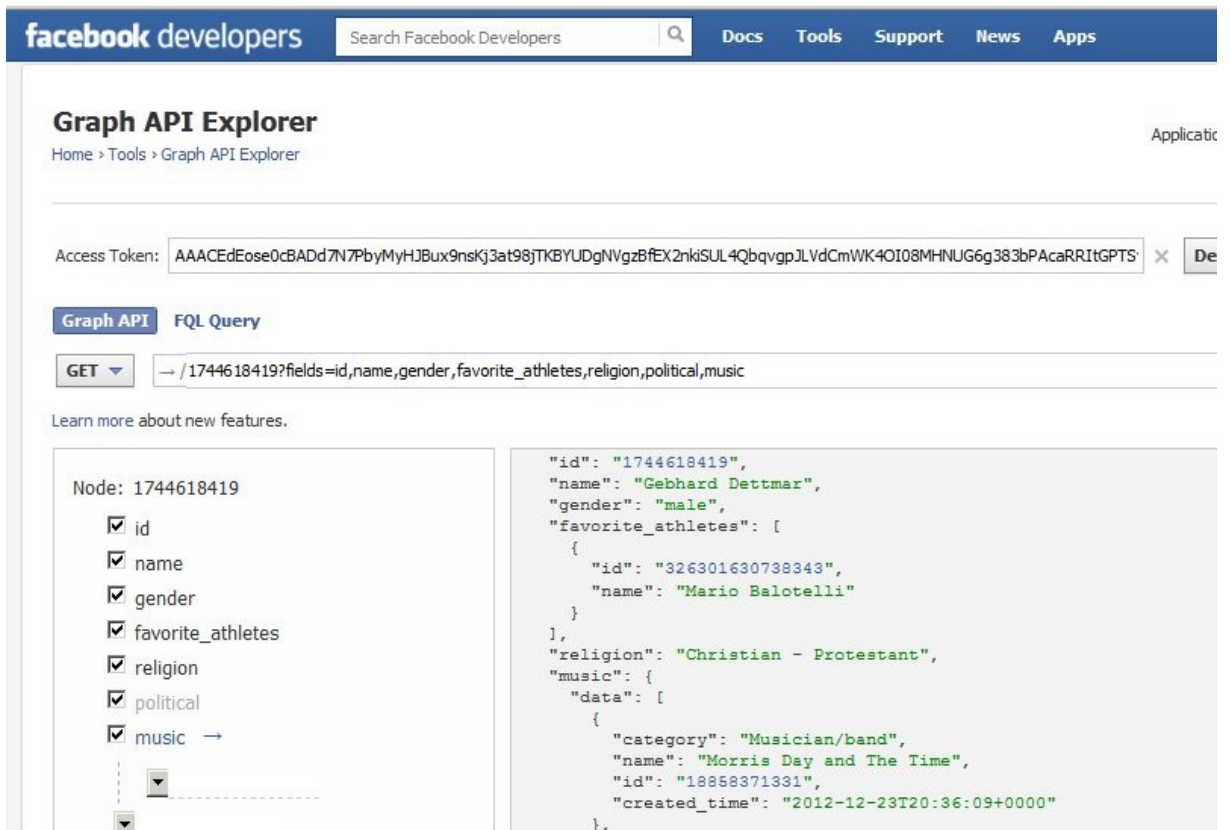
2 LARGE ITEMSET METHOD p. 8

Apriori ist ein Sortier-Algorithmus. Er sucht nach Regeln wie: wenn vorher Spaghetti und Tomatensoße, dann folgt Brot (e.g.). Dazu benutzt er einen Schwellwert (Threshold): der Support einer Assoziationsregel misst das Auftauchen eines "Itemsets" an allen Transaktionen, also Spaghetti / alle Transaktionen, Brot / alle usw., die Konfidenz die Wahrscheinlichkeit, dass aus dem Antecedens A, B auch das Konsequens C folgt:

Support A, B, C / Support A, B, allgemein formuliert: Support der kompletten Regel / Support des Antecedens

Arbeitsauftrag: Errechne aus obigem Warenkorb die Konfidenz der Regel: Spaghetti, Tomatensoße → Brot.

6. Facebooks Graph API



facebook developers Search Facebook Developers Docs Tools Support News Apps

Graph API Explorer

Home > Tools > Graph API Explorer

Access Token: AAACEdEose0cBADd7N7PbyMyHJBux9nskj3at98jTKBYUDgNVgzBfEX2hkiSUL4QbqvqjLlVdCmWK4OI08MHNUG6g383bPAcaRRItGPTS

Graph API FQL Query

GET → /1744618419?fields=id,name,gender,favorite_athletes,religion,political,music

Learn more about new features.

Node: 1744618419

- id
- name
- gender
- favorite_athletes
- religion
- political
- music →

```
{
  "id": "1744618419",
  "name": "Gebhard Dettmar",
  "gender": "male",
  "favorite_athletes": [
    {
      "id": "326301630738343",
      "name": "Mario Balotelli"
    }
  ],
  "religion": "Christian - Protestant",
  "music": {
    "data": [
      {
        "category": "Musician/band",
        "name": "Morris Day and The Time",
        "id": "18858371331",
        "created_time": "2012-12-23T20:36:09+0000"
      }
    ]
  }
}
```

Abb. 1: Facebook's Graph API

Arbeitsauftrag: Erstelle nach dem Muster der Apriori-Folie eine Tabelle mit UserIDs, Attributen und deren Werten aus dem Facebookgraph ("name", "music", „athletes“ "relationship status", prinzipiell frei wählbar, Werte könnt ihr den ersten 5 Treffern entnehmen. Erstelle eine Assoziationsregel (mit Support und Konfidenz) nach dem Muster: favorite athelete X + education Y → relationship status +/-

7. Volkszählungsurteil und Recht auf Informationelle Selbstbestimmung

Von grundlegender Bedeutung für den Datenschutz ist das sog. Volkszählungsurteil vom 15.12.1983. In diesem hat das Bundesverfassungsgericht anerkannt, dass es ein Grundrecht auf informationelle Selbstbestimmung gibt. Der Verfassungsbeschwerde lag zugrunde, dass das Volkszählungsgesetz 1983 (VZG) eine Erhebung statistischer Daten der Bevölkerung vorsah. Darüber hinaus sah das VZG einen Abgleich mit dem Melderegister vor. Auch eine Übermittlung von personenbezogenen Einzelangaben an die fachlich zuständigen obersten Bundesbehörden und Landesbehörden sowie an die von ihnen bestimmten Stellen sollte gestattet werden, soweit diese personenbezogenen Daten von den Empfängern zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben benötigt werden. Zusätzlich sollte das VZG ermöglichen, die mit Hilfe der Gemeinden erhobenen personenbezogenen Daten ohne Namen auch dem kommunalen Bereich für bestimmte Verwaltungszwecke zur Verfügung zu stellen.

Da durch die Volkszählung jeder in gleichem Maße den Informationsanforderungen des Staates ausgesetzt war, schlug die bislang eher individuelle Betroffenheit um in eine kollektive. Die zunehmende Automatisierung ließ die Furcht vor der Verknüpfung von Daten und der unkontrollierten Persönlichkeitserfassung wachsen und führte zu dem Misstrauen, dass der Staat in das Leben der Bürger eingreifen würde.

Vor diesem gesellschaftspolitischen Hintergrund hat sich das Bundesverfassungsgericht ausführlich mit der Frage auseinandergesetzt, welche Anforderungen die Verfassung an die Verarbeitung personenbezogener Daten stellt und geht in seinen Urteilsgründen über den konkreten Einzelfall hinaus.¹

Wikipedia zum Volkszählungsurteil und Recht auf Informationelle Selbstbestimmung

Das Recht auf Informationelle Selbstbestimmung bezeichnet im [deutschen Recht](#) das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner [personenbezogenen Daten](#) zu bestimmen. Es handelt sich dabei nach der Rechtsprechung des [Bundesverfassungsgerichts](#) um ein [Datenschutz](#)-Grundrecht, das im [Grundgesetz](#) nicht ausdrücklich erwähnt wird. Der Vorschlag, ein Datenschutz-Grundrecht in das Grundgesetz einzufügen, fand bisher nicht die [erforderliche Mehrheit](#).

[...] Das informationelle Selbstbestimmungsrecht ist eine Ausprägung des [allgemeinen Persönlichkeitsrechts](#) und wurde vom Bundesverfassungsgericht im so genannten [Volkszählungsurteil](#) 1983 als [Grundrecht](#) anerkannt. Ausgangspunkt für das Bundesverfassungsgericht ist das [Allgemeine Persönlichkeitsrecht](#), also Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG. Die Kritik lautete konkret:

Die freie Selbstbestimmung wird durch die Fortschritte der modernen Datenverarbeitung in zunehmendem Maße gefährdet: *"Sie [sc. die Daten] können darüber hinaus - vor allem beim Aufbau integrierter Informations-systeme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekanntem Weise die Möglichkeiten einer Einsichtnahme und Einflußnahme erweitert, welche auf*

¹ aus: <https://www.zendas.de/recht/allgemein/volkszaehlunsurteil.html>

das Verhalten des Einzelnen [...] einzuwirken vermögen."² Wer nicht wissen oder beeinflussen könne, welche Informationen bezüglich seines Verhaltens gespeichert und vorrätig gehalten werden, werde aus Vorsicht sein Verhalten anpassen ([Panoptismus](#)). Dies beeinträchtigt nicht nur die individuelle Handlungsfreiheit sondern auch das Gemeinwohl, da ein freiheitlich demokratisches Gemeinwesen der selbstbestimmten Mitwirkung seiner Bürger bedürfe. *"Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."*

Das Recht auf informationelle Selbstbestimmung leitet sich nach Ansicht des EU-Parlamentes auch aus Artikel 8 Absatz 1 der [Europäischen Menschenrechtskonvention](#) ab: „Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.“

Aufbauend auf dieser Begründung hatte das EU-Parlament gegen die EU-Kommission Klage erhoben, weil die verbindliche Speicherung der Verkehrsdaten der EU-Bürger gegen diese Regelung verstoße. (aus: http://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung + <http://de.wikipedia.org/wiki/Volksz%C3%A4hlungsurteil>)

Arbeitsauftrag:

1. Welche Art von Misstrauen erfasst die Bürger gegen den Staat und wogegen klagen die Klageführer vor dem Bundesverfassungsgericht?
2. Wende die Argumentation des BVerfG und des EU-Parlamentes auf die Datenspeicherung bei Facebook und Google und deren Auswertung auf preferencetool.com an. Fülle den Satz: "Sie [sc. die Daten] können darüber hinaus [...] mit anderen Datensammlungen zu einem [...] weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann." mit Beispielen aus dem bisherigen Unterrichtsverlauf
3. Inwieweit ist der Panoptismus (Konformismus, Mainstream, GD) ein probates Mittel, um "Profiling" (Kategorisierung) auf fb zu entgehen?

² aus: <http://openjur.de/u/268440.print>

8. Das NPD-Verbot aus verfassungsrechtlicher Sicht

Kommentar vom Präsidenten des OLG a. D., Dr. Rudolf Wassermann, Aktivierung der wehrhaften Demokratie – Zum Antrag auf NPD-Verbot, abgedr. In: NJW (=Neue Juristische Wochenschrift) 2000, Heft 51, S. 3760-62:

(...) Die Demokratie des Grundgesetzes ist pluralistisch. Ihre ideologische Basis ist nicht die Fiktion der Homogenität des Volkes, der Klasse oder der Rasse. Sie beruht vielmehr auf der Einsicht in die Vielfältigkeit in der zum Staat verfassten Gesellschaft, in die Differenziertheit des Volkes und damit in die Unterschiedlichkeit und Gegensätzlichkeit der Meinungen und Interessen.

Was das Gemeinwohl ist, ist nicht a priori festgelegt. Es soll sich vielmehr im "Freihandel der Ideen" (*Oliver Wendell Holmes*) herausbilden, im offenen Prozess der Meinungs- und Willensbildung. Konflikte werden nicht nur als unvermeidlich anerkannt, sie werden bejaht als Instrumente der Gemeinwohlfindung wie des Wandels, der Politik und Gesellschaft vor Verharrung und Erstarrung bewahrt. Geistige und politische Auseinandersetzungen auf den Gebieten des staatlichen und gesellschaftlichen Lebens kennzeichnen die liberale politische Gesellschaft als ein in Freiheit pulsierendes Gemeinwesen, in dem Toleranz für abweichende oder gegensätzliche Meinungen herrscht.

Ein solches System, in dem konfligierende [widerstreitende, GD] Gruppen um die Macht im Staate ringen, funktioniert, solange sich diese wechselseitig zur Toleranz bekennen und darin übereinstimmen, dass die Spielregeln des Systems unangetastet bleiben müssen. Fehlt es daran, weil Gruppen zur Macht gelangen, die das System zu Gunsten eines anderen beseitigen wollen, so bricht es zusammen.

Arbeitsauftrag:

1. Beschreibe die Bedeutung des Meinungspluralismus für die Demokratie.
2. Stelle die Auswirkungen des Panoptismus auf die Privatsphäre und daraus resultierend die Bedeutung desselben für den Meinungspluralismus dar.
3. Erörtere die Rolle der SNS in der Demokratie unter Heranziehung deines Hintergrundwissens zu Datenauswertung von FB.

9. Die Wertordnungsrechtsprechung des Bundesverfassungsgerichts und die Frage ihrer theoretischen Basis³

1. Die Rechtsprechung des Bundesverfassungsgerichts

Locus classicus der Wertordnungsrechtsprechung des Bundesverfassungsgerichts ist das berühmte, in der Tat „epochemachende“ Lüth-Urteil aus dem Jahre 1958. Obwohl das Gericht bereits in einigen früheren Urteilen, namentlich den beiden Parteienverbotsentscheidungen, das Grundgesetz unter deutlicher Betonung seiner antirelativistischen Stoßrichtung als eine „wertgebundene Ordnung“ charakterisiert hatte, wird der eigentliche Grundstein hier gelegt.

Es ging in jenem Fall darum, daß der Hamburger Senatsdirektor und Leiter der Staatlichen Pressestelle der Freien und Hansestadt Hamburg zum Boykott eines (künstlerisch wohl nicht sonderlich belangvollen) Films von Veit Harlan mit dem Titel „Unsterbliche Geliebte“ aufgerufen hatte. Veit Harlan war im Dritten Reich Regisseur des berühmten Propagandafilms „Jud Süß“ gewesen und hatte sich dadurch nach Auffassung Lüths hinlänglich diskreditiert. Rechtlicher Kernpunkt des Streits war die Frage, ob in Lüths Appell ein sittenwidriger Boykottaufruf zu erblicken war. Das Landgericht Hamburg hatte das bejaht und Lüth gem. § 826 BGB zur Unterlassung verurteilt.

Das Bundesverfassungsgericht gab hingegen dem Recht der Meinungsäußerungsfreiheit den Vorrang. Die weit über den konkreten Anlaß hinausreichende Begründung des Urteils läßt deutlich erkennen, daß sich die Richter der weichenstellenden Grundsätzlichkeit der Entscheidung bewußt waren. Deren zentrale Passage lautet: "Ohne Zweifel sind die Grundrechte in erster Linie dazu bestimmt, die Freiheitssphäre des einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern; sie sind Abwehrrechte des Bürgers gegen den Staat (...). Ebenso richtig ist, daß das Grundgesetz, das keine wertneutrale Ordnung sein will, in seinem Grundrechtsabschnitt auch eine objektive Wertordnung aufgerichtet hat und daß gerade hierin eine prinzipielle Verstärkung der Geltungskraft der Grundrechte zum Ausdruck kommt. Dieses Wertsystem, das seinen Mittelpunkt in der innerhalb der sozialen Gemeinschaft sich frei entfaltenden menschlichen Persönlichkeit und ihrer Würde findet, muß als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gelten; Gesetzgebung, Verwaltung und Rechtsprechung empfangen von ihm Richtlinien und Impulse. So beeinflußt es selbstverständlich auch das bürgerliche Recht; keine bürgerlich-rechtliche Vorschrift darf in Widerspruch zu ihm stehen, jede muß in seinem Geiste ausgelegt werden."

Damit war der entscheidende Schritt getan. Die einschlägige Judikatur der folgenden Jahre baute den Ausgangspunkt konsequent weiter aus, differenzierte die Anwendungsfälle und bezog sich dabei regelmäßig auf die Lüth-Entscheidung als Grundlage.

[Anm. GD]: Im folgenden wird dieser objektiv-rechtliche Grundrechtsgehalt der Grundrechte näher erläutert: Wesentliche Funktion der Grundrechte sei die "Teilhabe" am politischen Gemeinwesen: "Für die Freiheit der Meinungsäußerung hat das Bundesverfassungsgericht diesen aktiv-gestaltenden Aspekt der Grundrechtswahrnehmung mit den berühmten Worten charakterisiert, sie sei für die Demokratie "schlechthin konstituierend".⁴ *Ihm komme daher eine Doppelfunktion zu: Im status negativus als liberalem Abwehrrecht*

³ in: Horst Dreier, [Dimensionen der Grundrechte. Von der Wertordnungsjudikatur zu den objektiv-rechtlichen Grundrechtsgehalten](#), Hannover 1993.

⁴ BVerfGE 7, 198: "Das Grundrecht auf freie Meinungsäußerung ist als unmittelbarster Ausdruck der menschlichen Persönlichkeit in der Gesellschaft eines der vornehmsten Menschenrechte überhaupt (un des droits les plus précieux de l'homme nach Artikel 11 der Erklärung der Menschen- und Bürgerrechte von 1789). Für eine freiheitlich-demokratische Staatsordnung ist es schlechthin konstituierend, denn es ermöglicht erst die ständige geistige Auseinandersetzung, den Kampf der Meinungen, der ihr Lebenselement ist (BVerfGE 5, 85 [205]). Es ist in gewissem Sinn die Grundlage jeder Freiheit überhaupt, "the matrix, the indispensable condition of nearly every other form of freedom" (Cardozo)", zit.n. <http://www.servat.unibe.ch/dfr/bv007198.html>

gegen den Staat und als demokratisches Mitwirkungsrecht: "(...) ob seine Wahrnehmung der privaten oder der öffentlichen Sache dienen soll, liegt in der Hand des Grundrechtssubjekts. (...) Die Doppelung besteht darin, dass das Gesamtziel des verfassungsstaatlichen Rechts- und Institutionenensembles, die individuelle "Freiheit der Person, sowohl durch die subjektiv-defensive, rechtsstaatliche als auch durch die subjektiv-aktive, demokratische Stoßrichtung der Grundrechte gewährleistet und abgesichert wird" (Dreier, S. 40) [...] Von besonderer Brisanz ist dies naturgemäß für den Bereich des Privatrechts, wo Differenzierung, Ungleichheit und Bindung oft gerade als Folge freiwillig eingegangener Verpflichtungen eintritt. Grundrechte wirken hier nicht direkt und unmittelbar auf die zivilen Rechtsverhältnisse ein, was im Endergebnis die Privatautonomie zerstören und die grundrechtlichen Freiheiten zu einer umfassenden Pflichtordnung denaturieren lassen würde. (S. 43) *Aber:* "In Umkehr der Schutzrichtung des subjektiv-defensiven Abwehrenspruchs sinnt der Schutzpflichtgedanke dem Staat an, den einzelnen Bürger vor Ein- und Übergriffen in dessen Rechtssphäre durch private Dritte zu schützen und (...) eine Rechtsgutsverletzung zu vermeiden. (S. 47) In ihrer Abwehrdimension grenzen Grundrechte den Staat aus, errichten eine Schranke, schirmen einen Raum ungestörter individueller Entfaltung vom hoheitlichen Zugriff ab; das Bundesverfassungsgericht selbst hat in konsequenter Zuspitzung (...) vom Recht des Bürgers gesprochen, vom Staat "in Ruhe" gelassen zu werden.⁵ Als Normen mit objektiv-rechtlichem Gehalt, die auf Verwirklichung und Umsetzung drängen, legitimieren Grundrechte nunmehr staatliches Handeln, ja verpflichten in Fällen hinlänglicher Eindeutigkeit zur Wahrnehmung staatlicher Aufgaben, in Extremfällen sogar zur Statuierung von Strafrechtvorschriften. (...) Damit ist die an ein Wunder grenzende Verwandlung der Grundrechte perfekt: Aus Normen, die in ihrer (...) Urfunktion den Staat ausgrenzen und fernhalten sollen, wird nun der Ausgangspunkt für die Statuierung von Staatsaufgaben. (S. 49).

Arbeitsauftrag:

1. Erläutere in eigenen Worten den Streitfall Harlan - Lüth bis zum Urteil des Hamburger Landgerichts – was genau sagt Lüth, was Harlan? (Boykottaufruf erklären – Harlan gewinnt vorm Landgericht)
2. Welches Recht wird im Lüth-Urteil konkret gestärkt und aus welchem Grundrecht wird es abgeleitet?
3. Welche allgemeingültigen Konsequenzen formuliert das BVerfG in der Urteilsbegründung?
4. Worin besteht die objektiv-rechtliche Funktion der Grundrechte konkret und was ist daran neu?
5. Führe unten beschriebenes Rollenspiel zu einer Verfassungsbeschwerde gegen Google/Facebook (=Datensammelindustrie, cf. Lorie Andrews), in der du die Argumentation aus dem Lüth-Urteil aufgreifst.

10. Rollenspiel Lüth-Urteil

Der Fall: Ein User von Gmail hat den Anbieter Google darauf verklagt, ihm diesen Dienst ohne das in den Geschäftsbedingungen erwähnte Textfiltern nach Schlüsselbegriffen anzubieten, des weiteren hat ein Facebook-User gegen die Profilerstellung geklagt. Das BVerfG soll dazu Stellung nehmen. Es gibt 3 Gruppen: Anhänger Böckenförde, Anhänger BVerfG und die "Je-nachdem"-Denkenden. Erstere versuchen letztere zu überzeugen (wovon?):

Gruppe Böckenförde: Du folgst dem Kritiker der neu definierten objektiv-rechtlichen Grundnorm, Ernst-Wolfgang Böckenförde. Der sagt: als objektiv rechtliche Grundnormen sind die Grundrechte überzogen. Aufgabe der (frei gewählten) Legislative ist die Rechtssetzung, wenn das BVerfG in jede dieser Setzungen

⁵ BVerfGE 27, 1/6: "Ein solches Eindringen in den Persönlichkeitsbereich durch eine umfassende Einsichtnahme in die persönlichen Verhältnisse seiner Bürger ist dem Staat auch deshalb versagt, weil dem Einzelnen um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein "Innenraum" verbleiben muß, in dem er "sich selbst besitzt" und "in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt"". Zit. n.

eingreifen kann, gewinnt es einen Einfluss auf die Legislative, der ihm nicht zulommt und nicht im Sinne der Gewaltenteilung ist. So mutiert der Staat zu einem Jurisdiktionsstaat, das BVerfG zu einem "Verfassungs-Areopag". Dem Bürger muss es möglich sein privatrechtliche Verträge nach eigenem Gusto einzugehen (vgl. "*was im Endergebnis die Privatautonomie zerstören und die grundrechtlichen Freiheiten zu einer umfassenden Pflichtordnung denaturieren lassen würde*" im Text). Was der Bürger mit Facebook, Google & Co. privatrechtlich in den TOLs vereinbart, geht den Staat mithin nichts an, jegliche Eingriffe staatlicherseits liefern auf eine Entmündigung des Gesetzgebers hinaus – das Privatrecht steht unter Oberaufsicht des Staats, "der Gesetzgeber hat die Vorhand, das Verfassungsgericht aber den Vorrang" – und ebenso des Bürgers, dem autonomes Handeln im Geschäftsverkehr nicht mehr zugetraut wird

Gruppe BVerfG: Du bist der Meinung, dass die Grundrechte konstituierenden Charakter für die Demokratie besitzen und deshalb als Grundnorm über dem positiven Recht stehen, aus der dieses abgeleitet wird. Freie Persönlichkeitsentfaltung und Meinungsfreiheit sind dabei von so entscheidender Bedeutung, dass privatrechtliche Vereinbarungen, die auf eine Aushöhlung dieser Grundrechte hinauslaufen, der freiheitlich-demokratischen Grundordnung zuwider laufen und daher als verfassungsfeindlich einzustufen sind

Weder-noch-Gruppe: Du musst dich im Vortrag entscheiden, wer dich mehr überzeugt. Du hast 2 Vorbehalte: Beim BVerfG besteht die Gefahr, dass die Judikative Staat und Gesellschaft die Werte vorschreibt, bei Böckenförde, dass Fundamentalkategorien der Demokratie im Privatrecht beliebig ignoriert werden können. Zudem ist nach der Stellung der Privatsphäre in der Wertehierarchie der heutigen Welt zu fragen, wenn Millionen Social Network-User ihre eigene fortwährend ignorieren.

11. Suche nach gefährlichen Wörtern

Amerikanische Behörden durchsuchen das Internet nach 377 verdächtigen Begriffen. Natürlich sind darunter Wörter wie "Terror" und "Angriff", aber warum suchen sie nach "Schwein" und "Schnee"? (SZ, 13.07.2013, Bernd Graff)

Als das amerikanische "Department of Homeland Security" (DHS) im Februar 2012 juristisch gezwungen worden war, seine interne Anleitung zur [Überwachung](#) von Sozialen Netzen mit den entsprechenden Richtlinien für "Reportings" durch seine Analysten zu veröffentlichen, erregte nicht die Tatsache Aufsehen, dass Soziale Medien von der Behörde gescannt werden. Dies war seit der Winter-Olympiade 2010 bekannt, die zwar im kanadischen Vancouver stattfand, aber wegen der Nähe zur amerikanischen Grenze augenscheinlich verstärkte Wachsamkeit von US-Behörden wie FBI, Customs Border Protection (CBP), Coast Guard und DHS erforderte.

Das DHS, so die Begründung damals, wolle während der Spiele über mögliche "Naturkatastrophen, Akte des [Terrorismus](#) und andere menschengemachte Desaster" informiert sein. Dazu observiere man die Sozialen Netze, aber nur, um sich *nach* einem Vorfall ein genaueres Bild der Lage machen zu können. Die Überwachung sei darum eine Maßnahme der Schadeneinschätzung und daher so etwas wie "der Kanarienvogel in der Kohlemine", so ein DHS-Sprecher damals gegenüber ABC News. Man verstehe die Sozialen Netze lediglich als eine Quelle für Echtzeit-Information im Ereignisfall.

Dieses DHS-Programm wurde nach dem Ende der Vancouver-Spiele nicht ausgesetzt, sondern um- und ausgebaut. Denn, wie die *New York Times* im Januar 2012 berichtete, hatte das DHS schon seit 2009 ein Unternehmen damit beschäftigt, die Sozialen Netze gezielt danach abzusuchen, wie Regierungsentscheidungen darin aufgenommen und diskutiert wurden - und dazu dann auch entsprechende Berichte zu verfassen.

Gezielte Suche nach Reaktionen aus der Bevölkerung

Man reagierte im DHS also nicht mehr lediglich auf Vorkommnisse im Sozialen Web, sondern man suchte gezielt nach Reaktionen aus der Bevölkerung. Als dann einen Monat später, im Februar 2012, der "Analyst's Desktop Binder", das interne Regularium des DHS aus dem Jahr 2011 veröffentlicht war, die auf juristisches Betreiben der unabhängigen Datenschutzorganisation "Electronic Privacy Information Center" (Epic) zugänglich gemacht werden musste, bestätigte sich nicht nur die Tatsache, dass die DHS Vorgänge im Netz im Anschluss an Regierungsentscheidungen protokolliert. Man sah nun auch, dass darin ein ganzer Katalog von "Items of Interest (IOI)" aufgestellt worden war.

Damit waren Bereiche definiert, die klassifiziert sind als von besonderer nationaler Bedeutung, und die als wesentlich für den Erhalt der Sicherheit, für die Aufrechterhaltung von Infrastrukturen und der Gesundheit der Bevölkerung erachtet werden. Darum ist in dem DHS-Manual eine Vielzahl von Themen aufgeführt, deren Erwähnung in den Sozialen Netzen als relevant für das Aufspüren und die Bekämpfung von Terrorismus und Naturkatastrophen eingestuft wird. Gemeint sind etwa Unfälle bei der chemischen Industrie, Flugzeugabstürze, Erdbeben, Amokläufe und - an erster Stelle - "Akte des Terrorismus (auch auf ausländischem Terrain)".

Um den Mitarbeitern des DHS nun Mittel an die Hand zu geben, Hinweise auf diese identifizierten, gravierenden Vorkommnisse und Bedrohungen in den Sozialen Medien zu finden, ist dem Papier eine Liste mit 377 Schlüsselbegriffen mitgegeben, bei deren Verwendung die Agenten tätig werden und berichten sollen. Es wird darauf hingewiesen, derartige Informationen nur in Sonderfällen auch personenbezogen zu erheben. Man ordnet daher an, "Personally Identifiable Information" (PII) aus den Reportings zu tilgen, fügt aber mit Nachtrag vom Januar 2011 eine Liste mit Ausnahmen an. Diese enthält den Hinweis, dass einschlägig bekannte Terroristen, Drogenhändler, Regierungssprecher und Journalisten namentlich in den DHS-Reportings geführt werden dürfen. Alle Schlüsselbegriffe sind eingestuft als von besonderer Bedeutung. Ihr Auftauchen in den Sozialen Medien verlangt nach Speicherung, weiterer Beobachtung und Reportings.

Eine Liste paranoider Angst

Diese Liste lässt sich auf den ersten Blick nur als Ausdruck paranoider Angst verstehen. Denn die mutmaßliche Sprache und Schlüsselreize des Terrors und der Gefährdung beinhaltet vor allem Allerweltsvokabeln. Erwartbar ist vielleicht noch, dass DHS-Agenten bei "Cyberattacke", "Hacker", "Selbstmordattentäter", "Terror", "Bombe", "Taliban", "Nuklear" und "Chemische Waffe" hellhörig werden sollen.

Dass aber Begriffe wie "U-Bahn", "krank", "elektrisch", "Schwein", "Schnee", "Blitz", "Heilung", "Grenze", "Welle", "Wolke", "Symptome", "Grippe", "Antwort", "Telekommunikation", "Rotes Kreuz", die Nennung Mexikos, der Stadt Tuscon in Arizona und jede Erwähnung des DHS schon als Anzeichen von (menschengemachter) Katastrophe und/oder [Terrorismus](#) hindeuten soll, vermag nicht einzuleuchten.

Normale Sprachverwendung

Das, was hier als Ausdruck von Gefährdung geführt wird, ist normale Sprachverwendung, der nur dann Verdächtigkeit zuzuschreiben wäre, wenn man schlichtweg alles für verdächtig hielte. Dann aber wäre nahezu jeder sprachliche Ausdruck Indiz für Terror, und jedes Soziale Netz müsste wie ein Trainingscamp der Taliban betrachtet werden.

Denn auch wenn Terroristen den Begriff "[Grippe](#)" ab und an gebrauchen könnten, sagt die Verwendung von "Grippe" zunächst einmal nichts über Terrorismus aus. Wenn aber jede "Grippe"-Nennung von Bedeutung für das DHS ist und nach seiner internen Logik eine Observierung nötig macht, wie will das Department dann die Abermillionen Postings auch nur sichten, in denen eines seiner verdächtigen Wörter verwandt wird?

Dieser Begriffsfuror des DHS erinnert daran an eine Episode von Jorge Luis Borges. In der Kurzgeschichte "Von der Strenge der Wissenschaft" beschreibt er das Reich mit der einzig vollkommenen Karte. Sie hatte nämlich "genau die Größe des Reiches und deckte sich mit ihm in jedem Punkt." Eine Karte also im Maßstab 1:1. So mutet die Wörterliste aus dem Giftschränk der DHS an, welche die Verwendung von Sprache generell unter Verdacht zu stellen scheint und entsprechend observieren will. Wie könnte das möglich sein?

Instrumentarium zur Erhebung und Auslese von Big Data

Die Liste des DHS deutet daraufhin, dass nicht ein einzelnes Instrument zur Aufzeichnung von Verdachtsmomenten im Kampf gegen Terror und Katastrophen eingesetzt wird, sondern ein gestaffeltes, ineinander greifendes Instrumentarium zur Erhebung und Auslese von Big Data Verwendung finden muss.

Erst die Profilierung der Daten unter Einsatz smarterer Algorithmen macht es möglich, aus vielen Datensätzen unterschiedlicher Provenienz Muster zu erkennen. So scheint die Veröffentlichung der Schlüsselbegriffe des DHS nun zu belegen, dass US-Sicherheitsbehörden unterschiedliche Daten-Pools errichten, deren kluge Verknüpfung erst konkretere Hinweise möglich macht. Denn anders als Hinweisverstärker zur Verdachtsfindung machen die Suchbegriffe des DHS keinen Sinn.

12. Die Botschaft des Kojoten

Böses Spiel! Eine Münchner Tagung prüft das Ausmaß der Datenspionage. (SZ, 15.07., Bernd Graff)

„Wenn ein Kojote die Falle erkennt, die ihm ein Trapper gestellt hat, dann läuft er nicht einfach davon weg. Nein, er macht einen großen Haufen darauf. Warum macht er das wohl?“, fragt Sean Devlin die etwa 30 Teilnehmer eines Workshops, die locker vor ihm auf dem Fußboden in der Eingangshalle der Münchner Akademie der Bildenden Künste sitzen. „Um seine Artgenossen zu warnen“, kommt schnell als Antwort. „Klar“, sagt Devlin. „Aber der Kojote zeigt dem Jäger auch, dass er die Falle gesehen hat. Er kommuniziert gewissermaßen mit dem Trapper und sagt: ‚I see you . . . Ich habe dich erkannt und durchschaue dich. Du stellst mir keine Fallen.‘“

Devlin war einen Tag zuvor Teilnehmer des Symposiums „Limits of Control. Wem gehören unsere Daten?“ gewesen, einer Veranstaltung der Akademie, begleitend zur Jahresausstellung, die ab dem 20. Juli unter demselben Rubrum stattfindet. Da allerdings sah Devlin nicht nur ganz anders aus, er wurde auch anders vorgestellt: als „Rex Bearchcode“, angeblich Sprecher der US-Firma Stratfor, eines Privat-Unternehmens, das strategische Untersuchungen anstellt und daraus mögliche Szenarien für seine Kunden ableitet.

Stratfor ist also so etwas wie ein privates Spionage-Unternehmen, und Devlin gab sich – verkleidet, mit Perücke – glaubhaft als dessen Sprecher aus. Markerschütternd glaubhaft. „Prism, das Datensammelsystem der NSA, ist nötig für unsere Sicherheit und bedeutsam im Kampf gegen den Terror. Verschlüsseln Sie Ihre Mails daher bitte nicht, wenn Sie nichts zu verbergen haben. Sie machen sich sonst nur verdächtig. Außerdem interessiert sich sowieso niemand für das, was Sie schreiben, weil es für uns wertlos ist“, sagte er etwa. Bearchcodes/Devlins Sätze kamen in solchen Salven, dass das Auditorium verwirrt und sprachlos war, die Moderatorin Ania Mauruschat von einem „Kultur-Clash“ sprach, der sich gerade ereigne. Alles nur ein Fake, wie sich dann herausstellte! Devlin ist Mitglied der „Yes Men“, einer amerikanischen Aktivistengruppe, deren politischer Protest sich in Form der Überassimilierung äußert: Sie geben sich als diejenigen aus, die sie kritisieren, und übernehmen deren bis ins Groteske verstärkten Argumente und Attitüden, um ihre Verlogenheit herauszustellen.

„Identitäts-Korrektur“ nennt die Gruppe das. Solche Überzeichnung scheint angesichts der Datenspionage durch die USA, die der Whistleblower Edward Snowden enthüllt hat, erst einmal nötig zu sein, um überhaupt begreifen zu können, was da eigentlich (mit uns) geschieht. „Man muss psychisch und intellektuell wieder auf Augenhöhe mit den Institutionen kommen, die uns ausspionieren“, sagte etwa der Techniker und „Evangelist“ der Open-Source-Firma Red Hat, Jan Wildeboer. Darin waren sich alle Vortragenden des Symposiums einig: Angesichts dessen, was mit unseren Daten im Internet mutmaßlich passiert, hat sich ein „diffuses Gefühl der permanenten Überwachung eingestellt, aber weiter sind wir noch nicht“. Denn, so die ernüchternde Feststellung der Tagung: Die Enthüllung von staatlicher Datenspionage im größtmöglichen Stil und der willfährigen Kooperation von Firmen wie Facebook, Microsoft, Apple, den großen privaten Datenaggregaten, „hat nicht zu Internetabstänzen und massenhaften Austritten bei Facebook geführt“.

Der Jurist Julius Mittenzwei, er ist Mitglied des Chaos Computer Clubs, erörterte, dass heute keine soziale Interaktion mehr ohne Online-Komponente auskomme, dass unser digitales Leben aber komplett erfasst werde. So bewahrheitete sich die Behauptung des Google-Bosses Eric Schmidt, der dem Menschen zwei Lebenszustände attestierte: Entweder er schläft oder er ist online. Da nun die Methoden zur Analyse unserer Online-Existenz, das Datamining, immer ausgefeilter werden, seien neue Machtpositionen entstanden, die Demokratie und Gesellschaft gefährden. Es sei darum eine „Notwehr durch Verschlüsselungs- und Anonymisierungs-Technologien“ im Netz nötig. Mittenzwei empfahl den Gebrauch des Anonymisierungsdienstes TOR (The Onion Router).

Felix Stalder, Professor für Digitale Kultur an der Universität Zürich, sprach von einem „Krieg der Daten gegen die Kommunikation“. Seine Unterscheidung ist hilfreich: Während auf der Ebene der Kommunikation, des menschlichen Austauschs, neue, dezentrale und offene kulturelle Formen im Netz entstehen, verhärtet sich die Ebene der Daten. Letztere werden maschinenlesbar und -analysierbar, sie liegen standardisiert und immer zentral vor, „aber eben nicht bei demjenigen, der sie produziert: nicht bei uns“. Kommunikation und Daten erleben daher unterschiedliche Dynamiken. „Es kann sein, dass Remix-Kultur und Polizeistaat jetzt miteinander kompatibel sind“, so Stalder.

Thomas Petri, der bayerische Landesbeauftragte für Datenschutz, forderte angesichts der Überwachung einen „Rußfilter für den Datenschutz“. Kein Auto würde ohne Filter ausgeliefert, also müsste auch die Kommunikations- und Internettechnologie damit automatisch ausgerüstet werden. Nur so sei „die Handlungs- und Mitwirkungsfähigkeit jedes Einzelnen zu erhalten. Die geschützte Privatsphäre schafft erst die freiheitlich demokratische Gesellschaft.“ Es scheint, wir sind angesichts der Komplettüberwachung noch nicht wesentlich weiter als der Kojote, der die Falle erkennt: Mehr als „Ich sehe dich“ können wir noch nicht sagen. Das aber immerhin.