Berendt, B., Dettmar, G., Demir, C., & Peetz, T. (2014). Kostenlos ist nicht kostenfrei. Oder: "If you're not paying for it, you are the product". LOG IN 178/179, 41-56.

http://www.log-in-verlag.de/1942-2/unterrichtsmaterial_informatikunterricht/

Bettina Berendt, Gebhard Dettmar, Cihan Demir, Thomas Peetz

Vorversion, 2014-06-01

1. Privatsphäre und Soziale Netzwerke im Unterricht – eine interdisziplinäre Herausforderung

Soziale-Netzwerk-Sites wie Facebook und Twitter erfreuen sich einer großen und noch immer steigenden Beliebtheit bei Jugendlichen wie Erwachsenen. Gleichzeitig stehen sie immer stärker im Fokus einer Vielzahl von Bedenken hinsichtlich ihrer Auswirkungen auf unsere Privatsphäre. Es geht um direkte und zeitnahe Auswirkungen, wenn etwa Facebook-Kontakte einen Wortbeitrag mit Dritten „teilen", das vom Autor für den kleinen Kreis gedacht war und in der nun schnell geschaffenen Öffentlichkeit als kompromittierend erfahren wird; es geht um indirekte Auswirkungen, wenn etwa früher arglos „geteilte" Partyfotos für potenzielle Arbeitgeber sichtbar sind; es geht um penetrante Werbung, die ganz offensichtlich früher besuchte Webseiten widerspiegelt. Darüber hinaus sind, wie wir spätestens seit dem Sommer 2013 wissen, all diese Inhalte auch diversen Geheimdiensten bekannt und der Bürger somit in zunehmendem Maße „gläsern".

Die Beliebtheit gerade bei Jugendlichen – die z.T. täglich mehrere Stunden auf Facebook verbringen – gibt besonderen Anlass zur Sorge. Eine wachsende Vielfalt von Aufklärungsmaterialien wird produziert und in verschiedener Weise im schulischen Kontext gebraucht, um die Medienkompetenz im Umgang mit diesen Plattformen zu erhöhen. Broschüren versuchen, zur Vorsicht zu rufen, ohne diese Absicht gleich durch den erhobenen Zeigefinger selbst zu unterlaufen. So schreibt z.B. [Klicksafe, 2013], produziert vom Safer Internet Programme der Europäischen Union (S.4):

> „Für den Schutz Deiner Privatsphäre bist Du auch selbst verantwortlich. Achte darauf, wie Du Dich im Netz zeigst!
>
> • Ein Foto darf ruhig auch mal lustig sein. Allzu peinliche oder beleidigende Fotos oder Meinungen haben in Sozialen Netzwerken aber nichts zu suchen. Sie können auch Jahre später wieder im Netz auftauchen und Dich sogar den Ausbildungsplatz kosten.
>
> • Überlege auch, was eine Gruppenmitgliedschaft über Dich aussagt. Die Gruppe „Saufen bis der Arzt kommt" ist keine gute Werbung für Dich. Hassgruppen, in denen andere gezielt beleidigt werden, gehen gar nicht.
>
> • Sei sorgsam mit Deinen Profil-Daten: Lass Anschrift, Telefon- oder ICQ-Nummern weg. Sie sind nicht nötig, wenn Du Dich mit anderen aus- tauschst. Auch Deine private E-Mail-Adresse solltest Du nicht jedem geben.
>
> • Überprüfe regelmäßig Deine Privatsphäre-Einstellungen. [...]

• Prüfe genau, wem Du freien Zugang zu Deinen privaten Fotos und Daten gibst. Du weißt nie, was sie mit den Informationen machen!“

Dennoch scheinen solche Aufrufe weitgehend ungehört zu verhallen. Woran liegt das? Auch wenn die Ratschläge in den meisten existierenden Materialien zweifelsfrei sinnvoll sind, erscheinen sie uns aufgrund von Erkenntnissen aus der interdisziplinären Privacy-Forschung[1] zu kurz zu greifen:

1. **Tragweite, Konzept.** „Privacy“ existiert gegenüber unterschiedlichen Klassen von „potenziellen Wissern“. Der Hauptaugenmerk in sozialen Netzwerken liegt gegenwärtig auf der *sozialen Privacy* (gegenüber anderen Menschen wie z.B. MitschülerInnen, LehrerInnen, Eltern oder potenziellen ArbeitgeberInnen), Informationsmaterialien gemahnen daran, wie wichtig es ist, das passende Publikum für seine Postings, Fotos usw. auszusuchen, und viel Zeit wird mit dem „richtigen“ Setzen von Sichtbarkeitseinstellungen in Websites verbracht. Hierbei wird aber leicht übersehen, dass unabhängig von den Privacy-Settings der Betreiber, also Facebook, sowieso Zugang zu allen Informationen hat und diese auch nutzt – unter anderem für personalisierte Werbung. Der Schutz vor solchem unerwünschten Mitwissen und entsprechender Nutzung ist erforderlich für die Wahrung *institutioneller Privacy*. Schließlich wünschen Bürger auch einen *Schutz vor Überwachung* durch allwissende staatliche Organe.

   Sowohl eine zu starke Fokussierung auf einzelne Aspekte als auch eine zu starke Vermischung der unterschiedlichen Interessen- und Problemlagen greift zu kurz. So vergisst man beispielsweise gern, dass restriktive Privacy-Settings in einem sozialen Netzwerk zwar Schutz gegen bestimmte Verletzungen der sozialen Privacy bieten können, aber dem Betreiber des Netzwerkes einen ökonomischen Vorteil verschafft, da er über „Monopolwissen“ über den Nutzer verfügt, was die institutionelle Privacy des Nutzers stark schädigen kann. Und das Wissen, dass man (von Institutionen, vom Staat oder auch von Privatpersonen) überwacht wird, kann nicht nur zum Abstumpfen gegenüber penetranter Werbung führen, sondern auch Meinungsfreiheit und damit Demokratie ernsthaft beschädigen.

2. **Verständnis von Datensammlung und –verarbeitung.** Was genau können Unternehmen und andere Akteure eigentlich mit unseren Daten machen, und woraus und worin bestehen dann die Privacy-Verletzungen? Hierüber wird gerade in den Medien oft eher undeutlich geraunt, und wohlmeinende Empfehlungen erschöpfen sich darin, dass man mit seinen „sensiblen“ Daten vorsichtig umgehen sollte (seine Adresse nicht verraten, keine Partyfotos einstellen, usw.) und sich auf diese Weise „schützen“ könne. Wer „nichts zu verbergen“ habe, brauche „nichts zu befürchten“. Diese Denkweise wurzelt fest im Glauben an kausale Modelle, im Glauben, dass wir einschätzen können, welche Rückschlüsse aus welchen Informationen gezogen werden können. Eine informatisch fundiertere Sichtweise zeigt jedoch, dass dieser Alltagsglaube zweierlei Kontrollillusionen beinhaltet: der Glaube an bewusste Datenpreisgabe und der Glaube an semantisch sinnvolle Wenn-Dann-Regeln. Die gebräuchliche Datensammlung durch das *Tracking* von Verhaltensdaten und die nicht-kausalen Modelle von Data Mining / „Big

[1] Vergleiche z.B. die Materialien des Projekts SPION (http://www.spion.me), in dem die AutorInnen Berendt und Peetz tätig sind.

Data“ unterlaufen jedoch diese Art von Kontrolle und Vorhersagbarkeit und erfordern weitergehende Informations- und Medienkompetenzen.

3. **Erweitertes Verständnis von Datensparsamkeit als Lösungsansatz.** „Privacy“ ist nicht nur Verstecken von Informationen und „Rückzug in die Privatsphäre“. Im Gegenteil sind sozialer Austausch *und* sozialer Rückzug normale Verhaltensweisen jedes Menschen, notwendige Elemente unserer fortwährenden Identitätsentwicklung und Bestandteile jeder Kultur. Die Bedürfnisse dieser Grenzziehungen zu anderen sind nicht nur individuell verschieden, sondern verändern sich auch situativ sowie in Antwort auf die Grenzziehungen des (sozialen, institutionellen oder staatlichen) Gegenübers, und oft führt eigene Verschwiegenheit in einer Situation zu einem umso größeren Mitteilungsbedürfnis später. Einseitige Appelle, „weniger von sich preiszugeben“, sind daher unrealistisch und werden daher langfristig im besten Falle ignoriert. Im Gegenteil geht es um das *effektive Nutzen von Tools*, das Kommunikation genauso umfasst wie Datensparsamkeit.

4. **Kompetenzen.** „Man kann sich dem Ganzen doch sowieso nicht mehr entziehen in unserer zunehmend digitalisierten Welt“. Gerade um Jugendliche besorgte Erwachsene äußern oft einen derartigen Technikdeterminismus oder –fatalismus. Und warum sollte man sich Gedanken machen um etwas „Alternativloses“, das „man eh nicht ändern kann“ ? In der Forschung gilt der Glauben an Technikdeterminismus als längst überholt – wenn es um Digitalisierung, Internet und Privatsphäre geht, müssen wir aber von Neuem daran arbeiten, Zuversicht und Engagement für das Gestalten sozio-technischer Systeme zu stärken. Zentral hierfür sind sowohl ein fundiertes *Verständnis* von Privacy und den Chancen und Risiken, die das Internet und soziale Netzwerke liefern, als auch *Kompetenzen*, um diese Räume für sich und andere (mit)zugestalten.

5. **Politisch; Interessenkonflikte.** Privacy ist „keine Privatsache“, sondern im Gegenteil ein Gut, das vielfältigen Interdependenzen unterliegt, das gesellschaftlich definiert, verhandelt, und geschützt werden muss, und steht damit auch im Spannungsfeld verschiedener Interessen, die keine allgemeingültige Definition zulassen, sondern das Anerkennen dieser Interessenkonflikte und ihre (im allgemeinsten Sinne) politische Lösung erfordern.

6. **Interdisziplinarität.** Neben die vermeintliche Alternativlosigkeit stellt sich oft eine vermeintliche Überkomplexität. Dieses kann gerade, wenn in der Schule versucht wird, das Thema Privacy zu behandeln, zur Resignation führen: LehrerInnen ohne informatischen Hintergrund können dann oft nur schematische Handlungsanweisungen vermitteln, die dem aktuellen Stand der Technik (oder dem von gestern) entsprechen mögen und in diesem Kontext „Medienkompetenz“ verkörpern, aber kaum Kompetenzen für morgen schaffen; Informatik-LehrerInnen können sich hingegen leicht von den vielfältigen soziologischen, politischen und psychologischen Fragen überfordert fühlen und sich dann eher auf spezifische Techniken oder Anwendungen z.B. zur Verschlüsselung konzentrieren. Das Thema Privacy *ist* komplex und kann daher nur interdisziplinär behandelt werden. Gerade hierin liegt aber auch sein didaktischer Reiz.

In diesem Artikel wollen wir eine Unterrichtsreihe darstellen, die sich dieser Herausforderungen annimmt. Sie besteht aus 10 Doppelstunden und wurde in den Jahren 2012 und 2013 zweimal durchgeführt: einmal zur Hälfte in der achten Klasse und einmal vollständig in der 11. Klasse der

gymnasialen Oberstufe. Die Reihe fokussiert auf institutionelle Privacy in den in den Punkten 2-6 erläuterten Dimensionen; klammert also zum Zweck der Fokussierung die Probleme staatlicher Überwachung aus. In ihrer gegenwärtigen Form ist die Reihe im Fach PGW (Politik, Gesellschaft und Wirtschaft) verankert; wir betrachten sie jedoch im vorliegenden Artikel aus der Perspektive der Informatik. Diese Perspektive stützt sich auf drei Säulen: Die AutorInnen Bettina Berendt und Thomas Peetz sind universitäre InformatikerInnen; der Autor Gebhard Dettmar ist Lehrer mit informatischem Hintergrund in Studium und Fortbildung. Schließlich behandelt die Reihe zentrale Themen schulischer Rahmenpläne (z.B. Berlin[2]): Datenbanken/Datenschutz, Netzwerke, Algorithmen, sowie fächerübergreifende Zusammenhänge.

2. Die Unterrichtsreihe: Überblick, Ziele, Themen und Methoden, Schulstufe

Überblick. Die Reihe behandelt die Auswirkungen, die Tracking im Internet und Datenauswertung der Datensammelindustrie, insbesondere von Internet-(Quasi-)Monopolisten wie Facebook oder Google, auf eine staatliche Ordnung haben müssen, die das Recht auf freie Persönlichkeitsentfaltung in das Zentrum ihrer "objektiven Wertordnung" stellt. In den Stunden 1-5 werden die sicherheits- und datenschutzrechtlich relevanten Themen der Reihe schrittweise entwickelt: Tracking und passgenaue Werbung, Data Mining und soziale Ausgrenzung (Krankenversicherung/Kreditrahmen), Psychometrie zu Facebook-Likes ("Big 5" der "Personal Traits" plus IQ). Darauf aufbauend gelangt die Reihe ab Stunde 6 zu den Folgen für Privatsphäre und die damit verbundenen Rechtsgarantien. Der Kurs wurde als S1/2 oder 3 PGW Kurs (= 11./12. Klasse, Politik/Gesellschaft/Wirtschaft) im Profil (4-stündig) entwickelt.

Ziele. Die SuS entwickeln Sensibilität gegenüber der Problematik von Datenschutz und SNS (Soziale-Netzwerk-Sites) und gelangen selbständig zu der Einsicht: *If you're not paying for it, you are the product*. Sie erwerben Kenntnisse über moderne Methoden der Datensammlung im Internet und ihrer Analyse mit Hilfe von statistischen Verfahren des Data Mining. Die SuS entwickeln nicht nur individuelle Kompetenzen zur besseren Steuerung von Datenströmen, sondern auch ein staatsrechtliches Bewusstsein als „Grundrechtssubjekte“ und mündige Bürger.

Themen und Methoden. Technische Details wie Third-Party-Cookies, Browsereinstellungen, Plugins, Proxies etc. werden eingeführt, vorgestellt und erläutert, die Hausaufgaben dienen der selbständigen Erarbeitung der Funktionsweise von Online-Tracking, dito das Rollenspiel zur Erarbeitung sozialer Ausgrenzungsmechanismen. Das Datenvolumen, das der "Datensammelindustrie" zur Verfügung steht, und die schier unbegrenzten Möglichkeiten bei deren Auswertung werden anhand des "preference tool" des Psychometric Centre der University of Cambridge vorgestellt und verdeutlicht. Anhand der Facebook Graph API wird eine Methode des Data Mining vorgestellt, der Apriori-Algorithmus zur Assoziationsregelentdeckung. Damit wird die oben formulierte Einsicht, dass der Nutzer das Produkt ist, konkretisiert und mit Inhalt gefüllt: ein Produkt, das am Markt platziert werden soll, muss aufbereitet werden. Das geschieht

[2] http://www.berlin.de/imperia/md/content/sen-bildung/unterricht/lehrplaene/sek2_informatik.pdf?start&ts=1283429474&file=sek2_informatik.pdf

auf Grund der Datenmengen, die der Industrie durch die User wissentlich oder unwissentlich zur Vefügung gestellt werden, maschinell, über Algorithmen des maschinellen Lernens und Data Mining.

Die Implikationen für die Privatsphäre liegen ab Stunde 6 auf der Hand, so dass die rechtliche Seite der Problematik ab nun im Zentrum steht: das Recht auf informationelle Selbstbestimmung, die freie Persönlichkeitsentfaltung und freie Meinungsäußerung und deren Bedeutung und Funktion innerhalb der Demokratie. Ein Rollenspiel mit Präzendenzfallcharakter steht am Ende der Reihe, in dem die SuS die zuvor erarbeiteten Themen im Kontext der Grundrechte – und ihre Rolle als mündige Bürger mit Anspruch auf Wahrung und Schutz dieser Grundrechte reflektieren.

Details inclusive der verwendeten Materialien und einer Stundenverlaufsplanung sind unter http://www.schul-web.org/geschichte/kiwi/pgw.html zu finden.

3. Ansatz „Informatik im Kontext“: Erarbeitung der vielschichtigen Rolle informatischer Prozesse für die Privatsphäre

In diesem Abschnitt sollen Konzept und Aufbau der Reihe aus einer informatischen und interdisziplinären Perspektive dargestellt werden. Das Konzept wird mit Hilfe eines „Zwiebelmodells“ der Informatik und des Wegs der Unterrichtsreihe durch diese „Schichten“ dargestellt (Abb. 1). Das Ablaufdiagramm in Tabelle 1 zeigt die spezifischen Konkretisierungen dieser allgemeinen Aspekte der Informatik sowie spezifische Themen aus Politik, Gesellschaft und Wirtschaft.

Wir stellen diese konzeptuellen Betrachtungen an den Anfang, um zu verdeutlichen, dass die Reihe je nach fachlicher Einordnung auch stärkere Akzente auf bestimmte Inhalte setzen könnte. So könnten die angesprochenen Datenmodelle, Algorithmen und Webtechnologien bei Verortung im Informatikunterricht detaillierter behandelt und z.B. durch Eigenentwicklungen der Schüler (Datensammlung, Programmierung, Datenanalyse) vertieft werden. Unsere eigene derzeitige Planung sieht die Weiterentwicklung der Reihe sowohl innerhalb des jetzigen Rahmens PGW als auch innerhalb des im Bundesland Hamburg derzeit entwickelten Profils *Informatik-PGW* vor.

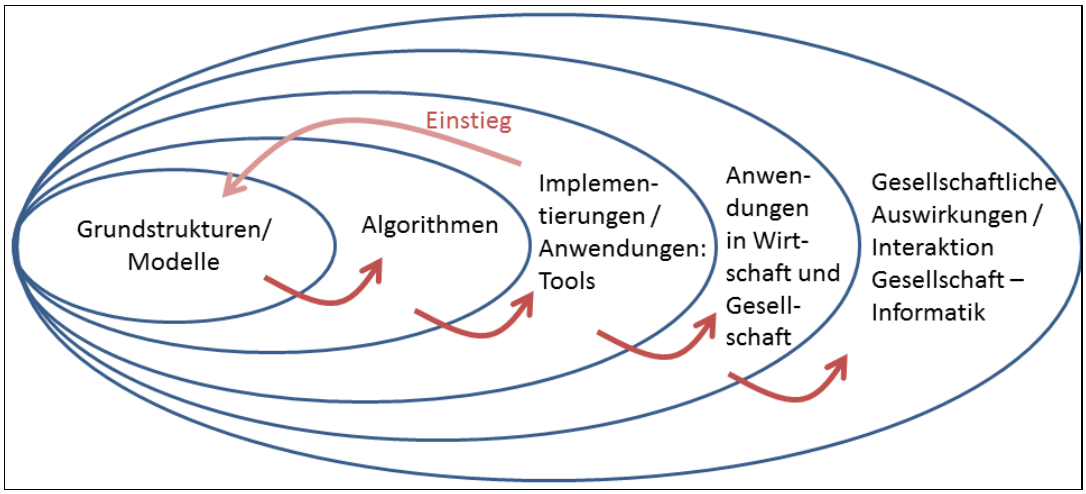

Abbildung 1: „Zwiebelmodell“ der Informatik und der Weg der Reihe durch diese Schichten

Datensammlung: Tracking (N)
Datenverarbeitung: Profil- und Verhaltensdaten, Data Mining (M, D), Korrelation statt Kausalität
Datenverarbeitung und Nutzung für personalisierte Werbung: Geschäftsmodelle von „Gratis“diensten → Interessenkonflikte → Rollenspiel
Datenverarbeitung und Nutzung für Zugang zu Produkten und Dienstleistungen: Data Mining und „Weblining“
Datenverarbeitung: Profilbildung und Vorhersagen (D)
Datenverarbeitung: Assoziationsregellernen mit Apriori, auf Daten aus der Facebook-API (A, N)
Datenverarbeitung und mögliche Nutzung für Zugang zu Bildung, Arbeitsplätzen: Regression und Vorhersagen (D)
Das Recht auf Informationelle Selbstbestimmung
Die Bedeutung des Meinungspluralismus für die Demokratie
Grundrechtskonflikte: Vertragsfreiheit vs. Informationelle Selbstbestimmung? → Rollenspiel

Tabelle 1: Ablaufmodell der Reihe mit Kernaussagen der Unterrichtsstunden. Im engeren Sinne informatische Inhalte sind durch A (Algorithmen), D (Datenbanken) und N (Netzwerktechnologie) markiert.

4. Details: Die drei Teile der Reihe: Inhalt, Didaktik und Unterrichtsmethodik

4.1. Teil I: Tracking und Profiling – Datenerfassung und –auswertung

Als Einstieg wurde das Video *Datenschutz und Datenverschwendung – NDR Extra 3 vom 07.03.2010* [NDR, 2010] gewählt, in dem die aufgezeigte Naivität der "Probanden" bzgl. ihrer Privatsphäre für Spott und Unverständnis sorgt (was im weiteren Verlauf der Reihe mit der Erkenntnis der eigenen „Sorglosigkeit“ auf sozialen Netzwerken kontrastiert wird). Anschließend wird mit dem ***Tracking*** ein Grundmerkmal von Online-Welten in den Fokus gerückt: Was immer man tut, hinterlässt (Daten)spuren, und diesen folgen verschiedene Arten von Programmen, die dadurch Verhaltens- und allgemeiner Persönlichkeitsprofile erstellen. Hierzu arbeiten wir mit dem Tracker-Manual [Peetz & Berendt, 2012], in dem die Funktionsweise von Third-Party-Cookies und anderen Trackern erläutert wird und die SuS durch Aufgaben dazu gebracht werden, Browserplugins zum Beobachten und Blockieren bestimmter Tracker zu installieren und zu gebrauchen. Hiermit wird nach dem anfänglichen

Erschrecken der SuS, dass sie beobachtet werden, ein handlungs- und kompetenzorientierter Einstieg gewählt.

Durch die verwendeten Methoden werden unterschiedliche Kompetenzen geschult, was hier exemplarisch nur für die ersten beiden Doppelstunden beschrieben wird: Die ersten beiden Doppelstunden finden im Computerraum statt. Die Erstellung einer Mindmap in der Mitte der ersten Doppelstunde dient der Verständnissicherung, und die SuS üben die Visualisierung komplexer Zusammenhänge und Ordnung von Begrifflichkeiten und Gedankengängen. Plugin-Installation und Präsentation von Proxies schult die Medienkompetenz am PC. Die Lerner-Aufgaben aus dem Tracker-Manual werden in Gruppenarbeit bearbeitet, da sich über gemeinsame Surfpräferenzen die Funktionsweise des Onlinetrackings am besten erschließt. Die schriftliche Dokumentation der Bearbeitung dient neben der Ergebnissicherung auch dem Einüben des Erstellens schriftlicher Dokumentationen, Pflichtenhefte usw. – Dingen, die in der Arbeitswelt auch gefragt sein werden.

4.2 Teil II: Data Mining – Datenanalyse ohne Kausalität?!

Darauf folgen zwei Texte zur **Auswertungsmethodik** des so gewonnenen Datenmaterials. Diese Methoden tauchen in der öffentlichen Diskussion über Privatsphäre und Social Networks bisher selten bis nie auf, obwohl sie es doch sind, die das Bedrohungspotential der Datensammelindustrie für die Privatsphäre so unkalkulierbar machen. Die Texte [Graff, 2010a, 2010b] vermitteln den SuS die Attraktivität und das Potential des Trackings anschaulich und nachvollziehbar: Parteizugehörigkeit aus Twitter-Kontakten, das rein korrelative Vorgehen vieler Methoden des maschinellen Lernens / Data Mining und die Folgen für das kausal determinierte Weltbild seit der kopernikanischen Wende – kurz: die Mächtigkeit der Auswertungsmethoden und ihre völlige Undurchschaubarkeit. Anhand dieser Texte wird ein Überblick über informatische Methoden erarbeitet, insbesondere Induktion, maschinelles Lernen, Data Mining und unüberwachtes Lernen, die für die Datenauswertung zentral sind.

Ein Verständnis der Implikationen dieser informatischen Methoden erfordert Wissen über ihre **Anwendung in den kommerziellen Kontexten** von eCommerce und SNS. Dieses wird mit Hilfe eines Auszug aus einem Artikel über KDD (Wissensentdeckung in Datenbanken) im eCommerce [Dettmar, 2002] sowie FBs Datenverwendungsrichtlinien [Facebook, 2013ff.]. Letztere liefert einen ersten Eindruck zu den Implikationen des maschinellen Lernens für FBs Geschäftsmodell: Sämtliche persönlichen Daten, die der Nutzer oder andere explizit angeben, alle (Verhaltens-)Daten, die durch die Nutzung der Plattform entstehen, und alles, was daraus abgeleitet werden kann (mittels i.d.R. nicht-öffentlichen Data-Mining-Modellen), wird „verwendet“. Auch wenn diese Verwendung keine Weitergabe oder gar Verkauf von Datensätzen beinhaltet, die den Nutzer mit Namen o.ä. identifizieren (obwohl auch dieses in gewissem Rahmen durch neuere

Versionen der Datenverwendungsrichtlinien ermöglicht wird), so wird Geschäftspartnern doch Zugang zu Nutzern mit wohldefinierten Eigenschaften verschafft (z.B. indem sie Werbung auf bestimmten Profilen schalten).

Um der weitverbreiteten Auffassung entgegenzutreten, dieses involviere doch „nur" lästige Werbung, die man im Interesse der umsonsten Nutzung von Online-Angeboten in Kauf nehmen und ansonsten ignorieren könne, folgen nun **praktische Beispiele für die Anwendung dieser Methoden durch die Datensammelindustrie**. Andrews [2012] stellt Szenarien vor, die über passgenaue Werbung weit hinausgehen: Wer in Gitarrengeschäften einkauft, ist weniger kreditwürdig. Die notwendige Folge der Stereotypisierung des „Produkts Nutzer" ist eine neue Form der sozialen Distinktion und Ausgrenzung: aus *Redlining* wird *Weblining.*

Die Erkenntnisgewinne der bis hierhin gelesenen Texte werden nun in einem **Rollenspiel** verarbeitet, in dem alle drei beteiligten Rollen zur szenischen Darstellung gelangen: Anbieter, Kunde und Produkt (= Nutzer). Die Durchführung in Form eines Spiels gewährleistet ein vertieftes Verständnis der beteiligten Interessen mit allen sich daraus ergebenden Konsequenzen. Die von Andrews [2012] beschriebene Ausgrenzung zeigt den weiteren zu erwartenden Weg auf: die kontinuierliche Durchlöcherung der Privatsphäre im Zuge der Datenauswertung. Damit stellt sich aber auch die Frage, welche Rolle der Privatsphäre innerhalb der Demokratie zukommt. Ebendies ist Thema des weiteren Reihenverlaufs.

Die szenische Darstellung des Rollenspiels setzt eine genaue Reflexion über die Geschäftsinteressen der Anbieter und deren Kunden voraus. In unserem Unterricht und auch in anderen Diskussionen sorgen der Text und insbesondere das Beispiel „Gitarrengeschäft → mangelnde Kreditwürdigkeit" zuverlässig für Aufsehen, Empörung und Ungläubigkeit.

Deshalb wird im weiteren Stundenverlauf an einem möglichst nachvollziehbaren Beispiel in die Funktionsweise eines ausgewählten Data Mining-Algorithmus, i.e. **Apriori**, eingeführt, der zu verdeutlichen geeignet ist, wie sich aus einer hinreichend großen Datenbasis Assoziationsregeln gewinnen lassen, ohne dass kausalgeleitete Vorannahmen des Analysten am Anfang der Auswertung standen. Die Hausaufgabe leistet den Transfer zu SNS, indem die Attribute und daraus erstellbare Assoziationsregeln nun aus der **Facebook Graph API**[3] gewonnen werden.

Es bleibt jedoch nicht bei Vorhersagen zur Kreditwürdigkeit. Anfang März 2013 berichtete die Presse, dass Forscher des Psychometric Centre der University of Cambridge aus Facebook-Likes die "Big Five" der Persönlichkeitsmerkmale vorhersagen können, dazu Intelligenzquotient, Drogenkonsum, sexuelle Orientierung, Hautfarbe, Beziehungsstand der Eltern im Alter von 21 u.ä. [Kosinski et al., 2013] Für jedes dieser Persönlichkeitsmerkmale erläutert das ***Preference***

[3] https://developers.facebook.com/tools/explorer

Tool (www.preferencetool.org) auch Aussagegehalt und Nutzen für Werbetreibende, Arbeitgeber, Schulen und Universitäten ("Educational Settings"). Zugespitzt ausgedrückt, ließen sich damit ließen die Assessment-Center von Firmen ersetzen, die Jobsuche (und –vergabe!) könnte über Facebook stattfinden. Die Implikationen dieses Tools für Zukunft der Privatsphäre sind nicht auszudenken: bald kennt Facebook uns beser als wir uns selbst.

Daher sollen die SuS zunächst in Partnerarbeit gegenseitig Persönlichkeitsprofile erstellen, um diese im nächsten Schritt mit YouAreWhatYouLike.com (einer von denselben Autoren entwickelten App) abzugleichen. In der Spion-Schülergruppe sorgte dies, gelinde gesagt, für Irritationen. Im Folgenden lesen die SuS, je nach Englischkenntnissen, entweder den wissenschaftlichen Text aus PNAS, oder sie durchstöbern preferencetool.org, wobei man ihnen zumindest den Abschnitt "Predictive Power of Likes", S. 3, präsentieren sollte, da hier die Autoren die Frage nach dem kausalen Zusammenhang behandeln. Wenn das Recht auf informationelle Selbstbestimmung zur Behandlung ansteht, wird klar, warum das so wichtig ist.

4.3 Teil III: Demokratie – unser Grundrecht auf informationelle Selbstbestimmung und auf den Schutz dieser Rechte

Nachdem die Privatsphäre der Facebook-User, also auch der KursteilnehmerInnen, derartig unter Beschuss geraten ist, stellt sich nun die Frage nach ihrer Funktion innerhalb der Demokratie. Definitionen wie „Privacy ist the right to be let alone“ mögen im Ansatz hilfreich sein, doch die eigentlich interessante Frage ist, wie und wohin sich eine Demokratie ohne Privatsphäre entwickelt. Das wurde im **Volkszählungsurteil** 1983 im Zuge der Definition der Informationellen Selbstbestimmung beantwortet: wer nicht absehen könne, was zu welchem Zweck über ihn gespeichert werde, der sehe sich gezwungen, sein Verhalten am Mainstream auszurichten (Panoptismus führt zu Konformität). Interessanterweise hat die Verwendung des Preference Tools gezeigt, dass Konformität auch nichts mehr nutzt, da (a) auch aus „ganz normalem Verhalten“ (wie z.B. dem *Liken* von Coca Cola oder Converse) unerwünschte Vorhersagen (wie z.B. ein extrem niedriger IQ) getroffen werden und (b) eben *aus beliebigen Eigenschaften und Verhalten* völlig unvorhersehbare Vorhersagen und damit Konsequenzen folgen können. Deshalb ist die Kausalitätsfrage (s.o.) so bedeutend: Die nicht kausal-basierten Auswertungsmechanismen machen jede Steuerung des Nutzers unmöglich.

Der folgende Text von Rudolf Wassermann [2000] definiert den **Meinungspluralismus** und seine Funktion für die Gemeinwohlfindung innerhalb der Demokratie. Das eigentliche Thema, NPD-Verbot, wurde gekappt, so dass die SuS einzig Wassermanns Ausführungen zur Rolle des Meinungspluralismus zu lesen bekommen. Damit sind sie nun in der Lage, Meinungspluralismus und Panoptismus einander gegenüberzustellen, so dass die demokratiegefährdende Wirkung der Datenspeicherung und –auswertung durch große Internetfirmen wie auch andere

(insbesondere staatliche Akteure, vgl. die Diskussion seit 2013 rund um die Snowden-Enthüllungen) deutlich werden, die sie im Arbeitsschritt zuvor dem Panoptismus zugeordnet haben.

Bis hierhin werden die SuS bereits einige Male gefragt haben, was "der Gesetzgeber" zu all dem sagt, d.h. sie beginnen, sich in ihren Grundrechten beschränkt zu fühlen, wozu ja auch aller Grund besteht. Auch wenn ein Nutzer in die Geschäftsbedingungen und Privacy-Richtlinien eines Unternehmens eingewilligt hat, werden die Grundrechte durch solche privatrechtlichen Vereinbarungen nicht außer Kraft gesetzt. Der hier zu konsultierende Ort ist das **Lüth-Urteil** des Bundesverfassungsgerichts von 1958,dessen Urteilsbegründung in nuce lautet: Die Grundrechte gehen nicht in ihrer Abwehrrolle gegen staatliche Eingriffe auf, sie besitzen einen "objektiv-rechtlichen Grundrechtsgehalt", sind aktive Rechte, die in jeden Bereich des Rechts, also auch das Privatrecht, also auch in *Terms of usage* ausstrahlen: "In Umkehr der Schutzrichtung des subjektiv-defensiven Abwehranspruchs 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." [Dreier, 1993, S. 47].

Hier liegen also alle Voraussetzungen für eine kontroverse Diskussion vor, die den Abschluss der Reihe bildet: Wenn der "Big Brother" des 21. Jahrhunderts die Datensammelindustrie ist, muss dann der Staat den Bürger vor sich selbst schützen oder ist das auch dann noch als Paternalismus zu bezeichnen, wenn eine Erosion der Grundrechte zu konstatieren ist? Kann der datenschutzbewusste Bürger die Dienste der Industrie nutzen und gegen die Auswertung des so entstehenden Datenmaterials klagen, da nicht grundrechts-konform? Kurz: sind Internetnutzung und Datenschutz noch unter einen Hut zu kriegen, und welche Aufgaben erwachsen dabei dem Staat? Die hier zutage tretenden Wechselwirkungen und Konflikte zwischen den Grundrechten der Privatautonomie und freien Vertragsgestaltung einerseits und dem Recht auf informationelle Selbstbestimmung und Schutz der Privatsphäre andererseits behandeln wir in einem abschließenden **Rollenspiel**, in dem je eine Gruppe für eine dieser beiden Seiten argumentiert und eine dritte Gruppe überzeugen muss.

5 Erfahrungen mit der Durchführung der Reihe

Der folgende Erfahrungsbericht fokussiert auf didaktische Entscheidungen und Verhalten der SuS. Wo für den Lesefluss erforderlich, wurden inhaltliche Punkte der Gestaltung aus den Abschnitten 4.1-4.3 wieder aufgegriffen und/oder näher ausgeführt. Schlussfolgerungen, die sich aus den Erfahrungen ergaben und die auch direkt die Reihengestaltung beeinflussten, sind

kursiv markiert. Wir schließen mit Beobachtungen zu den Ergebnissen aus Lehrer- und Schülersicht.

5.1 Teil I: Tracking und Profiling – Datenerfassung und –auswertung

Die Reihe wurde testweise im Schuljahr 2012/13 im Informatikkurs einer 8. Klasse gehalten, sowie auszugsweise in einem PGW-Profilkurs (4-stündig) der 11. Jahrgangsstufe (S2). Da sie für die Oberstufe entwickelt wurde und ihre vollständige Durchführung Voraussetzung für belastbare Ergebnisse darststellt, beschränke ich mich i.f. auf die Darstellung der Durchführung in einem S1-Kurs PGW im Schuljahr 2013/14[4] und ziehe die Testdurchläufe dort heran, wo sie meine Beobachtungen zu ergänzen geeignet sind.

Alle SuS haben haben hohe Kompetenzen bzgl. sozialer Privacy[5] und nehmen diese ernst. Auch in der analogen Welt ist Privatsphäre von hoher Bedeutung für sie. Entsprechend fielen die Reaktionen auf das Einstiegsvideo (NDR, 2010)[6] - aus, Ungläubigkeit, Hohn und Spott, gemischt mit der Vorahnung, dass sie angesichts des Reihenthemas ihre online-Privacy auf Facebook, Whatsapp, Tumblr etc. auch nicht eben mustergültig wahrnehmen. In der anschließenden Diskussion fragte eine Schülerin nicht ohne Selbstironie, wer denn bitte vor der Account-Erstellung die Nutzungsbestimmungen läse.

Damit war der vorentlastende Einstieg in das Tracker-Manual von Berendt und Peetz (2012) vollzogen. Der Inhalt in nuce: Behandelt wird das Thema Tracking im Internet am Beispiel eines Shop-Assistants in z.B. einem Smartphone-Shop. Durch genaue Kunden-Beobachtung erschließt er die Kundenpräferenzen. Nun wird das Szenario ausgeweitet: der Verkäufer erhält eine Prämie auf alles, was der Kunde kauft, analog zu Vorgehen im Smartphone-Shop müsste er nun den Kunden auf Schritt und Tritt in sämtlichen Lebensbereichen verfolgen und beobachten, was, darüber herrschte Einigkeit, jedermann die Polizei rufen lassen würde.

Das bewirkte einen gewissen Überraschungseffekt im Fortlauf der Lektüre, da im Internet exakt dies geschieht: 3rd-party-cookies und Austausch der gesammelten Daten seitens der Datensammelindustrie gewährleisten eine lückenlose Kontrolle über Surfverhalten und Konsumgewohnheiten im Web.

Im Laufe der Besprechung fiel von Schülerseite der Ausdruck 'Stalking' für das Vorgehen des Shop-Assistants, was den Sachverhalt recht gut trifft. Dieses Stalking wurde nun visualisiert durch die Browser-Plugins Collusion und Ghostery – die SuS surften auf ihren Lieblingsseiten und analysierten anschließend die Tracking-Pfade in Collusion. Dabei fiel auf, dass ihre User-Kompetenz recht gering ausgeprägt war – viele wussten nicht, was Browser-Plugins sind, wie man Cookies löscht, wie man seine Browser-Einstellungen (am Beispiel Mozilla) anpasst etc.

---

[4] Alle besprochenen Texte mit Arbeitsaufträgen sind online verfügbar unter http://www.schul-web.org/geschichte/kiwi/texte-spion-neu.pdf, der Unterrichtsentwurf unter http://www.schul-web.org/geschichte/kiwi/unterrichtsentwurf_spion-neu.pdf .

[5] Getestet mit PrivacyCheck, http://www.rabidgremlin.com/fbprivacy/, mit dem auf Facebook niemand unter 17 von 21 Punkten kam.

[6] In dem Video lassen sich Passanten von als Datenschützern getarnten Extra 3 – Mitarbeitern zur Herausgabe sensibler Daten wie Konto-Pin u.a. verleiten, obwohl, bzw. weil ihnen der Schutz ihrer Daten wichtig ist.

Dies lieferte einen ersten Hinweis auf einen Umstand, der zentral für die Planung der Reihe und das Projekt SPION ist und auch in den vorausgegangenen Testläufen zu beobachten war: Die User lassen sich in der online-Welt eine Ausspähung, cf. oben erwähntes Stalking, gefallen, die sie in der offline-Welt sofort die Polizei rufen lassen würde. Woran liegt das? Zu einem nicht geringen Teil daran, dass wesentliche technische Voraussetzungen schlicht unbekannt sind. Die Ausspähung vollzieht sich geräuschlos und unsichtbar, das ist der entscheidende Unterschied zur analogen Welt. Exakt hierin unterscheiden sich auch soziale und institutionelle Privacy – über Verletzungen derselben im sozialen Bereich bekommt man unmittelbar Rückmeldung, für den institutionellen gilt das nicht – wir haben hier eine kafkaeske Situation, die allerdings nicht als Bedrohung wahrgenommen wird.

5.2 Teil II: Data Mining – Datenanalyse ohne Kausalität?!

Bei der Lektüre zweier Artikel aus der Süddeutschen Zeitung zum Thema (Graff 2010a,2010b) ging es nunmehr um folgende Lernziele: (a) die Unterscheidung zwischen "statischer" und "prozessual-dynamischer Merkmalserfassung", wobei mit ersterer Angaben wie Namen, Körpergröße etc. gemeint sind, mit letzerer Verhaltensdaten wie Kommunikationsspuren, Ortsangaben und Konsumnachweise; (b) die Überlegenheit der maschinellen Auswertung dynamischer gegenüber statischen Merkmalen; und (c) die Fragwürdigkeit des in allen Geschäftsbedingungen betonten "Schutzes" persönlicher Daten, wenn dies nur bedeutet, dass sie zwar vielleicht nicht oder nur anonymisiert an Dritte weitergegeben werden, aber ausgewertet werden, um Dritten selektiv und zielgenau nach hochprädiktiven "Profilen" Zugang zu ausgewählten Nutzern zu geben. (Wer dann auf ein solches, beispielsweise als Werbebanner eingeschaltetes Angebot klickt, gibt sich als Mensch mit dem spezifizierten Profil zu erkennen.

Konsequenz: Der in der Datenverwendungsrichtlinie versprochene Schutz suggeriert eine illusorische Sicherheit, die dazu verleiten kann, sehr mächtige Typisierungsalgorithmen beständig mit Datenmaterial zu versorgen, was den „Schutz" vollständig aushöhlt – ein trojanisches Pferd. Daher erscheint folgendes Szenario nicht mehr weit entfernt: "*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.*" Dieses Lernziel wurde gut erreicht und aufgenommen, die SuS erhielten Klarheit darüber, dass die gerade bei Jugendlichen sehr verbreiteten Fake Accounts nur einen äußerst geringen Schutz für die eigene Privatsphäre bieten.

Die folgende Stunde behandelte einen Aspekt, der für das Bedrohungspotential sozialer Netzwerke sehr wesentlich ist, in der Öffentlichkeit aber kaum behandelt wird: beim "unüberwachten Lernen" finden die Algorithmen ihre Hypothesen (z.B. Assoziationsregeln) selbst, z.B. Korrelationen wie "Menschen, die X ihre Lieblingsspeise nennen, den Sport Y niemals betrieben haben und nichts gegen weiße Socken einzuwenden haben, wählen Partei Z."

Hier war ein wissenschaftspropädeutischer Exkurs nötig: den SuS waren (erwartungsgemäß) Verhältnis und Unterschiede der Begriffe Kausalität, Koinzidenz und Korrelation nicht geläufig, ein Rekurs auf die kopernikanische Wende diente zur Rekapitulation unseres kausal geleiteten Weltbildes, das im gängigen Data Mining durch den Fokus auf Korrelationen ersetzt wird.

Dies impliziert u.a., dass die erfolgte Stereotypisierung und Profilerstellung für den Nutzer selbst dann vollkommen undurchschaubar ist, wenn er die verwendeten Auswertungsalgorithmen und ihre Funktionsweise kennt. Das wirft die Frage auf, ob die in der gegenwärtigen Diskussion zur Novellierung des Datenschutzrechts häufig geäußerte Forderung, die "Logik" der Auswertung offenzulegen (z.B. Council of Europe, 2010), nicht zu kurz greift: Es sind die Daten und die aus ihnen gewonnenen Mining-Resultate (und nicht der Algorithmus), die ein wohlbehütetes und rechtlich geschütztes Geschäftsgeheimnis bilden, aber denen eben auch die soziale Sprengkraft innewohnt. Diese Diskussion wird zwar in Wissenschaft und Politik bereits (noch relative vereinzelt) geführt, ist aber in der öffentlichen Wahrnehmung noch kaum angekommen.

Diese Überlegungen sind Ziel der beiden Arbeitsaufträge für die SuS: 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.

Erwartet wurde zu 1.: Das Beispiel, das Facebook angibt, ist harmlos und banal (*an advertiser can choose to target 18 to 35 year-old women who live in the United States and like basketball.*), tatsächlich ist es unvorhersagbar, in welchem Profil ich lande und wer sich demzufolge dafür interessieren könnte. Zu 2.: "*but we do not tell the advertiser who any of those people are.*" bietet keinerlei Schutz meiner Privatsphäre, wenn man voraussetzt, dass personalisierte Werbung "funktioniert".

Diese Einsicht erfolgte schleppend und erforderte ein gewisses Maß an Lehrerlenkung, was offensichtlich darauf zurückzuführen ist, dass der Mensch sich ungern von kausalem Denken verabschiedet. Dazu kommt, dass SuS Werbung grundsätzlich ignorieren, was als Erwachsener weit schwieriger durchzuhalten ist, wenn sich die Werbung auf Grundbedürfnisse wie Vermietung, Krankenversicherung, Job u.ä. bezieht.

Offen blieb bislang, wie solche Profile in der Realität aussehen können. Das von Andrews [2012] gelieferte Beispiel aus dem Bereich Risk Management bei Banken und Kreditkartenunternehmen – Herabsetzung des Kreditrahmens nach Einkauf in Gitarrengeschäften – war zu verknüpfen mit den bisher gelesenen Texten: Wir wissen, dass unser Online-Konsumverhalten dank Tracking verschiedenster Firmen – Andrews benutzt den Ausdruck „Datensammelindustrie" – bestens bekannt ist, wir wissen, dass die Auswertung nicht kausalitätsbasiert erfolgt, so dass sich Fragen nach dem Zusammenhang von Gitarre spielen und Kreditwürdigkeit erübrigen, wir wissen, dass die Generierung von Wissen über Kunden im Interesse ökonomischer Selektion zu sozialer Ausgrenzung führen kann.

Trotz des Wissens um die nicht kausalitätsbaiserte Auswertung erzeugte dieses Beispiel Ungläubigkeit, Unbehagen, ja Empörung, was zunächst völlig im Sinn der Reihe ist, die ja die Ignoranz gegenüber institutioneller Privacy und ihren täglichen Verletzungen erschüttern soll. Allerdings besteht dabei die Gefahr, dass die als bedrohlich empfundene Wirklichkeit mit Wunschdenken und Realitätsverweigerung konterkariert wird – was nicht sein darf, kann auch nicht sein, ergo machen wir weiter wie bisher. Dies wurde im Verlauf der Reihe immer deutlicher.

In dem folgenden Rollenspiel wurden die bisherigen Lernerfolge geprüft: eine Gruppe von Facebook-CEOs (Gruppe 1) wertete zusammen mit potentiellen Kunden (Gruppe 2) die Chats von Nutzern (Gruppe 3) aus und entwickelte daraus Profile – im Unterschied zu den vorher diskutierten Methoden jedoch dadurch, dass hier menschliche Analysten kausalbasierte Schlüsse ziehen. Dies wurde als legitim erachtet, da die Auswertung das Verständnis der Problematik nicht voraussehbarer Profilerstellung überprüfen soll und die SuS bis hierhin genügend kausal nicht erklärbare Auswertungen kennengelernt haben. Der Chatverlauf nahm die Anregungen aus den Rollenkarten auf – Mountainbiken vom Tibi Dabo, Snowboarden – einer der Kunden war ein Krankenversicherer, der daraufhin sofort die Erstellung des Profils „Risikosportarten-affin" forderte, um von den über dieses Profil hergestellten Kontakten höhere Monatsbeiträge zu erheben.

Weniger erfolgreich verlief ein für das Reihenziel bzw. dessen Verständnis unabdingbarer Baustein: die Behandlung des Apriori-Algorithmus. Hier wurde einhellig eine zu informatische Ausrichtung der Reihe beklagt, die sich im PGW-Rahmenplan gewiss nicht wiederfände. *Schauen wir dazu in die aktuell gültige Fassung von 2009[7], so finden wir: „Ein verständiger Umgang mit aktuellen Informations- und Kommunikationstechnologien und ihren Kooperations- und Kommunikationsmöglichkeiten wird zunehmend zu einem wichtigen Schlüssel für den Zugang zu gesellschaftlichen Wissensbeständen [...]". Im Fortlauf wird jedoch deutlich, dass mit der hier als Ziel identifizierten Medienkompetenz lediglich „sicherer Umgang mit dem PC" gemeint ist. Im Gegensatz hierzu wird in unserer Unterrichtsreihe das Verständnis informatischer Methoden als Voraussetzung für das Verständnis politisch und gesellschaftlich relevanter Sachverhalte betrachtet. Auch wenn fächerübergreifendes Lernen anhand des Herstellens auch außerfachlicher Bezüge gesellschaftlich relevanter Aufgaben laut Rahmenplan expressis verbis nur im Profilbereich angestrebt wird[8] (und unsere Reihe in einem Grundkurs stattfand), möchten wir doch als Desiderat festhalten: Wann immer Algorithmen gravierende Auswirkungen auf politische, gesellschaftliche, wirtschaftliche und wissenschaftliche Zusammenhänge und Entwicklungen haben (hier: Abkehr von einem kausal determinierten Weltbild), , muss ein/e Lehrer/in zumindest exemplarisch einen dieser Algorithmen in jedwedem Fach behandeln können, das Lerninhalte aus den genannten Bereichen vermittelt, um einen konzisen und konsistenten Reihenverlauf garantieren zu können.*

Umgekehrt wäre bei einer Einbettung der Reihe in den Informatik-Unterricht ein analoger kritischer Bezug auf die Rahmenpläne zu erwarten: hier könnten insbesondere die Texte aus dem letzten Teil der Reihe als „zu gesellschaftswissenschaftliche Ausrichtung" gebrandmarkt werden. Aber die hier untersuchten Folgen des Einsatzes von Informatik können eben auch nur vollständig verstanden werden unter Bezug auf ihre Folgen für unsere Grundrechte, inkl ihrer Relevanz und inneren Logik. *Die Thematik „Privatsphäre" zeigt also exemplarisch auf, wie zentral echte*

[7] s. http://www.hamburg.de/contentblob/1475228/data/p-g-w-gyo.pdf, S. 6

[8] a.a.O., S.7

Interdisziplinarität im Schulunterricht ist.

Leider wurde auch die mit dem Thema „Apriori-Algorithmus“ verknüpfte Hausaufgabe, selbständig mit Hilfe des Algorithmus und Daten aus der Facebook Graph API eine Assoziationsregel abzuleiten, nicht bearbeitet. Dies wirkte sich auch nachteilig auf den folgenden Themenschwerpunkt aus: das Psychometric Centre der University of Cambridge, seine u.a. in [Kosinski et al., 2013] beschriebenen Forschungsresultate und sein kommerzielles “Preference Tool“.

Es ging vielversprechend los: Die „Big 5 der Persönlichkeitseigenschaften“ stellen für sich in der Selbstfindungsphase befindende Heranwachsende ein relevantes und interessantes Thema dar. Die Vorhersage dieser Eigenschaften aus Facebook-Likes führte zu noch stärkerer Überraschung als Assoziationsregeln wie „Gitarrengeschäfte → eingeschränkte Kreditwürdigkeit“. Auch dieser Artikel (genau wie der Einsatz der beschriebenen Befunde im Tool) zeigt Beispiele rein korrelativer Zusammenhänge und ihrer Anwendung zur Vorhersage. Der Artikel zeigt einerseits auf, wie kausal zu erwartende Zusammenhänge oft nicht auftreten. Andererseits erlaubte die Verwendung des Tools (wir benutzten einen nicht-kommerziellen Test-Account) die Demonstration widersinnig erscheinender, aber doch potenziell für Vorhersagen genutzter, Zusammenhänge wie „Menschen, die Converse liken, sind unterdurchschnittlich intelligent“ oder Gegenüberstellungen von Zusammenhängen wie „Dunkin Donuts → geringe Intelligenz“ und „Curly Fries → hohe Intelligenz“ (in beiden Fällen geht es um Junkfood). Die SuS (allesamt mit Converse-Schuhen an den Füßen) schauten sich zwar das Converse-Beispiel im Tool an, und es löste allgemeine Empörung aus. Dennoch insistierten sie auf der Frage nach dem kausalen Bezug und begegneten diesen – als durchaus bedrohlich empfundenen - Beobachtungen durch Abgrenzung: „Das ist doch Quatsch“ (und mithin nicht relevant).

Im Kurs versuchten wir, das Verständnis und die Glaubwürdigkeit der vorgestellten Probleme durch weitere Erläuterung des Konzepts „Korrelation“ sowie die Methodik wissenschaftlicher Publikationen („das wurde im Peer Review von anderen Experten überprüft und ist daher eben nicht Quatsch“) zu erhöhen. Beide Themen sind nicht Standard-Schulstoff. Die Bemühungen waren nur sehr eingeschränkt erfolgreich und führten, ähnlich wie die Beobachtungen bzgl. des Apriori-Algorithmus, wieder zur Frage, ob diese für das Verständnis heutiger Datenanalysemethoden grundlegenden Konzepte nicht stärker in den Fokus schulischer Lehrpläne rücken sollten.

Wir sind hier am zentralen Punkt der Reihe angelangt, auf dessen umfassendem Verständnis in allen Implikationen der gesamte Rest beruht: Institutionelle Privacy ist kaum aufrecht zu erhalten, wenn die Ergebnisse der Profilerstellung kausal nicht erklärbar sind. Ich kann auf Facebook nicht einmal Yoghurt Gums liken, ohne Gefahr zu laufen, als unintelligent, faul (cf. Conscientiousness), rückständig (Openness), wenig kooperativ, daher kaum teamfähig (Agreeableness) und labil (Stability) engestuft zu werden, denn ich habe nicht den geringsten

Anhaltspunkt für die Korrelationen von Yoghurt Gums.

Diese Unvorhersehbarkeit wird durch eine andere Fähigkeit des Preference Tools noch schwerwiegender: Das Tool erstellt auch ein Profil demographischer Eigenschaften: Aus den Likes (prozessual-dynamischen Eigenschaften) werden Geschlecht, Anzahl der Facebook-Freunde, Beziehungs-Status und Alter (statische Merkmale) vorhergesagt, und diese Profilbildung erwies sich bei allen Probe-Likes der SuS als korrekt.

Korrekte demographische Daten aber erhöhen die Identifizierbarkeit von Profilen, so dass das Versprechen der Facebook-Datennutzungspolicy „If the advertiser chooses to run the ad (...), 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" kaum noch beruhigen kann. Es besteht die realistische Chance, dass die demographischen Daten eines Nutzers mit seiner/ihrer echten Identität, aber nicht kausal vorhersagbaren (und überprüf- oder korrigierbaren!) Einschätzungen verknüpft werden.

Dieses Lernziel wurde auf kognitiver Ebene insgesamt (gemessen durch die Resultate der Semesterklausur) zufriedenstellend erreicht. Inwieweit es in einen Kompetenzzuwachs mündete, der den Schülern ermöglicht, erworbene kognitive Fähigkeiten in verschiedenen Situationen bewusst, sinnvoll und angemessen anzuwenden, muss offen bleiben, doch vorerst skeptisch beurteilt werden - s. dazu unten die in Abschnitt 5.4 dargestellte Sicht einer Schülerin.

5.3 Teil III: Demokratie – unser Grundrecht auf informationelle Selbstbestimmung und auf den Schutz dieser Rechte

Zunächst galt es, die Ergebnisse anzuwenden in ihren Implikationen für Privatsphäre, Demokratie und Grundrechte, in Relation zum Grundgesetz in seiner Funktion als Garant der freiheitlich demokratischen Grundordnung der Bundesrepublik Deutschland.

Zu diesem Zweck wurde in Stunde 7 das Volkszählungsgesetz und das Volkszählungsurteil des BverfG behandelt. In der Urteilsbegründung finden sich insb. folgende Sätze, die in unmittelbarem Zusammenhang zum bisherigen Reihenverlauf stehen: *„Sie [sc. die Daten] können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. […] 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.*"

Die Empörung über die Converse-Ergebnisse im Preference Tool wirkte sich hier natürlich vorteilhaft aus: Beispiele für das Zusammenfügen von Persönlichkeitsbildern, deren Richtigkeit die Betroffenen nicht kontrollieren können, mussten nicht erst mühsam aus bislang gelesenen Arbeitsblättern zusammengeklaubt werden. Schwieriger wurde die geforderte Zuordnung von „abweichenden Verhaltensweisen“ - nach dem bisherigen Reihenverlauf erforderte das folgende Kausalkette: Panoptismus führt zu Orientierung am Mainstream. Den Mainstream bestimmen a) die Schüler, z.B. durch Facebook-Likes und b) Schule, Uni und Arbeitgeber durch erwünschte Anforderungsprofile: high in consientiousness, high in openness, high IQ etc.. Wir haben also zwei Arten von Mainstream: den Massengeschmack und geforderte Schlüsselqualifikationen. Mainstream-konformes Liken auf Facebook kann zu desaströsen Ergebnissen bei den Schlüsselqualifikationen führen (cf. Dunkin Donuts), aber auch bestens mit diesen korrelieren (Curly Fries).

Damit funktioniert die vom BverfG „vorgeschlagene“ Lösung nicht mehr, unerwünschtes Abweichen durch Orientierung am Mainstream zu vermeiden. Das Recht auf Informationelle Selbstbestimmung, das aus dem allgemeinen Persönlichkeitsrecht resultiert, ist heute also in ganz anderem Ausmaß bedroht, als dies 1983 der Fall war.

Dieses Lernziel wurde durch fragend entwickelndes Unterrichtsgespräch erreicht.

Der Auszug aus der NJW 2000, 51 behandelt das zur Frage stehende NPD-Verbot aus Sicht des Meinungspluralismus, der als konstitutiv für das Gemeinwohl gesehen wird, und der erfordert, dass freie Meinungsäußerungen möglich sind und nicht z.B. unterbleiben, weil sie zu unabsehbaren Folgen für das Individuum führen können. (Weitere Details des Arguments s.u.) Insoweit die freie Äußerung einer Meinung durch Einsatz von Data Mining zu unabsehbaren Folgen für Individuen führt, kann Datamining zu einem Demokratieproblem werden. Die SuS gelangten also zu dem Schluss, dass eine so banale Form der Meinungsäußerung wie Facebook-Likes (bzw. die Folgen und Einschränkungen dieser Äußerungen) demokratiegefährdend sein könne und daraus zu der selbständig formulierten Fragestellung, wie Gesetzgeber und Verfassungsorgane sich gegenüber diesem Befund zu verhalten haben.

Hierzu ist das Lüth-Urteil zur Ausstrahlung der Grundrechte auch auf das Privatrecht maßgeblich. Der Text ist eine Zitatzusammenstellung aus Dreier [1993] und überforderte die SuS deutlich; es ist für die Zukunft zu überlegen, ob die Lehrperson ihn in eigener Paraphrase vorentlastet. Hier wurde abschnittsweise gelesen und anschließend erläutert, zwei Schülerinnen gelangten mit leichteren Hilfestellungen zu selbständigen Analysen, die wiederum der Rest des Kurses benötigte, so dass beide Schülerinnen als Expertinnen fungieren konnten. Steht man also vor der Wahl, wissenschaftlich anspruchsvolle Texte mit starken Eingriffen der Lehrperson bzw. leistungsstarker Schüler oder schülernahe Texten mit weitgehend selbständiger Erarbeitung im Unterricht zu lesen, kann die erste Alternative durchaus zu

besseren Ergebnissen führen.

Auch wenn durch diesen Abschnitt des Kurses deutlich geworden war, dass aktuelle Praktiken der Datensammelindustrie u.U. Grundrechte verletzen, so nahmen die SuS doch an, dass „man nichts tun könne", weil ja eben jeder Nutzer den Datenschutzbestimmungen der jeweiligen Firma zugestimmt hat. Die Privatautonomie war also als Konzept sehr präsent, auch wenn ihr hoher Rang in Rechtsstaaten wie der Bundesrepublik den SuS nicht explizit deutlich war (obwohl dieses aus dem Geschichtsunterricht bekannt sein sollte).

Das Rollenspiel, das eine Klage gegen Facebook et al. simulierte, dauerte deutlich länger als 90 Minuten; die Beteiligung wie auch das Niveau waren erfreulich hoch.[9] Insbesondere eine SuS-Gruppe beschrieb die Position des Bundesverfassungsgerichts im Lüth-Urteil (mittelbare Drittwirkung der Grundrechte) als geradezu entmündigend für das selbstbestimmte Individuum und vereinnahmte somit den Schutz des allgemeinen Persönlichkeitsrechts sehr wirkungsvoll für die unbedingte, von keiner mittelbaren Drittwirkung eingeschränkte Geltung der Privatrechtsautonomie. Hierdurch vollzog die Gruppe die Konfliktlinien aus Wassermann (2000)nach:

1.) Meinungspluralismus macht ein NPD-Verbot unmöglich. / Ein selbstbestimmtes Individuum mit uneingeschränkter Persönlichkeitsentfaltung muss ebenso uneingeschränkt vertragsfähig sein. 2.) Meinungspluralismus setzt Meinungsfreiheit als Prämisse; wer diese abschaffen will (wie die NPD, was Voraussetzung für ihr Verbot ist), kann sich nicht vorher auf sie berufen. / Die Vertragsfreiheit kann zur ernsthaften Beschädigung der Informationellen Selbstbestimmung führen. Beide folgen aus dem allgemeinen Persönlichkeitsrecht, das Vorrang hat. Ein informationell selbstbestimmtes Individuum kann nur unter einem Schutz vor bestimmten Verträgen existieren.

5.4 Ergebnisse: Kognitive Lernziele und Kompetenzzuwachs?

Den Abschluss der Reihe bildete die Klausur:Als Text[10] diente der Entwurf zur Europäischen Datenschutzverordnung von Jan Philipp Albrecht, der dank gezielter Lobby-Arbeit beständigen Verwässerungsversuchen ausgesetzt ist. Das Gesetzesvorhaben ist hervorragend geeignet, sämtliche Teilziele der Reihe zu rekapitulieren, damit diente die Klausur zur Evaluation der Erreichung sämtlicher Lernziele. Im Durchschnitt erreichten die 10 SuS 7,5 von 15 Punkten; der Median lag bei 7, mit beinah normalverteilten weiteren Noten zwischen 4 und 12 Punkten.

Inwieweit das erreichte Verständnis, wie umfassend auch immer, das Kommunikationsverhalten der SuS beeinflusst, lässt sich momentan nicht sagen. Im Folgenden nimmt eine Schülerin, die auch an dem Reihentwurf mitgearbeitet hat, dazu Stellung.

[9] Die „universitäre Ko-Autorin" des Beitrags, Bettina Berendt, die bei dieser Unterrichtsstunde dabeisein durfte, kann diese Einschätzung aus Lehrersicht vollständig unterschreiben!.

[10] Gekürzte Fassung aus http://www.zeit.de/2013/41/privatsphaere-internet-datenschutz

Eine Schüler/innensicht (Beitrag von Cihan Demir)

Wenn Herr Dettmar sagt, wir können auf Facebook nichts mehr liken, ohne unsere Zukunft gravierenden Risiken auszusetzen, orientiert er sich am Schule-/Uni-/Arbeitgeber-Mainstream. Das sind Erwachsenen-Kriterien, ich bin nicht erwachsen, habe andere Maßstäbe und Werte und fühle mich dadurch fremdbestimmt. Eltern und Lehrer planen mein Leben komplett durch, ständig dieser Job- und Bildungs-Opportunismus/Dünkel. Meine Privatsphäre ist mir keineswegs egal, doch wenn ich in Berlin Dunkin Donuts esse, will ich das an meine Freundin, von der ich genau weiß, dass sie das jetzt auch gern täte, posten können, ohne mir gleich Gedanken machen zu müssen, ob ich deswegen irgendwann in ferner Zukunft 1000 EUR weniger im Monat verdiene. Die Konsequenzen, die sich aus Datamining-getriebener Informationsgewinnung ergeben, sind mir zu abstrakt, um mein reales Leben und Handeln zu beeinflussen. Die ganze Reihe war sehr abstrakt, sie war sicher eine gute Uni-Vorbereitung, doch reale Konsequenzen hat sie für mich zumindest momentan nicht: ich nutze WhatsApp intensiv und werde das auch weiterhin tun.

Allerdings bleibt ein leises Unbehagen: wir waren auf einer Podiumsdiskussion mit Jan-Philipp Albrecht und einem Facebook-Anwalt, in deren Verlauf der Anwalt Facebooks privacy policy über die von WhatsApp stellte – einen Tag später stand in der Zeitung, dass Facebook WhatsApp übernimmt. Insb. der hohe Übernahme-Preis korreliert völlig mit den Lernzielen der Reihe – man müsste blind sein, das nicht zu sehen. Dass mit der Nutzung dieses Dienstes mein gesamtes Adressbuch auf Servern in den USA landet, ist mir keineswegs geheuer. Und selbstverständlich ist mir bewusst, dass mein Online-Verhalten z.T. purer Bequemlichkeit geschuldet ist und Datensparsamkeit nicht nur aus Sicht der institutionellen Privacy empfehlenswert ist.

Im Anschluss an diese Podiumsdiskussion und die WhatsApp-Übernahme befragte ich die anderen Kursteilnehmer (10 SuS), was sie von der Übernahme hielten: die Reaktion war bei allen gleich – sie ärgerten sich, dass WhatsApp einen Tag nicht erreichbar war, diesbezügliche Sprüche auf Facebook („Zuckerberg, du *****, mach WhatsApp wieder an“ u.ä.) fanden sie lustig, alle nutzen weiterhin WhatsApp und Facebook, Konsequenzen aus der Reihe im Umgang mit sozialen Netzwerken sind für mich nicht ersichtlich.

Entsprechendes gilt für den Zusammenhang Privatsphäre, freie Meinungsäußerung, Demokratie. Der in der Reihe vermittelte Zusammenhang erschließt sich mir, doch mit den Konsequenzen hapert es. Wenn meine Mutter in mein Zimmer durchsucht, schreie ich sofort: „Privatsphäre!“ Im Zusammenhang mit Demokratie interessiert sie mich jedoch nicht – er ist zu abstrakt, zu entfernt, zu unpersönlich, begreif- aber nicht erfassbar.

Allerdings merke ich immer häufiger nach dem Schreiben, dass ich mich plötzlich frage, ob es bei den von mir benutzten Wörtern Korrelationen gibt, und dass ich, wenn ja, nicht die leiseste Ahnung habe, wie diese aussehen könnten.

Im Zuge meiner Recherche zu einem Referat über Präimplantationsdiagnostik stieß ich auf das Blog eines Befürworters, Julian Savulescu.[11] Dort findet sich eine Debatte, ob es für von furchteinflößenden Diagnosen betroffene Eltern vertretbar ist, die Entscheidung pro oder contra Abtreibung via Internet-Abstimmung zu treffen. Der Aspekt Privatsphäre interessiert in der Diskussion auf diesem Blog wohlgemerkt niemanden.

Zusammenfassend würde ich sagen, meine Haltung schwankt zwischen indifferent, irritiert und entsetzt.

6 Fazit und Ausblick

Die hier vorgestellte Unterrichtsreihe bietet eine interdisziplinären Perspektive auf das komplexe Thema „Privatsphäre/Privacy und ihre Bedeutung“ und hilft den TeilnehmerInnen insbesondere, ein umfassendes Verständnis von Datensammlung und –verarbeitung durch soziale Netzwerke und andere kommerzielle Dienstanbieter wie z.B. Suchmaschinen zu entwickeln. Hierbei erwerben die SuS informatische Kenntnisse über Data Mining und seine Modelle und Algorithmen, sie arbeiten mit Tools und bekommen dadurch auch einen Einblick in einige Internet-Technologien. Die Folgen für die institutionelle Privacy (und nicht nur die soziale Privacy gegenüber anderen SchülerInnen, Eltern und potenziellen Arbeitgebern) sowie die hiervon ausstrahlenden Risiken für ein demokratisches Gemeinwesen werden deutlich. Es wird deutlich, dass es keine eindeutigen Antworten gibt, sondern dass verschiedene Interessenkonflikte vorliegen und individuell wie gesellschaftlich verhandelt werden müssen. Die SuS erwerben Kompetenzen, um sicherer und kritischer im Internet handeln zu können und als mündige BürgerInnen keinem defätistischen Technikdeterminismus anheim zu fallen.

Die Reihe lässt sich in unterschiedlicher Weise variieren und ausbauen. So können die informatischen Anteile vertieft und verbreitert werden, z.B. indem man die SuS selbsttätig Daten aus Web-APIs gewinnen lässt, indem man ihnen Visualisierungswerkzeuge zur Verfügung stellt, um diese Daten zu analysieren, oder indem man Data-Mining-Verfahren über Tools[12] ausprobieren oder auch selbst programmieren lässt. Hierbei sollten insbesondere mobile Technologien berücksichtigt werden, da die Internetnutzung über Mobiltelefone besonders bei SchülerInnen zunehmend an Bedeutung gewinnt (vgl z.B. die Unterrichtsreihe von Hinzmann, Hüttemann, Wittke und Schulte, 2014).

Andere Erweiterungsmöglichkeiten, gerade auch für den Einsatz im Informatikunterricht, setzen an der Frage der Handlungsorientierung an. Wir haben oben ein skeptisches Fazit hinsichtlich des Kompetenzzuwachses beim „privacy-verträglichen Kommunikationsverhalten“ gezogen. Wir

[11] http://juliansavulescu.typepad.com/blog/
[12] z.B. WEKA , *www.cs.waikato.ac.nz/ml/**weka**/*

haben hierbei v.a. an Datensparsamkeit gedacht (z.B. aufs „Liken“ verzichten). Im Laufe der Reihe und unserer Diskussionen über sie haben wir uns aber immer öfter gefragt, ob wir mit diesem Ansatz heutige SuS überhaupt noch erreichen können – ob sie nicht einfach in Hinsicht darauf, was sie (elektronisch) „teilen“ wollen, an einem anderen Punkt stehen als unsere Generation. In den Vordergrund rücken dann der Erwerb von Wissen und Kompetenzen über die Verschlüsselung von Kommunikation sowie über die Anonymisierung von Kommunikationen, die eine persönliche Identifikation nicht erfordern (z.B.die meisten Suchanfragen). Dieses Feld bietet eine Reihe kerninformatisch hochinteressanter Themen, aber auch praktische Kompetenzen bei der Toolverwendung und gesellschaftlich relevante Fragen.

Zur Vertiefung der Frage, was „der Gesetzgeber“ tue, um unsere Privacy zu schützen, bietet sich eine Ergänzung um Grundzüge des deutschen und europäischen Datenschutzrechts an, das maßgeblich vom Volkszählungsurteil 1983 und den anschließenden Diskussionen um Informationelle Selbstbestimmung geprägt wurde. Einen Kurzüberblick für Studierende, der mit entsprechenden Anpassungen auch für SchülerInnen verwendbar sein sollte, gibt der Foliensatz von Berendt (2012). Dieser betont u.a., dass es hier nicht nur um Rechte geht, sondern auch um Pflichten: Grundkenntnisse im Datenschutzrecht sind für die SuS nicht nur „als BürgerInnen“ relevant, sondern auch hinsichtlich beruflicher Verantwortlichkeiten, die (nicht nur) InformatikerInnen übernehmen müssen, die mit den persönlichen Daten anderer Menschen umgehen. In diesem Zusammenhang können auch ausgewählte Texte zu kürzlichen oder aktuellen Rechtsstreits gelesen werden, in denen insbesondere die Datenschutzrichtlinien von Facebook und Google von privaten oder öffentlichen Datenschützern als unvereinbar mit dem Datenschutzrecht bezeichnet werden. Gute Beispiele sind die Aktivitäten von Europe vs. Facebook, dokumentiert auf http://www.europe-v-facebook.org; die erfolgreichen Klagen europäischer Daten- und Verbraucherschutzverbände wie z.B. der Verbraucherzentrale Bundesverband, dokumentiert auf www.surfer-haben-rechte.de oder der französischen Datenschutzbehörde CNIL gegen Google[13], sowie Beiträge aus dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, gesammelt auf https://www.datenschutzzentrum.de/facebook). Des Weiteren kann die aktuelle Diskussion, ob das primär in Vor-Internet-Zeiten entwickelte Datenschutzrecht unter Data Mining / „Big Data“ noch greift und wie es verändert werden könnte/sollte, aufgegriffen werden. Hierzu können politikberatende Texte (z.B. Article 29 Working Party, 2013) ebenso wie populärwissenschaftliche Bücher (z.B. Mayer-Schönberger & Cukier, 2013) als Materialquelle herangezogen werden.

[13] z.B. http://www.cnil.fr/english/news-and-events/news/article/google-failure-to-comply-before-deadline-set-in-the-enforcement-notice/

Schließlich bieten die seit den Snowden-Enthüllungen seit 2013 (wieder) eröffneten Diskussionen zur Datensammlung und –verarbeitung und damit Überwachung durch den Staat weitere aktuelle Fragen zu den Zusammenhängen zwischen Privacy, Grundrechten und Demokratie.

7. Literatur:

a. In der Unterrichtsreihe verwendete Literatur (Zusammenstellung inclusive weiterer Arbeitsblätter auf http://www.schul-web.org/geschichte/kiwi/pgw.html), in der Reihenfolge ihrer Verwendung:

[NDR, 2010] *Datenschutz und Datenverschwendung – NDR Extra 3 vom 07.03.2010.* http://www.youtube.com/watch?v=S06u4ugb0xc (21. März 2014).

PEETZ, T. & BERENDT, B. (2012). A TRACKER MANUAL FOR HIGH SCHOOL TEACHERS. TECHNICAL REPORT, KU LEUVEN. http://people.cs.kuleuven.be/bettina.berendt/SPION/TrackerManual.pdf (21. März 2014).

GRAFF, B. (2010A). MAN ERKENNT UNS, WEIL WIR LEBEN, SÜDDEUTSCHE ZEITUNG, 25.01.2010, http://www.sueddeutsche.de/computer/912/501171/text/ (21. März 2014).

GRAFF, B. (2010B). DER GLÄSERNE BÜRGER 2.0 –DAS NEUE PROFIL DES MENSCHEN, SÜDDEUTSCHE ZEITUNG NR 126, 05./06.06.2010.

[FACEBOOK, 2013FF.] FACEBOOK. DATA USE POLICY. https://www.facebook.com/full_data_use_policy (DIESE POLICY WIRD KONTINUIERLICH ANGEPASST. IN DER BESCHRIEBENEN DURCHFÜHRUNG DER REIHE HABEN WIR MIT DER VERSION VOM 12.05.2012, DER IM SEPT. 2013 AKTUELLEN FASSUNG, GEARBEITET; ES EMPFIEHLT SICH, DIE JEWEILS AKTUELLE ZU VERWENDEN.]

DETTMAR, G. (2002). 3. ECOMMERCE. AUS: DERS., 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/ (21. März 2014).

ANDREWS, L. (2012). AUSWERTUNG PERSÖNLICHER INFORMATIONEN: WIE DIE DATENSAMMEL-INDUSTRIE HINTER FACEBOOK UND CO. FUNKTIONIERT. IN: SZ 20.02.2012, http://www.sueddeutsche.de/digital/auswertung-persoenlicher-informationen-wie-die-datensammel-industrie-hinter-facebook-und-co-funktioniert-1.1280573-2 (20. Dezember 2014).

DREIER, H. (1993). DIMENSIONEN DER GRUNDRECHTE. VON DER WERTORDNUNGSJUDIKATUR ZU DEN OBJEKTIV-RECHTLICHEN GRUNDRECHTSGEHALTEN, HANNOVER.

KOSINSKI, M., STILLWELL, D., & GRAEPEL, T. (2013). PRIVATE TRAITS AND ATTRIBUTES ARE PREDICTABLE FROM DIGITAL RECORDS OF HUMAN BEHAVIOR. PROCEEDINGS OF THE NATIONAL ACADEMY OF SCIENCES, 110 (15), 5802–5805.

WASSERMANN, R. (2000). AKTIVIERUNG DER WEHRHAFTEN DEMOKRATIE – ZUM ANTRAG AUF NPD-VERBOT, IN: NEUE JURISTISCHE WOCHENSCHRIFT, HEFT 51, S. 3760-62.

B. Weitere zitierte Literatur

ARTICLE 29 DATA PROTECTION WORKING PARTY (2013). OPINION 03/2013 ON PURPOSE LIMITATION. 00569/13/EN WP 203. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (21. März 2014).

BERENDT, B. (2012). DATENSCHUTZBEWUSSTSEIN (FOLIENSATZ). http://people.cs.kuleuven.be/~bettina.berendt/Talks/berendt_2012_datenschutzbewusstsein.ppt (21. März 2014).

COUNCIL OF EUROPE (2010). RECOMMENDATION CM/REC(2010)13 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA IN THE CONTEXT OF PROFILING. https://wcd.coe.int/ViewDoc.jsp?id=1710949 (21. März 2014).

HINZMANN, P., HÜTTEMANN, V., WITTKE, T. & SCHULTE, C. (2014). MOBILFUNKNETZ - WAS STECKT DAHINTER? WORKSHOP AUF DER TAGUNG DER GI-FIBBB, POTSDAM, 6.3.2014. http://www.informatikdidaktik.de/Fachgruppe/tagung13/ws2_2014 (21. März 2014).

KLICKSAFE (2013). DATENSCHUTZ TIPPS FÜR JUGENDLICHE. http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Jugendliche/klicksafe_Flyer_Datenschutztipps_Jugend_2013.pdf (21. März 2014).

MAYER-SCHÖNBERGER, V. & CUKIER, K. (2013). BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK AND THINK. LONDON: JOHN MURRAY.