Jens Gallenbacher (Hrsg.): INFOS 2015 – Informatik allgemeinbildend begreifen
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 33

Datenschutz im 21. Jahrhundert – Ist Schutz der Privatsphäre (noch) möglich?

Bettina Berendt[1], Gebhard Dettmar[2], Bernhard Esslinger[3], Andreas Gramm[4], Andreas Grillenberger[5], Alexander Hug[6] und Helmut Witten[7]

Abstract: Die Bedrohung der Privatsphäre hat im 21. Jahrhundert im Wesentlichen zwei Dimensionen: zum einen die Datensammelindustrie (Facebook, Google & Co.) zusammen mit der „freiwilligen" Veröffentlichung personenbezogener Daten der Internet-Nutzer, zum anderen die anlasslose Massenüberwachung durch die Geheimdienste. Im Workshop sollen unterschiedliche Ansätze zur Behandlung des Privacy-Diskurses im Unterricht der Sekundarstufen I und II zur Diskussion gestellt werden. Besondere Aktualität hat das Thema durch die z. Zt. wieder von interessierten politischen Akteuren geforderte Möglichkeit gewonnen, auch verschlüsselte Informationen mitlesen zu können (Crypto Wars 2.0 bzw. 3.0). Auf der anderen Seite gibt es z. B. den Versuch, durch Massenklagen Facebook zu zwingen, sich an die europäischen Normen des Datenschutzes zu halten.

Keywords: Datenschutz, Privacy bzw. Privatsphäre, Datensammelindustrie, Ausspähung durch Geheimdienste, informatische Bildung, fächerübergreifender Unterricht

1 Einleitung

Es steht schlecht um den Datenschutz in Deutschland. Jochen Koubek[8] fasst die Situation folgendermaßen zusammen:

> Es gibt ein historisch gewachsenes und sowohl durch Rechtsnormen ausformuliertes als auch durch die Urteilspraxis ausgeformtes Persönlichkeitsrecht, das insbesondere den Umgang mit personenbezogenen Daten umfasst. Wir haben Firmen, denen dieses Recht gleichgültig ist, weil sie in ihrer Selbstwahrnehmung gar nicht im deutschen Rechtsraum operieren. Wir haben eine Regierung, der dieses Recht gleichgültig ist, wenn es um die Wahrung ihrer

[1] KU Leuven, Department of Computer Science, Celestijnenlaan 200A, 3001 Heverlee, Belgien, bberendt@gmx.net
[2] BSB Hamburg, B 52-4, Moorkamp 7-9, 20357 Hamburg, g.dettmar@web.de
[3] Universität Siegen, IT-Sicherheit und Kryptologie, bernhard.esslinger@uni-siegen.de
[4] Gymnasium Tiergarten, Altonaer Straße 26, 10555 Berlin, gramm@gymnasium-tiergarten.de
[5] Friedrich-Alexander-Universität Erlangen-Nürnberg, Didaktik der Informatik, Martensstr. 3, 91058 Erlangen andreas.grillenberger@fau.de
[6] Universität Koblenz-Landau, Fachbereich Informatik, Universitätsstraße 1, 56070 Koblenz, hug@uni-koblenz.de
[7] GI-Fachgruppe IBBB (Informatik-Bildung in Berlin und Brandenburg),Brandenburgische Str.23, 10707 Berlin, helmut@witten-berlin.de
[8] (Ko14), s. a. Vortrag „Datenschutz und Persönlichkeitsrechte" vom 23.9.2014: http://medienwissenschaft.uni-bayreuth.de/assets/Uploads/Koubek/forschung/KoubekDatenschutzPersoenlichkeitsrechtePreprint.pdf.

> eigenen Interessen geht. Und wir haben Bürger, denen dieses Recht ebenfalls gleichgültig ist, wenn es mit Einschränkungen der persönlichen, digitalen Lebensgestaltung einhergeht oder wenn zu einer Durchsetzung politische Aktivierung erforderlich wäre.

Im Volkszählungsurteil von 1983 hat das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht (ein Grundrecht, das sich aus Art. 1, Absatz 1 GG in Verbindung mit der freien Entfaltung der Persönlichkeit aus Art. 2 ergibt) das Recht auf ***informationelle Selbstbestimmung*** abgeleitet (s. z. B. [Ko14]).

Wir stellen im folgenden drei Unterrichtsreihen vor, die informatische mit politischer Bildung auf eine Weise kombinieren, die es Schülerinnen und Schülern ermöglicht, die Auswertungsmechanismen der Datensammelindustrie nachzuvollziehen und die daraus resultierenden Konsequenzen für sie als Grundrechtssubjekte zu erkennen, um daraus mögliche Handlungskonzepte und -strategien zu entwickeln.

Dazu ist es erforderlich, den Lernenden zu vermitteln, warum die unbegrenzte Weitergabe persönlicher Daten überhaupt ein Problem darstellt und wie man sich mit den heute zur Verfügung stehenden Mitteln schützen kann. Mit welchen Argumenten man den bekannten Einwände „Ich habe doch nichts zu verbergen“ etc. begegnen kann, behandeln wir im folgenden Abschnitt.

2 Erfahrungen

Das Thema Datenschutz in all seinen Facetten ist ein Unterrichtsthema, das ein fester Bestandteil im Informatikcurriculum ist. Im Folgenden werden einige gelungene Reihen zu diesem Thema kurz vorgestellt.

2.1 Spuren im Internet – Das „Planspiel Datenschutz 2.0 – Wer weiß was über dich im Internet“

Schon Ende der 80er, Anfang der 90er Jahre gab es die ersten Vorläufer des kontextorientierten Unterrichtsprojekts „Planspiel Datenschutz 2.0“ [IniK], einem Rollenspiel, in dem es darum geht, Themen und Zusammenhänge des Datenschutzes zu erarbeiten. Ausgangspunkt des Rollenspiels ist die Aussage „Ich habe nichts zu verbergen!“, um dann am Ende des Spiels die Schüler zu überzeugen, dass aus ihren Informationen leicht falsche Rückschlüsse u. Ä. gezogen werden können.

Während die ursprüngliche Version eine Fassung ist, die mit Papier und Bleistift arbeitet, so ist die Version 2.0 eine von Frank Oppermann und Alexander Dietz weiterentwickelte Datenbank-gestützte Alternative. Nachdem die Schüler in einer ersten Phase des Spiels auf Basis einer ihnen zugewiesenen Rollenbeschreibung Handlungen im Netz durchgeführt haben, die wiederum von einem „fiktiven“ Provider, den der Lehrer zuvor eingerichtet hat, protokolliert werden, wechseln die Lernenden in der zweiten Spielphase die Rolle und ermitteln das Verhalten eines anderen Mitspielers. Dabei erstellen sie ein

Profil aus den protokollierten Daten des Providers, um z. B. eine möglicherweise begangene Straftat aufzuklären. In der folgenden Vertiefungs- und Vernetzungsphase werden im Rahmen einer Gruppenarbeit Themen wie „informationelle Selbstbestimmung“, „Cybermobbing“, „Datenschutzgesetz“, … behandelt.

Einer der Autoren hat im Rahmen der fachdidaktischen Ausbildung mit den Studierenden das Planspiel in einem GK Informatik der Stufe 11 an einem Gymnasium im Februar 2015 durchgeführt, wobei jeweils einer der Studierenden die Lehrerrolle innehatte. Am Ende der Reihe wurden die Schüler gefragt, inwiefern sie aufgrund des neu erworbenen Wissens und der neuen Erkenntnisse ihr Verhalten ändern werden. Auch wenn vereinzelte Schüler kritische Anmerkungen machten und nach der Stunde weitergehende Fragen z. B. nach Tools stellten, zeigte die Mehrheit doch ein Verhalten, wie es schon in [Be14b] beobachtet wurde: Da sie ja noch jung seien, über kein Girokonto verfügen und keine Terroristen seien, hätten sie nichts zu verbergen; weder ihr Verhalten würden sie ändern noch irgendwelche Werkzeuge (Browser-Plug-Ins, kryptographische Hilfsmittel, …) nun nutzen.

2.2 „E-Mail (nur?) für Dich“ revisited: Sicher chatten statt mailen mit PGP?

Mit der Unterrichtsreihe „E-Mail (nur?) für Dich“[9] schlagen [GHW11] vor, Möglichkeiten des Kompromittierens unverschlüsselten E-Mail-Verkehrs in einer geschützten Umgebung im Unterricht erlebbar zu machen und so die Erarbeitung verschiedener kryptographischer Verfahren von Caesar bis zu RSA zu motivieren, um am Ende E-Mails ganz praktisch mit PGP (bzw. enigmail) zu verschlüsseln und zu signieren.

Einer der Hauptkritikpunkte an der Unterrichtsreihe ist, dass viele Jugendliche zwar E-Mail-Benutzerkonten haben, diese aber kaum noch für ihre eigentliche Kommunikation mit Freunden nutzen. Hinweise auf mögliche spätere Mailnutzung im beruflichen Umfeld und der Gefahr der Industriespionage werden zwar akzeptiert, aber als „weit weg“ vom persönlichen Leben empfunden. Darüber hinaus werden z. B. die Risiken des „Web of Trust“ als Infrastrukturelement von PGP kritisch diskutiert[10].

Wir schlagen daher vor, Möglichkeiten einer vertraulichen und verlässlichen Kommunikation zu thematisieren, die der tatsächlichen Kommunikation von Jugendlichen so nahe kommen, dass sie sie als ernsthafte Alternative zu bisher genutzten Angeboten erkennen. Hier haben sich verschiedene Anbieter wie etwa *TextSecure*, *Cryptocat*, *Silent Text* oder *Threema* etabliert. Die *Electronic Frontier Foundation (EFF)* hat eine Liste solcher Kommunikations-Anwendungen erstellt[11], in der sie diese hinsichtlich verschiedener Kriterien wie Ende-zu-Ende-Verschlüsselung, Authentifikation von Kommunikations-

[9] http://informatik-im-kontext.de/index.php/entwuerfe/email-nur-fuer-dich/
[10] vgl. z. B. Padmos, Arne: Why is GPG "damn near unusable"? [31c3]: https://www.youtube.com/watch?v=4gz9TBt-DAQ
[11] https://www.eff.org/secure-messaging-scorecard

partnern oder der Nachvollziehbarkeit des Quellcodes untersucht. Für den Unterricht bietet sich vor allem das *Off-the-Record (OTR) Messaging*[12] an, das auf dem auch als *Jabber* bekannt gewordenen *Extensible Messaging and Presence Protocol (XMPP)* aufsetzt und von verschiedenen Client-Anwendungen unterstützt wird[13].

Im Bereich von Desktop-Anwendungen ist *Pidgin*[14] ein weit verbreiteter Client. Der SPIEGEL hat eine schrittweise Anleitung zum verschlüsselten Chatten mit OTR/XMPP mit Pidgin veröffentlicht[15]. Damit Chatten mit OTR aber zu einer tatsächlichen Alternative zu WhatsApp & Co. wird, sollten mobile Implementierungen im Unterricht vorgestellt werden, wie z. B. *Xabber*[16] für Android-Smartphones. Den Netzwerkverkehr eines Smartphones zu verfolgen ist etwas aufwendiger als auf einem PC. Zwar gibt es entsprechende Apps, wie z. B. das *Wireshark*-Pendant *Shark for Root*[17], doch erfordern diese Apps meist Root-Rechte und sind deutlich weniger intuitiv zu bedienen als entsprechende Versionen für einen PC. Bis hier einfach zu bedienende Anwendungen zur Verfügung stehen, schlagen wir vor, die Grundlagen der Verschlüsselung und Authentifizierung von Kommunikationsteilnehmern mit E-Mail zu erarbeiten, um dann aufzuzeigen, welche Möglichkeiten es gibt, diese Anforderungen auch für einen Chat mit Instant Messaging Apps auf mobilen Endgeräten zu erfüllen.

2.3 Zur Bedeutung der Privatsphäre in Zeiten der Datensammelindustrie

Diese in [Be14b] genauer beschriebene Unterrichtsreihe behandelt fächerübergreifend die Auswirkungen des Trackings im Internet und der Datenauswertung der Datensammelindustrie, Facebook, Google & Co. auf eine staatliche Ordnung, die das Recht auf freie Persönlichkeitsentfaltung in das Zentrum ihrer Wertordnung stellt[18].

Die Reihe befasst sich explizit *nicht* mit dem, was im Vordergrund vieler Unterrichtsempfehlungen zur „Kompetenz in sozialen Netzwerken und im Internet“ steht [z. B. Kl13]: Welche Fotos stellt man online, wie viel postet man und an welchen Em-

[12] https://otr.cypherpunks.ca

[13] Die Eigenschaften von OTR wurden kürzlich gut nachvollziehbar beschrieben in Lautebach, Urs: „Neee, das hab ich nie gesagt! Das Chatprotokoll Off-the-Record (OTR)“ in LOG IN Heft 181 (2015), im Druck

[14] https://pidgin.im

[15] http://www.spiegel.de/netzwelt/netzpolitik/mit-jabber-pidgin-und-otr-so-chatten-sie-verschluesselt-a-912957.html (29. April 2015) Als Jabber-Server sollte man jabber.de verwenden, nicht den jabber-Server vom CCC, der im Spiegel-Artikel empfohlen wurde und danach so überlastet war, dass seitdem keine Neuanmeldungen mehr entgegen genommen werden.

[16] http://www.xabber.org

[17] https://play.google.com/store/apps/details?id=lv.n3o.shark

[18] Materialien und weitere Links finden sich auf http://people.cs.kuleuven.be/~bettina.berendt/Privacybildung/ (29. April 2015). Zu Erweiterungen von Literaturbasis und curricularen Vorschlägen s. [Be14a]. Eine interessante Alternative sind die von verschiedenen öffentlich-rechtlichen Fernsehsendern (u. a. Arte) erarbeiteten interaktiven Selbstlernmaterialien zum Themenkomplex „Tracking“´: https://donottrack-doc.com/de/. Eine Zusammenfassung der Hauptaussagen dieser Materialien findet sich in dem Film http://www.ardmediathek.de/tv/Do-Not-Track/Do-Not-Track-Internet-Tracking-das-/Bayerisches-Fernsehen/Video?documentId=29004966&bcastId=29004948

pfängerkreis? So berechtigt diese Fragen und so wichtig diese Kompetenzen auch sind: Es geht nicht nur um die Entscheidungen des Einzelnen, wie viel er oder sie durch bewusste und rational fundierte Entscheidungen von sich „preisgibt". Vielmehr geht es darum, zu zeigen, dass eine bewusste Datensparsamkeit zwar nützlich sein kann (z. B. kann man sich entscheiden, nichts zu „liken", Anonymisierungsdienste zur Reduktion des Trackings nutzen, oder seine Kommunikation verschlüsseln), dass dies aber nur punktuell wirkt. Wenn die Nicht-Nutzung sämtlicher Kommunikations- und Informationsmedien *keine* Option ist, dann kann der *Einzelne* nur begrenzt effektiv handeln. In einer vernetzten digitalen Welt müssen Grundrechte auch gesetzlich effektiv geschützt werden. Aber Bürger müssen dies auch einfordern, und dazu müssen sie sich sowohl der Realitäten von Datensammlung und -nutzung als auch ihrer Rechte bewusst sein. Dieses Bewusstmachen durch entsprechende Wissensvermittlung ist unser Ziel.

Zunächst wird in der Reihe mit der Hilfe eines Browser-Plugins visualisiert, wie „Tracker" (z. B. Cookies) ohne unser Zutun und seitenübergreifend aufzeichnen, was wir tun, auch wenn wir „einfach nur" im Netz unterwegs sind, selbst ohne überhaupt etwas zu posten. Anschließend wird erklärt, wie mit Hilfe von Data Mining aus solchen Verhaltensdaten, ggf. kombiniert mit Transaktions- und anderen Daten, Zusammenhänge und Vorhersagen abgeleitet werden. Ein (echtes) Beispiel ist die von einem Kreditkartenunternehmen gefundene Korrelation, dass Menschen, die in Gitarrengeschäften einkaufen, weniger kreditwürdig sind. Ein weiteres (ebenfalls echtes) Beispiel ist die Vorhersage von Persönlichkeitseigenschaften aus Facebook-Likes: Wer Converse-Schuhe „liket", der gilt als dumm.

Diese Zusammenhänge sind rein korrelativ. Damit entfällt die Grundannahme der in anderen Unterrichtsplänen und Materialien zum Thema „Privatsphäre" so gern genannten Verhaltensregeln, die von (zumindest sozial) kausalen Zusammenhängen ausgehen: *Weil* jemand, der viel trinkt, wahrscheinlich kein zuverlässiger Arbeitnehmer ist, wird er schlechter einen Job bekommen. *Daher* ist es sinnvoll, keine Partyfotos für die Öffentlichkeit zu posten; bzw. wenn man das *nicht* tut, dann erscheint man auch als zuverlässig. In einer Welt, in der man aufgrund intransparenter Korrelationen (statt aufgrund bekannter und erlernbarer sozialer „kausaler" Regeln) als guter oder schlechter Kunde oder Arbeitnehmer (etc.) erscheint, gibt es aber keine Möglichkeit mehr, sich richtig oder falsch zu verhalten.

Anhand von Assoziationsregeln und einem Basisverfahren zum Lernen solcher Regeln wird in der Reihe dann die algorithmische Basis der Schlussfolgerungen im Data Mining illustriert[19]. Warum solche Schlussfolgerungen getroffen werden und warum sie problematisch sind, wird im Rollenspiel zwischen Nutzern mit Interesse an Umsonst-Diensten versus Unternehmen mit Interesse an vermarktbaren Daten erarbeitet. Hierbei werden Daten nicht nur für personalisierte Werbung vermarktet, sondern auch z. B. zur

[19] Grillenberger und Romeike [Gr15] merken zu Recht an, dass man bei der Darstellung und Erarbeitung von „Big-Data-Analyseverfahren" wie Assoziationsregeln und Clustering mit geeigneten Tools arbeiten sollte, die diese Algorithmen gut nachvollziehbar machen, und stellen hierfür gute Beispiele (Snap!) zur Verfügung.

Kundensegmentierung von Kreditkartenunternehmen oder Vorauswahl in Bewerbungsverfahren. Aus Datenanalysen kann somit soziale Ausgrenzung entstehen.

Wenn aber für den Bürger intransparent ist, wie er sich „richtig" verhalten kann, um nicht als Kreditrisiko, unzuverlässiger oder dummer Arbeitnehmer etc. zu gelten, dann besteht die Gefahr, dass er gar nichts mehr sagt und tut und auch sonstige demokratische Rechte nicht mehr wahrnimmt. (Eine detaillierte Analyse solcher „Chilling-Effekte" findet sich in [So11].) Mit anderen Worten: wenn man nicht weiß, was wer wie mit den eigenen persönlichen Daten tut, sind Meinungsfreiheit und freie Persönlichkeitsentfaltung in Gefahr. Genau dies (dass Bürger also das Recht haben müssen, Daten in Kenntnis der Auswertungsmethoden und ihrer Resultate übermitteln zu können) ist die Argumentation des Bundesverfassungsgerichts in seiner Herleitung des Rechts auf informationelle Selbstbestimmung. Dieses Recht und seine Begründung wie auch der Anspruch des Bürgers auf den Schutz der Grundrechte werden im letzten Teil der Reihe hergeleitet, und es wird in einem abschließenden Rollenspiel auch erarbeitet, warum es keine einfachen Lösungen gibt: Das Recht auf informationelle Selbstbestimmung und der Anspruch auf den Schutz dieses Rechts (z. B. durch Datenschutzgesetze und deren Durchsetzung) kann durchaus im Konflikt mit anderen Grundrechten wie der Vertragsfreiheit stehen. Denn hat der Nutzer nicht „freiwillig" seine Daten gegeben, um den „kostenlosen" Dienst zu bekommen (den der Anbieter natürlich anderweitig finanzieren muss)? Eben diese Frage ist im sog. Lüth-Urteil vom BverfG allerdings beantwortet – in den Worten Dreiers:

> „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." [Dr93, S. 47]

Aus diesem Urteil ergab sich für die Grundrechte a) ihre „Ausstrahlungswirkung": Jedes Gesetz, jede Rechtsnorm muss in ihrem Geist abgefasst sein, und b) die „mittelbare Drittwirkung: die Grundrechte wirken nicht unmittelbar zwischen den Grundrechtssubkjekten, also den Bürgern, doch ist ihre Geltung bei der Anwendung des Privatrechts zu beachten, mit anderen Worten: Grundrechte stehen über privatrechtlichen Vereinbarungen. Damit werden aus Grundrechten Grundnormen, die über dem positiven Recht stehen, welches sich aus ihnen ableitet. Freie Persönlichkeitsentfaltung und Meinungsfreiheit sind dabei von so entscheidender Bedeutung, dass privatrechtliche Vereinbarungen, die auf ihre Aushöhlung hinauslaufen, der freiheitlich-demokratischen Grundordnung widersprechen und als verfassungsfeindlich einzustufen sind.[20]

[20] Ähnlich argumentiert der lesenswerte Artikel des prominenten Datenschützers Thilo Weichert am Beispiel Facebook: „Datenschutzverstoß als Geschäftsmodell – der Fall Facebook", s.: https://www.datenschutzzentrum.de/facebook/20120921-facebook-geschaeftsmodell.pdf

3 Neue Unterrichtsideen zur Stärkung der informationellen Selbstbestimmung

Nachdem im vorangegangenen Abschnitt schon fertig ausgearbeitete Unterrichtsreihen vorgestellt wurden, zu denen auch Erfahrungsberichte aus dem Unterricht vorliegen , werden nun erste Ansätze und Ideen präsentiert, die sich noch in der Entwicklung befinden. Hierbei geht es auch darum, die in Abschnitt 2 vorgestellten Projekte mit den neuen Ideen zu verbinden, da jedes für sich bestimmte Fragen offen lässt.

3.1 Erste Überlegungen aus der Königsteiner Arbeitsgruppe

In der Arbeitsgruppe „Datenschutz im 21. Jahrhundert“ der 22. Fachdidaktischen Gespräche[21] zur Informatik in Königstein (Sachsen) vom 25.03. bis 27.03.2015 haben wir Erfahrungen in der Vermittlung dieses Themas zusammen getragen. Dabei haben wir uns gefragt, welche Themen und Oberbegriffe im Zusammenhang mit „Privacy und Datenschutz“ stehen, welche davon im Rahmen einer Unterrichtsreihe behandelt werden und welche möglichen Vernetzungen untereinander herausgestellt werden sollten. Darüber hinaus wurden frei zugängliche Materialien auf ihre Eignung für eine solche Unterrichtsreihe hin untersucht.

Zur Themensammlung und einer möglichen Strukturierung wurde eine Mind Map[22] erstellt, die einen guten Überblick über das gesamte Gebiet gibt. Als Projekttitel wurde „Meine Privatsphäre“ gewählt, weil dadurch zum einen der persönliche Bezug zur Sache („meine“) und zum anderen der gesellschaftswissenschaftliche Schwerpunkt der Unterrichtsreihe betont werden kann. Ziel ist die Erstellung einer oder mehrerer kontextorientierter Unterrichtsreihe(n) [IniK], die modular aufgebaut sein sollen, sodass die Lehrkraft je nach Altersstufe (Sek. I oder Sek. II) und Vorkenntnissen eine auf die Lerngruppe zugeschnittene Unterrichtssequenz zusammenstellen kann.

Einstiege in eine solche Reihe bieten sich aus drei Themenfeldern an: a) Kommunikationsmittel, b) gesellschaftlicher Diskurs, und c) informationelle Selbstbestimmung als zugrundeliegendes Prinzip. Ein Beispiel zu a) skizzieren wir im folgenden Abschnitt.

Darüber hinaus ist eine Sensibilisierung für das Thema „Meine Privatsphäre“ auch durch kurze Filme (z. B. „Wir lieben Überwachung“[23]) oder kritische Jugendbücher (z. B. „Little Brother“ von Cory Doctorow[24]) möglich. Im letzten Fall bietet sich zudem ein fächerverbindender Unterricht mit den Fächern Deutsch und/oder Ethik an.

---

[21] http://dil.inf.tu-dresden.de/Koenigsteiner-Gespraeche.262.0.html
In der Arbeitsgruppe haben mitgearbeitet: Rita Freudenberg, Andreas Grillenberger, Marc Hannappel, Alexander Hug, Peter Juknat, Holger Rohland, Michael Unger, Helmut Witten.

[22] http://bscw.schule.de/pub/bscw.cgi/d1205723/Meine%20Privatsph%C3%A4re.pdf

[23] https://www.youtube.com/watch?v=qGvZveB1osw und auch http://alexanderlehmann.net/

[24] http://de.wikipedia.org/wiki/Little_Brother_%28Roman%29

3.2 Ein möglicher Weg durch einen Einstieg über Messenger-Dienste

Der Einstieg in die Unterrichtsreihe „meine Privatsphäre“ könnte dadurch erfolgen, dass man mit den Schülern über die von ihnen genutzten Messenger-Diensten diskutiert. Dazu bieten sich folgende Leitfragen an: Welche Dienste nutzt Du? Wozu nutzt Du die jeweiligen Dienste konkret? Wie häufig ist dies am Tag? Welche Vorteile bieten Dir die Messenger-Dienste gegenüber anderen Kommunikationsmöglichkeiten? Es bietet sich je nach Kursgröße an, erste Diskussionen in Kleingruppen zu beginnen und anschließend ins Plenum zu wechseln, um alle Lernenden besser einbeziehen zu können und eine Vielzahl von Antworten zu erhalten. Damit diese Betrachtung nicht nur auf einer theoretischen Ebene verbleibt und geeignete Dienste auch genutzt werden, kann sich die Lerngruppe an dieser Stelle für ihre weitere Kommunikation auf einen Dienst einigen.

Im nächsten Schritt kann man unter Zuhilfenahme von Materialien (Artikel, Berichte auf Webseiten, …) einerseits die unverschlüsselte Kommunikation[25] und andererseits die Zusammenhänge diverser Dienste wie Facebook, WhatsApp, usw. herausstellen[26]. Aufgrund dieser Kenntnis muss den Schülern einsichtig werden, dass durch die Nutzung all dieser Dienste ein Datenschatten bzw. ein zweites „Ich“ von ihnen in der digitalen Welt existiert, dass dem zweiten „Ich“ Eigenschaften zugeordnet werden, die nicht gültig sein müssen, und dass das „Recht auf Vergessen“ in der digitalen Welt nicht automatisch existiert. In dieser Unterrichtsphase bietet sich an, analog der Beschreibung in [Be14b] im praktischen Teil Tracker einzusetzen.

Die Lernenden werden mit der Antwort „Ich habe nichts zu verbergen!“ argumentieren, was dann zur Diskussion über die Frage „Was ist Privatsphäre? Und wo sind die Grenzen zur Öffentlichkeit?“ überleitet. Wie in [Be14b] beschrieben, ist hier der Unterschied zwischen der institutionellen und der sozialen Privacy herauszuarbeiten.

An diesem Punkt der Reihe wird man sicherlich Schüler finden, die dem Gebrauch z. B. von Facebook kritisch oder gar ablehnend gegenüberstehen, und andererseits Schüler in der Lerngruppe haben, die ein System wie Facebook begrüßen. Daher bietet es sich an, Argumente und Gründe für oder gegen eine Nutzung von Facebook zu sammeln, wobei hier der Standpunkt, aus dem man argumentiert, eine entscheidende Rolle spielt. Als Fazit könnte sich schließlich eine Aussage wie „If you‘re not paying for it, you are the product” stehen.

Der Nutzung der Daten hat man durch Kenntnisnahme der AGB bestätigt (s. aber oben, Abschnitt 2.3: „Lüth-Urteil“). Somit steht nun die Analyse solcher Bedingungen an, wobei gruppendifferenziert verschiedene Dienste betrachtet werden können. Unweigerlich steht man nun an einem Punkt, wo der Begriff Datenschutz und damit Datenschutzgesetz und informationelle Selbstbestimmung eine Rolle spielen. Das Volkszählungs-

[25] Probleme bei der (angeblichen?) Verschlüsselung von WhatsApp wurden von Heise Security aufgezeigt: http://www.heise.de/security/artikel/Der-WhatsApp-Verschluesselung-auf-die-Finger-geschaut-2629020.html
[26] http://medien-mittweida.de/55145/whatsapp-instagram-oculus/

urteil von 1983 und seine Konsequenzen stehen nun im Folgenden im Mittelpunkt der Betrachtungen.

Die Lauschangriffe im Netz haben eine andere Dimension: Der Meinungspluralismus, der ein Kennzeichen der Demokratie ist, geht verloren und Uniformität gewinnt die Oberhand (vgl. dazu auch [Be14b] und [Ko14]). Durch Verwendung entsprechender Software und Werkzeuge (z. B. kryptografischer Tools oder verschlüsselnde Messenger-Programme) kann dem entgegen gewirkt werden. Daher scheint es nur konsequent, jungen Menschen die Verwendung solcher Selbstschutz-Möglichkeiten aufzuzeigen.

3.3 Crypto-Wars als Unterrichtsthema

Ein weiterer, historisch orientierter Einstieg zum Thema Datenschutz und Privacy kann über die Crypto Wars geschehen. Crypto Wars ist ein inoffizieller Name für den Versuch der U.-S.-amerikanischen Regierung, den Zugang zur Kryptographie für die Öffentlichkeit und andere Nationen soweit zu begrenzen, dass diese sich Entschlüsselung durch die NSA und andere Geheimdienste nicht widersetzen können[27].

4 Abschlussdiskussion

In diesem Artikel haben wir fertig ausgearbeitete und erprobte Unterrichtsvorschläge diskutiert und Überlegungen und Ideen zu neuen Unterrichtsreihen zur Stärkung der informationellen Selbstbestimmung vorgestellt. Diese Ideen gilt es nun weiter auszuarbeiten. Im Rahmen des Intensivworkshops möchten wir bislang gesammelte Materialien und Ideen zur Diskussion stellen, vor allem aber mit Hilfe der Teilnehmer weitere, noch nicht bedachte Aspekte herausarbeiten und ggf. weitere Unterrichtsideen entwickeln.

Literaturverzeichnis

Alle Internetquellen wurden am 20. Juni 2015 überprüft.

[Be14a] Berendt, B.; De Paoli, S.; Laing, C.; Fischer-Hübner, S.; Catalui, D. & Tirtea, R. (2014). Roadmap for NIS education programmes in Europe. ENISA Report. https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe.

[27] https://de.wikipedia.org/wiki/Crypto_Wars und http://en.wikipedia.org/wiki/Crypto_Wars. Inzwischen wurden von Helmut Witten und Frank Oppermann erste Materialsammlungen zu diesem Thema zusammengestellt: http://de.padlet.com/frank_oppermann/bi9ysn0gl7dp/wish/53630394 und http://bscw.schule.de/pub/bscw.cgi/1198421

[Be14b] Berendt, B.; Dettmar, G.; Demir, C. & Peetz, T.: Kostenlos ist nicht kostenfrei. Oder: If you're not paying for it, you are the product". LOG IN Heft 178/179 (2014), S. 41-56.

[Dr93] Dreier, H:. Dimensionen der Grundrechte. Von der Wertordnungsjudikatur zu den objektiv-rechtlichen Grundrechtsgehalten, Hannover 1993.

[Gr15] Grillenberger, A., Romeike, R.: Big-Data-Analyse im Informatikunterricht mit Datenstromsystemen: Eine Unterrichtsbeispiel. (2015) In diesem Band.

[GHW11] Gramm, A.; Hornung, M.; Witten, H.: "E-Mail (nur?) für Dich - Eine Unterrichtsreihe des Projekts Informatik im Kontext". Beilage zu LOG IN Heft 169/170 (2011).

[IniK] http://www.informatik-im-kontext.de.

[Kl13] Klicksafe: Datenschutz TIPPS für Jugendliche. (2013) http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Jugendliche/klicksafe_Flyer_Datenschutztipps_Jugend_2013.pdf.

[Ko14] Koubek, J.: Datenschutz und Persönlichkeitsrechte. LOG IN Heft 178/179 (2014), S. 21-26.
http://medienwissenschaft.uni-bayreuth.de/assets/Uploads/Koubek/forschung/KoubekDatenschutzPersoenlichkeitsrechtePreprint.pdf.

[So11] Solove, D.: Nothing to Hide: The False Tradeoff between Privacy and Security, Chapter 1, Yale University Press, 2011