Datenschutz und Informatikunterricht

Entwicklung eines Datenschutzkompetenzmodells und Erhebung der Datenschutzkompetenz bei Schülerinnen und Schülern zur Entwicklung von Handlungsempfehlungen für den Informatikunterricht

von
Alexander Hug

Genehmigte Dissertation zur Verleihung des akademischen Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
Fachbereich 4: Informatik
Universität Koblenz-Landau

Vorsitzender des Promotionsausschusses:	Prof. Dr. Jan Jürjens
Vorsitzende der Promotionskommission:	Prof. Dr. Viorica Sofronie-Stokkermans
Erster Berichterstatter und Betreuer:	Prof. Dr. Rüdiger Grimm
Zweiter Berichterstatter:	JProf. Dr. Mario Schaarschmidt
Dritter Berichterstatter:	Prof. Dr. Johannes Magenheim

Datum der wissenschaftlichen Aussprache: 27.05.2020

Widmung

Zusammenfassung

Studien der vergangenen Jahre haben gezeigt, dass im Bereich der Datenschutzkompetenz ein Mangel bei Jugendlichen und jungen Erwachsenen besteht, jedoch standen Kinder und Jugendliche im Alter von zehn bis 13 Jahren dabei nicht so stark im Fokus. Daher ist die Leitfrage der Arbeit, wie die Datenschutzkompetenz bei Kindern und Jugendlichen in dem jüngeren Alter ausgebildet ist, um für diese Altersgruppe passende Konzepte entwickeln zu können. Zu Beginn der Arbeit wird ausgehend von einem Medienkompetenzmodell ein Datenschutzkompetenzmodell abgeleitet, welches als Grundlage für die weitere Felduntersuchung dient. An allgemeinbildenden weiterführenden Schulen in Rheinland-Pfalz wurde eine Erhebung durchgeführt, die zeigt, dass die Befragten im Bereich der Risikoabschätzung noch eine ausreichende, aber im Bereich des Wissens, der Auswahl- und Nutzungskompetenz und der Handlungskompetenz eine mangelhafte Kompetenz besitzen. Um diesem Problem zu begegnen, werden im letzten Teil der Arbeit Handlungsempfehlungen in Form von Lernzielbeschreibungen formuliert, um ausgehend davon zukünftig passende Lehr-Lern-Settings implementieren zu können.

Abstract

Studies in recent years have demonstrate adolescents and young adults to have a deficient data protection competence, however children and adolescents between the ages of ten and 13 were mostly not focus of these studies. Therefore, the guiding question of the work is how data protection competence is developed in children and adolescents at a young age in order to be able to infer suitable, educational concepts for this age group. At the beginning of the work, a data protection competence model is derived from a media competence model, which serves as the basis for the further field investigation. A survey was carried out at general secondary schools in Rhineland-Palatinate, which shows that the respondents still have sufficiently developed Risk Assessment Competence, but were insufficiently developed in terms of knowledge, Selection and Usage Competence and the Implementation Competence. Recommendations for actions are given in the last part of the work – containing learning goal descriptions to be possibly implemented in an educational framework – in order to address this issue.

„Doch es ist eben nicht einfach, sich selbst zu schützen."
(Hansen 2015a)

Vorwort

In einer von Informatiksystemen beherrschten Welt, in der das Internet und seine Anwendungen eine entscheidende Rolle spielen, muss man lernen sich zu schützen, wie Marit Hansen richtig bemerkt. Daher muss es die Aufgabe der Schule sein, Kinder und Jugendliche auf die Gefahren, ihre Rechte, aber auch ihre Pflichten in ihrer vom Internet geprägten Lebenswelt vorzubereiten. Dazu gehört es, sie in entsprechenden Kompetenzen auszubilden.

An erster Stelle steht in diesem Zusammenhang die *Medienkompetenz* – ein Wort, welches schon seit mehreren Jahrzehnten zu einem feststehenden Begriff in den Medien- und Erziehungswissenschaften geworden ist. Dabei ist dieser Begriff schwer zu fassen, da er vielschichtig ist und durch ihn eine Vielzahl von Teilkompetenzen ausgedrückt werden können. Da Informatiksysteme und das Internet inzwischen zu den wichtigsten Medien zählen, weil sie den Alltag vieler Menschen im beruflichen bzw. schulischen und auch im privaten Bereich bestimmen, müssen Kompetenzen speziell in diesem Gebiet ausgebildet und gefördert werden, weshalb sich schon frühzeitig der Begriff der *Internetkompetenz* herauskristallisiert hat.

Aber zur Internetnutzung gehört zudem eine *Datenschutzkompetenz*, um den von Marit Hansen angesprochenen Schutz möglichst umfassend zu erreichen. Doch regelmäßig in der Presse erscheinende Schlagzeilen wie *Zehntausende Bürgerdaten auf SSD-Speicher bei Ebay entdeckt*[1], *Umgang mit Kundendaten: Datenschutzbeauftragter verhängt Millionenbußgeld gegen 1&1*[2] oder *158 Verfahren gegen Polizisten wegen Daten-Missbrauch*[3] stellen eine ausgebildete Datenschutzkompetenz der Bürgerinnen und Bürger infrage. Aber was zeichnet einen datenschutzkompetenten Menschen aus? Dieser Frage geht der erste Teil der vorliegenden Arbeit nach, indem ausgehend von einem Medienkompetenzmodell ein Datenschutzkompetenzmodell abgeleitet wird.

Kompetenzen erlernt man im Laufe seines Lebens, wobei viele davon so essentiell sind (z. B. die Lesekompetenz), dass sie schon sehr früh ausgebildet und im Laufe der folgenden Jahre verfeinert und verbessert werden. Zur Gruppe solcher essentiellen Kompetenzen gehört inzwischen auch eine Datenschutzkompetenz, da Kinder und Jugendliche mit digitalen Medien und dem Internet aufwachsen und dementsprechend grundlegende Dinge im Zusammenhang mit Datenschutz wissen und einen Selbstdatenschutz beherrschen müssen. Doch wie steht es um die Datenschutzkompetenz bei Kindern und Jugendlichen? Eine Antwort auf diese Frage wird im zweiten Teil der vorliegenden Arbeit gegeben.

[1] Siehe https://www.handelsblatt.com/technik/it-internet/medienbericht-zehntausende-buergerdaten-auf-ssd-speicher-bei-ebay-entdeckt/25356650.html (zuletzt geprüft am 27.12.19)
[2] Siehe https://www.spiegel.de/netzwelt/netzpolitik/datenschutz-grundverordnung-9-5-millionen-euro-bussgeld-gegen-1-1-a-1300415.html (zuletzt geprüft am 27.12.19)
[3] Siehe https://www.zeit.de/gesellschaft/zeitgeschehen/2019-11/datenschutz-polizisten-missbrauch-datenbanken-bussgeld-polizei (zuletzt geprüft am 27.12.19)

Aufgrund dieser Ergebnisse werden letztendlich einzelne Kompetenzen und Handlungsempfehlungen in Form von Lernzielbeschreibungen für den Unterricht abgeleitet, aus denen passende Lehr-Lern-Settings konstruiert werden können. Ein ganz wichtiges Lernziel muss die *Awareness* (das sich bewusst sein, das wahrnehmen) sein, denn erst mit ihr können passende Handlungsstrategien zum Selbstdatenschutz ergriffen werden - Kein leichtes Unterfangen für den Unterricht.

Mit der vorliegenden Arbeit möchte der Autor einen Beitrag zur Förderung einer Datenschutzkompetenz bei Kindern und Jugendlichen leisten. Auch wenn alle nur denkbaren Frage noch nicht vollumfänglich beantwortet sind, so ist hiermit jedoch ein Anfang gemacht, um das Thema *Datenschutz* in den Mittelpunkt eines (Pflicht-)Informatikunterrichts zu rücken.

Abschließend soll an dieser Stelle schon einmal erwähnt werden, dass innerhalb der Arbeit wegen der besseren Lesbarkeit in der Regel die maskuline Form genutzt wird. Dies schließt selbstverständlich weibliche und diverse Personen mit ein, sofern nicht explizit darauf hingewiesen wird oder es sich aus dem Kontext erschließt.

Während der Entstehung dieser Arbeit haben viele Menschen den Weg des Autors begleitet, bei denen er sich an dieser Stelle ausdrücklich bedanken möchte. Mein erster Dank gilt Prof. Dr. Rüdiger Grimm für die Betreuung der Arbeit, JProf. Dr. Mario Schaarschmidt für die Unterstützung und Diskussion im empirischen Teil und Prof. Dr. Johannes Magenheim für die Übernahme der Funktion als Drittgutachter. Dafür, dass die Arbeit in dieser Form gelingen konnte, möchte ich mich für die vielen Diskussionen und Gespräche bei Matthias Kramer, Dirk Homscheid, Dr. Katharina Bräunlich, Johannes G. Thielen, Andreas Dengel, Alexandra Kranz, Andreas Stahlhofen, Andreas Gramm, Timothy L. K. Gillespie, Prof. Dr. Alexander Kauertz, Prof. Dr. Tobias Walter, Marco Böhm und Dr. Johannes Groß bedanken. Christopher Biehl und Sebastian Kroll danke ich für den Beitrag zur Anfertigung vieler Grafiken. Für die Unterstützung im Rahmen der praktischen schulischen Umsetzungen danke ich Dr. Jörg Luggen-Hölscher und Fabian Bildhauer. Julian Dorn unterstützte dankenswerterweise unter anderem die Studierenden Jan Savelsberg und Daniel Steil bei der Umsetzung der Projekte in *InstaHub*. Bedanken möchte ich mich bei Prof. Dr. Stefan Müller und Brigitte Jung für die Gespräche und das „Rückenfreihalten“ während der Zeit. Ein ganz großer Dank gilt am Ende den Lehrkräften, die bereit waren, ihre Lerngruppe und Unterrichtszeit für die Erhebung zur Verfügung zu stellen, den Schülern, die an der Umfrage und an der Pilotierung teilgenommen haben, aber auch den „Testschülern“ aus den MNU-Stipendiatenkursen 2016 und 2017. Des Weiteren gilt mein Dank den Personen, die bei dem Prozess der Q-Sortierung mitgearbeitet haben, und den Studierenden, deren Ergebnisse von Abschlussarbeiten mit in diese Arbeit eingeflossen sind. Im Laufe der Zeit, als diese Arbeit entstanden ist, hat der Autor viele Gespräche mit diversen Personen geführt. Diese jedoch alle namentlich zu erwähnen, würde den Rahmen dieses Vorworts sprengen.

Koblenz, im Juni 2020

Alexander Hug

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
Abs.	Absatz
ADD	Aufsichts- und Dienstleistungsdirektion
AG	Arbeitsgemeinschaft
ANK	Auswahl- und Nutzungskompetenz
Art.	Artikel
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
CC	Common Criteria
DSGVO	Datenschutzgrundverordnung
DSK	Datenschutzkompetenz
EPA	Einheitliche Prüfungsanforderungen Abitur
EPOS	Elektronische Post für Schulleitungen/Schulen in Rheinland-Pfalz
GG	Grundgesetz
GW	Gestaltungswissen
HK	Handlungskompetenz
HW	Hintergrundwissen
IniK	Informatik im Kontext
KK	Kommunikatorkompetenz
KMK	Kultusministerkonferenz, Kurzform für *Ständige Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland*
LfDI	Landesbeauftragter für den Datenschutz und die Informationstechnik
MB	Ministerium für Bildung (Rheinland-Pfalz)
NSA	National Security Agency (Auslandsgeheimdienst der USA)
OW	Orientierungswissen
PL	Pädagogisches Landesinstitut (Rheinland-Pfalz)
PW	Prozedurales Wissen
RK	Risikobewertungskompetenz
RVK	Rezeptions- und Verarbeitungskompetenz

Sek.	Sekundarstufe
Tab.	Tabelle
TLS	Transport Layer Security (Netzwerkprotokoll)
UK	Urteilskompetenz
ÜSchO	Übergreifende Schulordnung (Rheinland-Pfalz)
VPN	Virtual Private Network
W	Wissen

„Vielmehr müssen die Bürger in einer digitalen Welt in die Lage versetzt werden, verantwortungsvoll mit ihren eigenen Daten und rücksichtsvoll mit den Daten anderer umzugehen. Deshalb muss der Datenschutz auch als Bildungs- und Erziehungsaufgabe verstanden werden."
Edgar Wagner (Wagner 2012)

1. Motivation

Unsere gesamte Gesellschaft ist in der heutigen Zeit in die Abhängigkeit einer unsicheren Informationstechnologie geraten. In fast allen Bereichen tauchen Computer, die immer kleiner und damit fast schon „unsichtbar" werden, auf. Daher ist es unabdingbar, sich mit der Sicherheit technischer Systeme auseinanderzusetzen, wobei zwischen *Sicherheit der Systeme* und *Sicherheit der durch die Systeme Betroffenen* unterschieden werden muss. Nutzer können sogar zu einem nicht zu unterschätzenden Risiko in diesem Zusammenhang werden, wenn durch fehlendes Wissen und unzureichender Ausbildung falsche Entscheidungen getroffen und ungünstige Handlungen durchgeführt werden (Wagner 2001, S. 7). Aus diesem Grund muss eine Ausbildung in IT-Sicherheit schon in den Schulen beginnen. Diese Forderung wurde schon 2006 seitens der *Gesellschaft für Informatik* (GI e. V.)[4] laut: „Alle Jugendlichen müssen während ihrer schulischen Ausbildung für das Thema IT-Sicherheit sensibilisiert werden" (Gesellschaft für Informatik e. V. 2006, S. 10). Die Lehrpläne der IT-Sicherheit beinhalten Datenschutz als ein Thema, welches aus diversen Gründen, die in Abschnitt 2.2 erläutert werden, im Schulunterricht behandelt werden muss.

Durch Big Data, ein Begriff der inzwischen nicht nur die Wissenschaft beschäftigt, sondern auch ins Blickfeld der Presse und der Gesellschaft geraten ist, wird der Aspekt der Systemsicherheit und des Datenschutzes noch verstärkt. Gerade durch die kaum vorstellbare Menge an Daten, die täglich in den unterschiedlichen Formaten neu von jedem Menschen produziert werden, und die zunehmende Durchlaufgeschwindigkeit entsteht ein Problem, das im Zusammenhang mit Datenschutz zu sehen ist. Bei dieser großen Zahl an Daten ist es nämlich nicht mehr möglich, diese vollumfänglich zur Kenntnis zu nehmen und zu bewerten, weshalb eine Prüfung auf den Wahrheitsgehalt in der Regel schon ausgeschlossen ist (Freytag 2014). Daher ist es unabdingbar, dass Schüler[5] sich mit Datenmanagement auseinandersetzen.

Große Beachtung fand 2014 die Veröffentlichung der Ergebnisse der ICIL-Studie[6], eine internationale Schulleistungsstudie zur Messung computer- und informationsbezogener Kompetenzen bei Schülern der 8. Klassenstufe und zur Messung des Erwerbs dieser Kompetenzen.

[4] Siehe www.gi.de (zuletzt geprüft am 06.01.20)
[5] Im Folgenden wird zur besseren Lesbarkeit das generische Maskulinum verwendet, welches gleichermaßen die weibliche Form impliziert.
[6] ICILS steht für *International Computer und Information Literacy Study*.

Deutsche Schüler besitzen ein im Vergleich zu anderen EU-Gruppen mittleres Kompetenzniveau. Zur angeleiteten Ermittlung von Informationen, zur Bearbeitung dieser und zur Erstellung einfacher Informationsprodukte ist nur knapp die Hälfte der Probanden fähig. „Damit verfügt ein nicht unerheblicher Teil der Jugendlichen nur über rudimentäre bzw. basale Fähigkeiten und Wissensstände hinsichtlich des kompetenten Umgangs mit neuen Technologien. … Das mittlere Kompetenzniveau von Jungen [liegt] statistisch signifikant hinter dem der Mädchen zurück“ (Bos et al. 2014, S. 5). Daraus kann man ableiten, dass die Jugendlichen, obwohl sie in einer digital geprägten Welt aufwachsen, die digitalen Medien nicht automatisch kompetent nutzen können. Abschließend stellen die Autoren fest, dass „eines der zentralen Ergebnisse der Studie ICILS 2013 ist, dass es vor allem denjenigen Ländern gelingt, digitale Kompetenzen erfolgreich zu vermitteln, die über eine Gesamtstrategie, die Aussagen über Zielsetzungen, Rahmenbedingungen und Umsetzungsstrategien und Qualitätssicherungsmaßnahmen verfügen“ (Eickelmann 2017, S. 21).

In diesem Kapitel wird ausgehend von der Motivation für das Thema der vorliegenden Arbeit der Prozess der datenschutzkonformen Internetnutzung detailliert betrachtet. Dem schließt sich die Legitimation des Themas an. Abschließend werden die Forschungsfragen und die Methodik thematisiert.

1.1. Datenschutz und Jugendliche

Die heutige Welt, in der sich Schüler zurechtfinden müssen, ist geprägt durch die stetige Verwendung von Informationstechnologien sowohl im schulischen bzw. beruflichen als auch im privaten Kontext. Die Möglichkeit der Zeit- und Ortsunabhängigkeit unterstützt zudem die Nutzungshäufigkeit von mobilen Informatiksystemen. Ein Smartphone ist viel mehr als nur ein Telefon; es dient unter anderem als Mediaplayer, Kamera, Spielekonsole, Navigator, Speichermedium, Lexikon, Terminkalender und vor allem auch als Kommunikationsplattform. Bei der Verwendung von Systemen, die eine Internetnutzung und eine Internetkommunikation zulassen, ist nicht ohne Weiteres ersichtlich, wie diese mit den (persönlichen) Daten umgehen, sodass der Fähigkeit sie zu schützen, besondere Aufmerksamkeit zu schenken ist.

An die Tatsache, für Internet-Dienste kein Geld zahlen zu müssen, haben sich Nutzer inzwischen gewöhnt. Dass aber stattdessen die eigenen Daten zum „Bezahlmittel“ werden, wird oft nicht realisiert. Dabei werden die Gefahren einer unbegrenzten Preisgabe und Analyse von Daten, die sich durch Big Data noch verstärken, noch unterschätzt (Hansen 2015a, S. 2). Einmal veröffentlichte Daten geraten zudem leicht außerhalb der eigenen Kontrolle, indem sie von anderen Nutzern kopiert und in einen anderen Kontext gebracht werden. Die Daten bekommen somit eine Art „Eigenleben“ (Müsgens 2015, S. 12). Eine Studie des Psychometrics Center der Universität Cambridge verweist auf Gefahren, die aus nicht-kausalen Verknüpfungen von Daten entstehen (Kosinski et al. 2013, S. 5805). Daraus werden Persönlichkeitsprofile, die bei

Bewerbungen schon zur Ablehnung geführt haben[7], entwickelt, um bei *Facebook* und *Google* gezielt Werbung zu schalten und damit Nutzer letztendlich zu beeinflussen (vgl. (Rieger 2013), (Saint-Mont 2013, S. 106), (Wolf 2011)).

Durch personalisierte Algorithmen kann eine sogenannte Filterblase entstehen, d. h. durch die Personalisierung bekommt der Nutzer nur noch die Inhalte angezeigt, die zu ihm – jedenfalls aufgrund der Algorithmen – passen, während gleichzeitig widersprechende Inhalte nicht mehr angezeigt werden. In *Facebook* z. B. werden vornehmlich nur noch Seiten, die der Nutzer „gelikt" hat, oder Posts gleichgesinnter „Freunde" angezeigt (Pariser 2011). Besonders aufsehenerregend konnte dies im Fall der US-Präsidentschaftswahl 2016 verdeutlicht werden. Aufgrund von „Gefällt-Mir"-Angaben bei *Facebook* sind von dem Unternehmen *Cambridge Analytica* 2016 rund 87 Millionen Persönlichkeitsprofile von US-Bürgern erstellt worden, um damit Informationen zur Unterstützung des Wahlkampfs zu streuen.[8] Solche Dinge zeigen zudem, wie stark inzwischen der Einfluss von *Facebook*, aber auch von *Google* auf die Politik ist (Rieger 2013).

Um Nutzerprofile zu erstellen, werden Cookies eingesetzt, die heute auf kaum einer Webseite noch fehlen. Da dies beim Surfen im Netz über mehrere Seiten erfolgt, spricht man vom *User-Tracking*[9] (Oberle et al. 2003). Aufgrund der Cookies kann eine personalisierte Werbung erfolgen, d. h. dass unbemerkt nur die für den Nutzer passende Werbung eingeblendet wird (Zeidler und Brüggemann 2014). Beim Online-Einkauf stellt zudem das sog. *Dynamic Pricing* ein Problem dar (Gönsch et al. 2009)[10]. Aufgrund des durch Cookies gespeicherten Einkaufverhaltens und des benutzten Geräts (Apple- oder Windows-Rechner) werden bei demselben Händler unterschiedliche Preise dem Kunden für ein und das selbe Produkt geboten. Dies soll einerseits den Kaufanreiz fördern und die Kaufschwelle herabsetzen und andererseits dem Anbieter den größtmöglichen Gewinn bieten, denn Nutzer, die mit einem teuren Gerät surfen und namhafte teure Produkte in der Vergangenheit gekauft haben, sind auch eher bereit für ein Produkt oder Dienstleistung mehr Geld auszugeben. Beim Online-Einkauf kommt zudem

[7] vgl. https://www.impulse.de/recht-steuern/background-checkbewerber/1032765.html (zuletzt geprüft am 19.09.19)

[8] vgl. dazu den Fernsehbeitrag *Fake America Great Again* (https://programm.ard.de/TV/arte/fake-america-great-again/eid_28724905318542, zuletzt geprüft am 07.11.19) und den FAZ-Artikel *Cabridge Analytica speicherte Facebook-Daten bis 2017* (https://www.faz.net/aktuell/wirtschaft/diginomics/cambridge-analytica-speicherte-facebook-daten-bis-2017-15578244.html, zuletzt geprüft am 25.09.19). In einem Videobeitrag berichtet ein früherer Arbeitnehmer von *Cambridge Analytica* über diesen Zusammenhang (vgl. https://www.theguardian.com/uk-news/video/2018/mar/17/cambridge-analytica-whistleblower-we-spent-1m-harvesting-millions-of-facebook-profiles-video zuletzt geprüft am 27.09.19). Die Autorin berichtet ferner, wie schon bei der Brexit-Kampagne 2016 auf die gleiche Art und Weise Facebook-User manipuliert worden sind (vgl. https://www.tagesspiegel.de/gesellschaft/journalistin-carole-cadwalladr-ich-konnte-es-zunaechst-selbst-nicht-glauben/24105126-all.html zuletzt geprüft am 27.09.19).

[9] Ein Tracking findet z. B. auch bei der Nutzung von sogenannte Smart-TV statt. Informationen über die Gerätenutzung und die Sehgewohnheiten werden – laut AGB anonym – an die Fernsehhersteller gesendet (vgl. Hansen 2015a, S. 3).

[10] zur Rechtmäßigkeit siehe https://www.datenschutzbeauftragter-info.de/ist-individuelles-dynamic-pricing-zulaessig/ (zuletzt geprüft am 19.09.19).

hinzu, dass Käufer freiwillig und unreflektiert persönliche Daten[11] herausgeben, weil sie in Formularen gefordert werden, die aber für den Kaufprozess nicht notwendig sind. Ein ähnliches Bild ergibt sich bei der Anmeldung von Online-Diensten oder Gewinnspielen.[12] Auf diese Art gelangen Datensammler an die persönlichen Daten von Nutzern. Unternehmen wie *PayPal* und *Amazon* sammeln ferner weitere Daten ihrer User. *Amazon* z. B. verfolgt nicht nur den Zeitpunkt und den Artikel eines Einkaufs, sondern speichert auch angeklickte Links, Suchanfragen, Artikel im Warenkorb, reagierte E-Mails, benutzte IP-Adressen und viele weitere Dinge.[13] Dadurch dass Nutzer bei der Internetnutzung häufig gleiche Passwörter zur Anmeldung bei unterschiedlichen Diensten nutzen (Florencio und Herley 2007, S. 660), besteht ein weiteres Gefahrenpotential, dass in einem Identitätsdiebstahl enden kann (Borges et al. 2011, S. 152).

Insbesondere mobile Apps, die auch schon bei Kindern und Jugendlichen beliebt sind, stellen eine Gefahrenquelle dar, da auf den Smartphones inzwischen alle persönlichen Informationen gespeichert sind und durch den *always-on*-Status eine ununterbrochene Netzverbindung besteht (Eckert 2013, S. 88)[14]. Durch die gesammelten Daten erstellt *Google Maps* Bewegungsprofile seiner Nutzer.[15] Wenn von einer Person ein Bild vorliegt (z. B. als biometrisches Bild bei der Beantragung des Personalausweises), so kann durch Überwachungskameras an öffentlichen Plätzen die Person identifiziert und ggf. verfolgt werden (Eckert 2013, S. 508). Eine dramatische Zuspitzung findet dann statt, wenn es wie im Fall von Südkorea eine gesetzlich verordnete Überwachung der Smartphones von Kindern durch die Eltern gibt.[16] Dies ist nur ein Beispiel, wie sich Gesellschaft entwickeln kann.

Schülern ist zudem häufig im Rahmen der Nutzung Sozialer Netzwerke[17] der Unterschied zwischen mündlicher und schriftlicher Kommunikation und privater und öffentlicher Kommunikation nicht bewusst. Datenschutz ist hier die „stillschweigende Annahme, dass die anderen sich nicht für meine Daten und Lebensäußerungen zu interessieren haben – egal, wie und wo ich sie von mir gebe“ (Koubek 2008, S. 39). Die Aspekte der Datenzusammenführung, die daraus erwachsende Profilierung und die Risiken, die davon ausgehen, werden nicht gesehen bzw. können nicht gesehen werden. Die Tragweite von Postings ist – so zeigen es die Studien – den Schülern nicht bewusst (vgl. Abschnitt 2.3.2). Falsche oder ungenügende Datenschutz-Einstellungen im persönlichen Profilbereich führen zu ungewollter Datenveröffentlichung und

[11] Im juristischen Bereich wird von personenbezogenen und personenbeziehbaren Daten gesprochen. In der Literatur hat sich synonym dafür auch der Begriff der persönlichen Daten eingebürgert. In der vorliegenden Arbeit wird der Begriff *personenbezogene Daten* bevorzugt verwendet.

[12] vgl. https://www.pcwelt.de/news/Gewinnspiele-CoPersoenliche-Daten-werden-oft-weitergegeben-137835.html (zuletzt geprüft am 26.09.19)

[13] vgl. https://www.spiegel.de/netzwelt/web/amazon-experiment-was-der-konzern-mit-jedem-klick-erfaehrt-a-1205079.html (zuletzt geprüft am 26.09.19)

[14] Für den Unterricht siehe (Rack und Sauer 2018)

[15] vgl. https://www.zeit.de/digital/datenschutz/2019-09/digitale-aengste-gps-datenschutz-internet-sicherheit/komplettansicht (zuletzt geprüft am 26.09.19); sein Bewegungsprofil kann man unter https://www.google.com/maps/timeline?pb einsehen.

[16] vgl. https://www.wiwo.de/technologie/digitale-welt/tracking-apps-wenn-eltern-das-handy-der-kinder-ausspaehen/11998838-all.html (zuletzt geprüft am 26.09.19)

[17] Zur Definition und zur Bedeutung des Begriffs *Soziale Netzwerke* in dieser Arbeit siehe Anhang A4.17.

-weitergabe. Der nachlässige Umgang mit persönlichen Daten führt zu einer Missachtung des Persönlichkeitsrechts (abgeleitet aus dem Recht auf informationelle Selbstbestimmung), sodass eine Sensibilisierung durch das „Sichtbarmachen ungewollter Konsequenzen“ (Koubek 2008, S. 39) erreicht werden kann. Durch die Sozialen Netzwerke ist eine „große Macht über die Achtung der Persönlichkeitsrechte ihrer Mitmenschen gegeben“ (Koubek 2008, S. 40), sodass hier eine große Verantwortung von den Nutzern verlangt wird.

Um die Fähigkeit im verantwortungsbewussten Umgang mit den eigenen Daten und den persönlichen Daten anderer zu stärken, muss im Unterricht eine Datenschutzkompetenz bei den Lernenden ausgebaut und gefördert werden. Hierzu müssen Möglichkeiten ausgelotet werden, „Kinder und Jugendliche so früh wie möglich direkt anzusprechen und auf mögliche Datenschutzprobleme hinzuweisen“ (Kramer und Spaeing 2014, S. 372). Der hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Johannes Caspar, schreibt dazu, dass „faktisch … sich die hohe Bedeutung, die eine Kompetenzförderung auf dem Gebiet des Datenschutzes vor allem für Kinder im Schulalter hat, nicht bestreiten [lässt]. Gerade bei den jungen Menschen bedarf es eines Bewusstseins über die zahlreichen ökonomischen, sozialen, kulturellen und rechtlichen Risiken und Nachteile. … Es besteht daher eine staatliche Schutzpflicht, die Datenschutzkompetenz gerade der Heranwachsenden zu fördern und sie in die Lage zu versetzen, informiert über ihre Entscheidungen der Internet-Nutzung zu reflektieren“ (Caspar 2013, S. 769).

Schaut man in die Lehrpläne und Bildungsstandards zum Informatikunterricht in Deutschland, so wird dort explizit das Thema *Datenschutz* erwähnt (vgl. Abschnitt 2.2). Aber es sind einerseits Schlagzeilen der Presse[18], in denen beispielhaft vom Fehlverhalten von Jugendlichen im Internet berichtet wird, und andererseits die Ergebnisse von Studien, die die Vermutung nahelegen, dass weder im Informatikunterricht noch im Unterricht anderer Fächer (im Sinne eines fachübergreifenden Unterrichts) der Datenschutz ausreichend thematisiert und daher bei den Schülern keine Datenschutzkompetenz ausgebildet wird (vgl. Abschnitt 2.3.2). Es ist ferner nach dem gegenwärtigen Stand der Wissenschaft auch nicht ausreichend geklärt, was man unter Datenschutzkompetenz genau zu verstehen hat und wie diese im Informatikunterricht gestärkt werden könnte. Dieser Aufgabe widmet sich die vorliegende Dissertation und möchte einen Beitrag zur Ausbildung von Datenschutzkompetenz bei Jugendlichen leisten.

Sowohl in der politischen wie auch in der erziehungswissenschaftlichen Diskussion wird gerne ein Fach *Medienkunde* gefordert, welches informatische Inhalte – und damit auch das Thema

[18] Z. B. Ungewollte Geburtstagseinladung in Facebook (https://www.spiegel.de/panorama/gesellschaft/nach-facebook-panne-tausend-gaeste-kommen-uneingeladen-zu-geburtstagsparty-a-766556.html), Schüler verbreiten Nacktfotos (https://www.sueddeutsche.de/bayern/neuburg-an-der-donau-schueler-verbreiten-nacktfoto-einer-14-jaehrigen-1.1728744) oder Schulleiter warnen von Sexting (https://www.tagesspiegel.de/gesellschaft/panorama/schueler-verschicken-ihre-nacktbilder-schulleiter-warnen-vor-sexting/9014968.html) (alle Adressen zuletzt geprüft am 19.09.19)

Datenschutz – integrieren soll.[19] Der Pädagoge Hilbert Meyer hat im Rahmen der INFOS-Tagung im September 2017[20] und auch beim MNU-Bundeskongress im März 2019 in einem öffentlichen Vortrag ein klares Bekenntnis für ein Pflichtfach *Informatik* in der Sekundarstufe I gegeben, da kein anderes Fach informatische Inhalte ausreichend anbieten kann. Nur im Primarbereich plädiert er für eine Integration informatischer Inhalte in den bestehenden Fächerkanon, vornehmlich den Sachunterricht. Die Presse berichtete Ende Juli 2019[21], dass der Präsident von BITKOM[22], Achim Berg, sogar ein Handy für jedes Grundschulkind und die Einbindung der Geräte in den Unterricht empfahl. Begründet wurde dies einerseits mit der Tatsache, dass man um ein Smartphone nicht herumkäme, und andererseits die Kinder ein Recht auf digitale Teilhabe besäßen. Untersuchungen von BITKOM zeigen, dass die meisten Kinder schon mit zehn Jahren ein eigenes Smartphone besitzen.[23] Dies ist ein weiterer Nachweis dafür, dass die Ausbildung einer Datenschutzkompetenz spätestens mit Eintritt in die Sekundarstufe I (mit 10 Jahren) im Unterricht erfolgen muss.

1.2. Internetnutzung als ein Spagat zwischen eigener Kontrolle und Vertrauen

Eine datenschutzkonforme Internetnutzung kann durch einen differenzierten Prozess beschrieben werden (vgl. Abb. 1.1), bei dem „der Mensch als Sicherheitsrisiko … selbst durch technische Vorkehrungen nicht völlig ausgeschaltet werden [kann]. Die spektakulären Angriffe auf Internet-Anbieter wie Yahoo und Amazon haben dies deutlich gemacht“ (Wagner 2001, S. 7). Es geht letztendlich darum, dass die Risiken der Internetnutzung im Hinblick auf Privatheit durch Kontrolle und/oder Vertrauen minimiert werden.

Der Nutzer kann das Ausmaß an Kontrolle dieses Prozesses bis zu einem gewissen Grad selbst bestimmen und damit Selbstdatenschutz (vgl. Abschnitt 2.1.1) betreiben. Dies ist jedoch abhängig von der Fachkompetenz, die wiederum mit dem Alter und dem Bildungshintergrund korreliert.[24] Selbstdatenschutz, der immer wieder neu vom Nutzer angestoßen wird, kann über zwei Wege erfolgen:

(1) Der Nutzer entscheidet selbst – sofern es möglich ist – welche Daten er angibt. (Z. B. in Sozialen Netzwerken kann man dies gut kontrollieren, beim Online-Einkauf jedoch muss man ein Minimum an Daten angeben, damit der Kaufvertrag zustande kommen kann.)

[19] Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. weist „auf die Notwendigkeit der Aufnahme des Fachs Medienkompetenz bezogen auf Datenschutz in das Curriculum“ hin (Kramer und Spaeing 2014, S. 372).
[20] Vgl. https://uol.de/ddi/infos2017/programm-tagungsband-u-videos (zuletzt geprüft am 19.09.19).
[21] z. B. siehe https://www.wz.de/panorama/bitkom-praesident-achim-berg-empfiehlt-ein-handy-ab-der-grundschule_aid-44636951 (zuletzt geprüft am 28.09.19)
[22] Siehe https://www.bitkom.org/ (zuletzt geprüft am 22.11.19)
[23] Siehe https://www.bitkom.org/Presse/Presseinformation/Mit-10-Jahren-haben-die-meisten-Kinder-ein-eigenes-Smartphone (zuletzt geprüft am 28.09.19); siehe auch https://www.zeit.de/news/2019-05/28/bitkom-smartphones-unter-kindern-selbstverstaendlich-190528-99-410795 (zuletzt geprüft am 28.09.19)
[24] Vgl. (Wagner et al. 2010, S. 3) und Abschnitt 2.3.

(2) Der Nutzer setzt Techniken und Werkzeuge (Tools) ein. (Z. B. durch die Kommunikation mit verschlüsselten E-Mails kann man einem Man-in-the-Middle-Angriff entgegenwirken, durch passende Browser-Add-Ons die automatische Ausführung von Skripten oder Third-Party-Cookies unterbinden.)

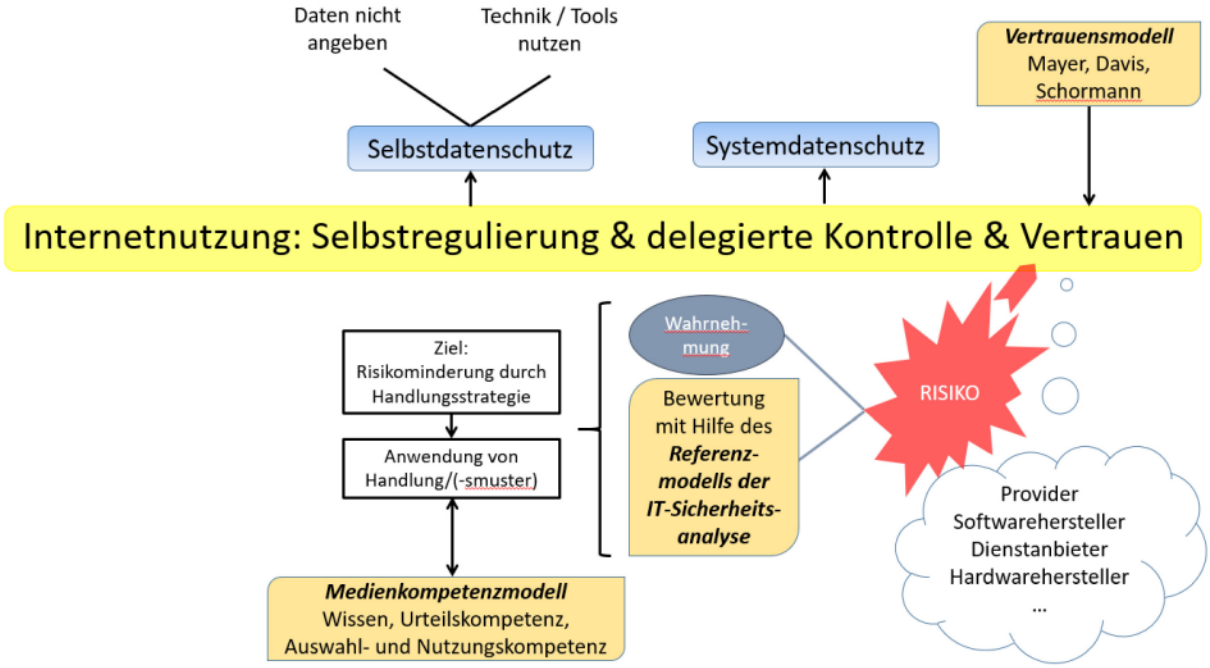


Abb. 1.1: Datenschutzkonforme Internetnutzung als ein Spagat zwischen eigener Kontrolle, delegierter Kontrolle und Vertrauen

Hinzu kommt der im Hintergrund laufende Systemdatenschutz, der bis zu einem gewissen Grad ebenso eine Datenschutzkompetenz des Nutzers erfordert (vgl. Abschnitt 2.1.1). Hierbei handelt es sich um eine delegierte Kontrolle, wozu das Schutzbedürfnis auf Andere übertragen wird.

Des Weiteren muss der Nutzer folgenden Parteien, die bei der Nutzung des Internets eine Rolle spielen, Vertrauen entgegenbringen[25]:

(1) Hardware-Hersteller, dem der Nutzer vertraut, dass das technische System keine Lücken zur Manipulation zulässt.

(2) Softwarehersteller (Anbieter von Browser, Mail-Clients, Add-Ons, Verschlüsselungssoftware usw.): Da die verschiedenen Systeme auch noch untereinander zusammenwirken, ist es dem Nutzer gar nicht mehr möglich, die Zusammenhänge des Datenzugriffs und der Datenweitergabe bis ins Detail zu kontrollieren.

[25] Der Aspekt des Vertrauens wird durch das Modell von Davis, Mayer und Schormann beschrieben, welches in Abschnitt 3.2 dargestellt wird (Mayer et al. 1995).

(3) Netz-Anbieter, dem der Nutzer vertraut, dass er nur die Daten der Internetnutzung protokolliert, die zur Abrechnung der Dienstleistung notwendig und vom Gesetzgeber gefordert sind.

(4) Anbieter von Diensten im Internet, die einerseits Nutzerdaten für die Abwicklung Ihrer Dienstleistung benötigen, die aber andererseits – je nach Ziel – mit den Nutzerdaten einen Handel betreiben.

In diese Vertrauensbeziehung greift immer ein Risiko ein, welches der Nutzer erst einmal erkennen und dann abschätzen bzw. bewerten muss.[26]

Ziel des Ganzen muss letztendlich eine Risikominderung durch passende Handlungen und Handlungsstrategien sein, die eine erfolgreiche Verknüpfung von Selbst- und Systemdatenschutz und Vertrauen darstellen, wobei das verbleibende Restrisiko bewusst und akzeptabel sein muss. Die Handlungsstrategien orientieren sich an der in dieser Dissertation entwickelten Datenschutzkompetenz. Dazu wird ausgehend von diesen Überlegungen in Kapitel 3 ein Datenschutzkompetenzmodell hergeleitet und Datenschutzkompetenzen werden abgeleitet.

1.3. Legitimation des Themas

Bei der Nutzung von Informatiksystemen fallen auf mehreren Ebenen personenbezogene Daten an. Einerseits kommunizieren Nutzer untereinander und nehmen Dienste in Anspruch, bei denen sie ihre Daten zweckgebunden einbringen, zum Beispiel Namen, E-Mail-Adressen und Lieferadressen, wobei die Durchsetzung der Zweckbindung nicht im Machtbereich der Nutzer liegt. Andererseits erzeugen die Nutzer unbewusst Datenspuren, die oft personenbeziehbar sind, wie zum Beispiel IP-Adressen und Sitzungscookies. So kommt eine Unmenge an unstrukturierten Daten zusammen (Big Data), die es zu beherrschen gilt. Durch die Technik des Data Minings wiederum werden neue Daten generiert, die in Verbindung mit vorhandenen Daten zu neuen Erkenntnissen führen. Diese Daten sind eine begehrte Ware für die Entwicklung von Nutzungsprofilen, unter anderem zum Zweck der personenbezogenen Werbung. Das entzieht sich der Einflussnahme der Nutzer. Der sich daraus ergebende Verlust von Privatheit wird weltweit als eines der Probleme des modernen Lebens angesehen (vgl. (Wagner 2012), (Wagner 2010), (Hansen 2015b), (Caspar 2013)).

Jedoch ist der Anspruch an Privatheit und das Recht auf informationelle Selbstbestimmung (vgl. Abschnitte 2.1.1 + 2.1.2), die sich aus den Artikeln 1 und 2 des Grundgesetzes ableiten, jedem garantiert. Somit ist Datenschutz ein Grundrecht eines jeden Einzelnen, selbst über die Nutzung, Weitergabe und Veröffentlichung seiner persönlichen Daten zu bestimmen. Die Fä-

[26] Hier greift das Referenzmodell für ein Vorgehen der IT-Sicherheitsanalyse von (Grimm et al. 2016) (vgl. Abschnitt 3.3).

higkeit, dieses Recht wahrzunehmen, wird im Folgenden als Datenschutzkompetenz angesehen. Eine exakte Definition von Datenschutzkompetenz wird aus dem Datenschutzkompetenzmodell in Kapitel 3 abgeleitet.

Wichtig ist die Frage nach dem Kontext, in dem Datenschutzkompetenz erworben werden soll und kann. In dieser Dissertation wird unterstellt, dass neben privater Selbsthilfe und beruflicher Weiterbildung die Schule ein geeigneter Lernkontext ist. Dabei stellt sich die Frage nach dem Alter, in dem man mit Aspekten des Datenschutzes (in der Schule) konfrontiert werden soll. Da Schüler häufig auch entgegen der AGB Sozialer Netzwerke und Messenger-Diensten unter einem Alter von 13 bzw. 16 Jahren solche Dienste nutzen[27], muss das Thema personenbezogene Daten und Schutz dieser Daten spätestens mit Eintritt in die weiterführende Schule (Klassenstufe 5) erfolgen. (Die Frage nach der Eignung des Themas für die Grundschule wird in dieser Dissertation nicht behandelt.[28]) Trotz des erhöhten Schwierigkeitsgrads und einer scheinbaren Theorielastigkeit des Themas muss durch entsprechende didaktische Reduktion und einen kontextorientierten Zusammenhang das Thema *Datenschutz* im Sinne eines Spiralcurriculums unterrichtet werden. In den Lehrplänen und Bildungsstandards der Informatik wird das Thema genannt und müsste damit im jeweiligen Unterricht thematisiert werden (vgl. Abschnitt 2.2).

[27] Vgl. KIM-Studie 2018 (Feierabend et al. 2019, S. 35) und JIM-Studie 2018 (Feierabend et al. 2018, S. 38); laut jeweiligen AGB ist das Mindestalter für eine Anmeldung bei *Facebook*, *Instagram* und *Snapchat* 13 Jahre, bei *WhatsApp* jedoch in der EU 16 Jahre.

[28] Für diese Altersstufe existieren entsprechende Angebote und Materialien bei „Internet-ABC“ (https://www.internet-abc.de/, zuletzt geprüft am 24.10.19).

1.4. Forschungsfragen und Gliederung der Arbeit

Die Ausgangslage stellt sich so dar, dass viele wissenschaftliche Arbeiten (vgl. (Masur et al. 2017)) darauf hinweisen, dass Datenschutzkompetenz – bei aller Unklarheit des Begriffs (soweit dazu die vorliegende Arbeit) – grundlegend zur Durchsetzung von Datenschutz ist. Der Erwerb von Datenschutzkompetenz bei Jugendlichen in dem Alter zu entwickeln, in dem die Nutzung von Smartphones und Sozialen Netzwerken beginnt, ist die Aufgabe der (Fach-)Didaktik mit Fokus auf Medien, Informatik und ihren Anwendungen.

In der vorliegenden Arbeit sollen folgende Forschungsfragen beantwortet werden:

1) Wie kann man Datenschutzkompetenz konzeptualisieren?

2) In welchen Dimensionen des in dieser Arbeit hergeleiteten Datenschutzkompetenzmodells weisen Schüler der Klassenstufe 5 bis 7 einen Mangel an Datenschutzkompetenz auf?

3) Wie könnte dem Mangel an Datenschutzkompetenz begegnet bzw. dieser behoben werden?

Zur Beantwortung der Forschungsfragen wird die Arbeit wie folgt gegliedert:

Nachdem in dem folgenden Kapitel 2 der Stand der Wissenschaft und bestehende Forschungsansätze zum Thema *Datenschutz und Informatikunterricht* dargestellt werden, steht im Kapitel 3 die Entwicklung eines Datenschutzkompetenzmodells im Vordergrund. Dies geschieht durch eine Ableitung aus einem Medienkompetenzmodell, einem Vertrauensmodell und einem Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse. Auf der Basis dieses Modells lässt sich eine Definition für Datenschutzkompetenz herleiten.

Das Datenschutzkompetenzmodell liefert nun eine Vorlage, die es ermöglicht, Untersuchungen zur Datenschutzkompetenz bei Schülern durchzuführen. Die Realisierung einer Erhebung bei Jugendlichen im Alter von zehn bis 13 Jahren an allgemeinbildenden Schulen in Rheinland-Pfalz wird in Kapitel 4 beschrieben. Die dabei gewonnenen Daten werden deskriptiv ausgewertet und interpretiert (sowohl in ihrer Gesamtheit als auch getrennt nach Geschlecht und Altersklassen). Ferner werden korrelative Zusammenhänge zwischen den Dimensionen des Datenschutzkompetenzmodells aufgedeckt.

Aus den Ergebnissen lassen sich Hinweise für die Ausprägung von Lehrinhalten zur Verbesserung der Datenschutzkompetenz ableiten, wobei der Schutz der eigenen Privatsphäre im Vordergrund stehen soll. Im Rahmen dieser Arbeit entstandene Abschlussarbeiten im praktischen Umfeld des Unterrichts werden in Kapitel 5 vorgestellt. Dem schließen sich mit Kapitel 6 Handlungsempfehlungen für den Unterricht an, bevor die Arbeit mit der Zusammenfassung der Ergebnisse und einem Ausblick (Kapitel 7) endet.

„You have zero privacy anyway. Get over it."
Scott Mc Neally, 1999
(Weichert 2012)

2. Grundlagen, Stand der Wissenschaft und Forschungsansätze zum Thema *Datenschutz und Informatikunterricht*

Im folgenden Kapitel wird der wissenschaftliche Stand zum Thema der Dissertation herausgearbeitet und die Arbeit in den wissenschaftlichen Kontext integriert. Nach der Definition von Grundbegriffen wird in einem zweiten Schritt das Thema *Datenschutz* für Schule und Unterricht legitimiert[29]. Im Anschluss werden existierende Studien, Forschungsarbeiten und Beiträge vorgestellt. Ein Blick auf die für Jugendliche und Unterricht entwickelten Materialien runden das Kapitel ab.

2.1. Grundbegriffe

Die folgenden Abschnitte dienen der Definition und Erläuterungen von Grundbegriffen und Zusammenhängen, die für das Verständnis der weiteren Arbeit dienlich sind.

2.1.1. Der Begriff des Datenschutzes

Der Grundlegendste aller Begriffe in dieser Arbeit ist der des Datenschutzes, der ein juristischer Begriff ist. **Datenschutz** ist ein „Sammelbegriff über die in verschiedenen Gesetzen zum Schutz des Individuums angeordneten Rechtsnormen, die erreichen sollen, dass seine Privatsphäre[30] in einer zunehmend automatisierten und computerisierten Welt … vor unberechtigten Zugriffen von außen … geschützt wird."[31] Die Rechtsnormen sind in erster Linie die EU-Datenschutzgrundverordnung (DSGVO), das Bundesdatenschutzgesetz und die jeweiligen Landesdatenschutzgesetze. Ferner zählen aber auch Gesetze wie das Teledienstgesetz, das Teledienstedatenschutzgesetz, das Telekommunikationsgesetz, die Telekommunikationsüberwachungsverordnung, das Telemediengesetz oder das Arbeitsrecht dazu. Sie dienen dem Schutz personenbezogener Daten vor Missbrauch. Nach Artikel 4 der DSGVO sind „personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person … beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt

[29] In diesem Abschnitt wird das Thema in dem Bezug auf Unterricht legitimiert, so wie dies innerhalb einer didaktischen Analyse erfolgt. Ziel ist es zu zeigen, dass das Thema mit Rechtsvorschriften (wie z. B. Lehrplänen) und wissenschaftlichen Ansätzen konform ist. Die Legitimation des Dissertationsthemas befindet sich in Kapitel 1.

[30] Zum Begriff *Privatsphäre* und *Privatheit* s. Abschnitt 2.1.2.

[31] Siehe http://wirtschaftslexikon.gabler.de/Definition/datenschutz.html#definition (zuletzt geprüft am 11.01.18)

oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“ (Europäische Union 2016).

Dem Problem des Schutzes personenbezogener Daten ist der Nutzer nicht nur bei der Benutzung von Computer und Smartphone, sondern auch in Alltagssituationen (z. B. Videoüberwachung einer U-Bahn-Station) ausgesetzt. Zudem kommt auch dem häufig unbedachten Umgang mit den Daten durch den Nutzer selbst eine entscheidende Rolle zu. Der Begriff *Datenschutz* umspannt daher einen sehr großen Bereich.

Die Sicherung des Grundrechts auf **informationelle Selbstbestimmung** eines Einzelnen ist der Zweck und das Ziel von Datenschutz. Dieses erwächst aus dem Volkszählungsurteil des BVerfG von 1983, welches eine Grundsatzentscheidung darstellt. Dort heißt es: „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. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“[32]

Damit ist sichergestellt, dass das Grundrecht gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten eines jeden Einzelnen gewährleistet ist. Somit kann jeder selbst über Preisgabe und Verwendung seiner Daten entscheiden.

Weitergehend wird der Datenschutz durch die 2018 in Kraft getretene EU-Verordnung für ganz Europa einheitlich geregelt. Diese Verordnung war insofern nötig, da europäische Firmensitze weltweit agierender Unternehmen (z. B. *Facebook* mit Sitz in Irland) sich auf die Datenschutzgesetze des Firmensitzlandes beriefen, die sich in Europa von Land zu Land unterschieden. Durch die EU-Richtlinie wird gewährleistet, dass ein einheitlicher Standard in den Ländern der EU gilt.

[32] Siehe http://www.servat.unibe.ch/dfr/bv065001.html, Fundstelle 154 + 155 (zuletzt geprüft am 11.01.18)

Aus dem Artikel 5 der Europäischen Datenschutzgrundverordnung (Europäische Union 2016) lassen sich die **Datenschutzprinzipien** (Grundsätze für die Verarbeitung personenbezogener Daten) ableiten. Dies sind (a) „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, (b) „Zweckbindung“, (c) „Datenminimierung“, (d) „Richtigkeit“, (e) „Speicherbegrenzung“, (f) „Integrität und Vertraulichkeit“ und (g) „Rechenschaftspflicht“.

Da der Begriff des Datenschutzes sehr weit gefasst ist, wird mit weiteren Begriffen gearbeitet, um die Zusammenhänge besser zu differenzieren. So versteht man z. B. unter *technischem Datenschutz* technisch-informatische Methoden und Funktionen zur Unterstützung der IT-Sicherheitsanforderungen, die sich aus dem Datenschutz ergeben. Dazu zählen z. B. Verschlüsselungstechnologien oder die VPN-Funktion.

Ein wichtiges Begriffspaar in diesem Zusammenhang ist das des **Selbstdatenschutzes** und des **Systemdatenschutzes**, die sich weder organisatorisch noch technisch scharf trennen lassen, da sie nicht getrennt voneinander funktionieren. Je nach Sichtweise auf einen Aspekt handelt es sich um die Zuweisung einer Maßnahme in den Bereich des Nutzers oder in den Systembereich. Wegen der unterschiedlichen Betrachtungsweise existieren Definitionen für beide Begriffe (Grimm 2015).

Unter *Systemdatenschutz* werden Datenschutzmaßnahmen verstanden, bei denen der Datenschutz in die Technik „eingebaut“ ist. „Für den Systemdatenschutz ist charakteristisch, dass seine Maßnahmen nicht greifen oder Nutzer die entsprechenden Funktionen nicht ausführen können, wenn sie nicht im System angelegt und von den Anbietern unterstützt werden.“ Beispiele sind der Einsatz des TLS-Protokolls während des Online-Bankings oder von Firewalls. „Einige Maßnahmen des Systemdatenschutzes funktionieren ohne weiteres Zutun des Nutzers … andere erfordern, dass Nutzer die Angebote des Systems wahrnehmen.“ (Roßnagel et al. 2003, S. 113)

Demgegenüber beschreibt der *Selbstdatenschutz*[33] jede Form von Aktivitäten zum Datenschutz, die vom Nutzer ausgehen (z. B. der Einsatz von einer Verschlüsselungssoftware für E-Mails, lokale Einstellungen des Browsers oder lokale Spam-Mail-Filter). Damit beschreibt Selbstdatenschutz „die Menge an Aktivitäten, die ein Betroffener aktiv zum Schutz seines Rechts auf informationelle Selbstbestimmung ergreifen kann“ (Wagner 2013, S. 9). Um Selbstdatenschutz auszuüben, ist eine Datenschutzkompetenz von Nöten. Nach Yong wurde „online privacy literacy … defined as a ‘principle to support, encourage, and empower users to undertake informed control of their digital identities’“ (Trepte et al. 2015b, S. 334). In Abschnitt 3.4 wird auf der Basis eines Datenschutzkompetenzmodells eine breiter angelegte und differenzierte Definition von Datenschutzkompetenz abgeleitet.

[33] Eine ausführliche und informative Seite für den Verbraucher zum Thema Selbstdatenschutz ist vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz herausgegeben worden (vgl. https://www.datenschutz.rlp.de/de/themenfelder-themen/selbstdatenschutz/; zuletzt geprüft am 18.08.2019).

Es gibt drei **Datenschutzmodelle**, die auf drei unterschiedlichen Hypothesen beruhen (Egger und Schillinger 1996, S. 49):

(1) **Sphärenhypothese:** In diesem Modell werden drei Sphären angenommen, nämlich die Intimsphäre, die Öffentlichkeitssphäre und die Privatsphäre, die bildlich zwischen den beiden anderen Sphären angeordnet ist. Innerhalb der Privatsphäre gibt es verschiedene Sektoren und es finden nur ausgewählte sektorale Zugriffe statt (s. Abb. 2.1). Jedoch ist eine klare Trennung zwischen den Sektoren häufig schwierig. „Es ist auch unmöglich, einen absolut geschützten bzw. einen gänzlich öffentlichen Bereich im Leben eines Menschen zu definieren. Denn die Privatsphäre ist etwas subjektiv Empfundenes, das von der jeweiligen Situation der Betroffenen abhängt. Die starre Einteilung der Daten nach ihrer Sensitivität trägt diesem Empfinden nicht Rechnung." (Egger und Schillinger 1996, S. 50)

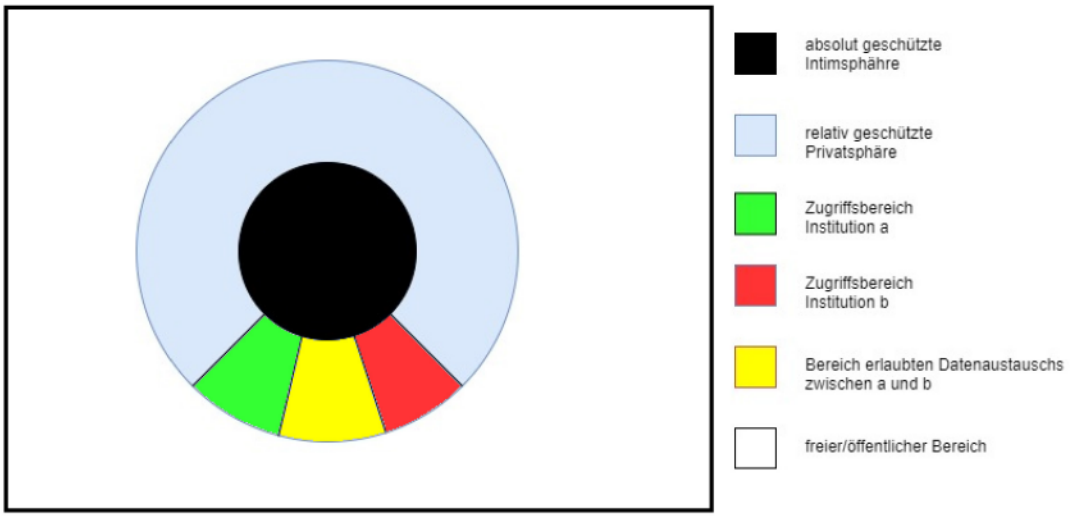


Abb. 2.1: Datenschutz nach der Sphärenhypothese
(Egger und Schillinger 1996, S. 50)

(2) **Mosaikhypothese:** Ausgangspunkt der Überlegungen, die an die Sphärenhypothese anknüpfen, ist, dass Daten von sich aus alleine nicht sehr viel aussagen, erst durch die Kombination mit anderen Informationen kann es zu ungewünschten Einblicken in die Privatsphäre kommen. Diese Betrachtung führt zur Erweiterung der Sphärenhypothese, nämlich, dass auch Daten zu schützen sind, die zwar nicht unmittelbar zur Intim- oder Privatsphäre einer Person gehören, aber zur Entwicklung eines Persönlichkeitsprofils beitragen.

(3) **Rollenhypothese:** Bei diesem Ansatz, der unabhängig von den anderen Hypothesen ist, tritt jeder Mensch in verschiedenen Rollen auf und gibt in diesen jeweils rollenspezifische Daten von sich preis. Eine Trennung zwischen intimer und öffentlicher Sphäre existiert dann nicht, „sondern es gibt verschiedene ‚Bilder', deren Sensibilität vom jeweiligen sozialen Interaktionspartner abhängt. Die Privatsphäre setzt sich aus den verschiedenen Bildern zusammen" (Egger und Schillinger 1996, S. 52). Aus diesem Modell

kann abgeleitet werden, dass alle personenbezogenen Daten eines Individuums prinzipiell schutzwürdig sind, was gängige Datenschutzgesetzgebung ist. Eine Entscheidung über die individuelle Preisgabe leitet sich aus dem Recht auf informationelle Selbstbestimmung ab.

Diese Datenschutzmodelle können auf den Umgang mit personenbezogenen Daten im Internet nicht übertragen werden, da die Begriffe Intim- und Privatsphäre in diesem Bereich nicht haltbar sind. Diese Entwicklung hat zur Folge, dass von Privatheit statt Privatsphäre gesprochen wird (vgl. Abschnitt 2.1.2).

Abschließend werden zwei Bezeichnungen vom Begriff *Datenschutz* differenziert. Während beim Datenschutz Personen die Objekte sind, deren Rechtsgüter gesichert werden sollen, was durch Datenschutzgesetze und vorgeschriebene technische und organisatorische Maßnahmen geschieht, sind bei der **Datensicherung** die Daten die Objekte, deren Inhalte es z. B. vor Manipulationen zu bewahren gilt. Durch Maßnahmen der Datensicherung wird **Datensicherheit** gewährleistet. „Die Datensicherheit … ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen." (Eckert 2013, S. 6)

2.1.2. Der Begriff der Privatheit und der Privatsphäre

Nach (Altman 1975, S. 18) ist **Privatheit** (**Privacy**)„the selective control of access to the self". Sie ist damit ein Optimierungs- und Regulationsprozess für den Zugang zur eigenen Person. Privatheit stellt nicht nur ein Recht auf Rückzug, sondern auch ein gesellschaftliches Gut dar, also die gesellschaftliche Teilhabe und trotzdem geschützt zu sein. „Privatheit bedeutet, dass Menschen mit ihrem Umfeld aushandeln, welche Informationen sie miteinander teilen wollen und welche nicht." Sie wird subjektiv wahrgenommen und dient der „Kontrolle über die persönliche Selbstoffenbarung" (Trepte et al. 2015a, S. 250). *Privatheit* und der Gegenpart *Öffentlichkeit* können als Pole eines Spektrums verstanden werden. Datenschutz (vgl. Abschnitt 2.1.1) wiederum ist die Implementierung eines Teils der Privatheit.

Davon abzugrenzen ist der Bereich (des juristisch geprägten Begriffs[34]) der **Privatsphäre**, die einen nicht-öffentlichen geschützten, individuell durchaus unterschiedlich abgegrenzten Raum darstellt. Ihre Funktion liegt in der Autonomie, der Selbstevaluation, der emotionalen Entlastung und der geschützten Kommunikation (Westin 2015, Pedersen 1997). Der Begriff bezieht sich auf das Sphärenmodell (vgl. Abschnitt 2.1.1), jedoch stößt es im Bereich der digitalen Kommunikation an seine Grenzen, da es im Digitalen keinen geschützten Raum mehr geben kann, weshalb innerhalb dieser Arbeit der Begriff nur begrenzt eingesetzt wird. In der Literatur werden zudem inkorrekterweise vereinzelt die Begriffe *Privatheit* und *Privatsphäre* nicht sauber voneinander getrennt.

[34] Ziel der Begriffsbildung ist, eine Skalierung der Begriffe *Intimsphäre*, *Privatsphäre* und *Öffentlichkeitsphäre* zu ermöglichen.

(Burgoon 1982) unterscheidet vier Dimensionen der Privatheit. In der **psychischen Dimension** steckt die Möglichkeit, Gefühle und Gedanken zu kontrollieren und mit anderen zu teilen. Die **physische Dimension** beschreibt die Möglichkeit der Zugangskontrolle zum eigenen Körper oder zu eigenen Räumlichkeiten. Mit der **sozialen Dimension** wird die Möglichkeit ausgedrückt, sich von sozialen Interaktionen zurückzuziehen oder diese zu kontrollieren. In der **informationalen Dimension** wird die Kontrollmöglichkeit über das Sammeln und das Weiterverarbeiten von Informationen und damit auch das Teilen dieser gesehen. Der letzte Aspekt spielt für die weiteren Betrachtungen eine Rolle.

Durch den Regulationsprozess bemühen sich Menschen einen Soll-Zustand zu erreichen, der nicht zwangsläufig mit dem Ist-Zustand übereinstimmt (Altman 1975). Dies wird im Zusammenhang mit einer informationalen Dimension der Privatheit im sogenannten **Privacy Paradox** beobachtet. „Das Privacy Paradox beschreibt die Diskrepanz zwischen den eigenen Einstellungen zum Umgang mit Privatheit im Internet und dem Privatheitsverhalten bei der Internetnutzung“ (Trepte und Teutsch 2016, S. 372).[35]

Als Gründe für dieses Verhalten werden fünf Hypothesen in der Literatur diskutiert (Trepte et al. 2015b). Die **Gratifikationshypothese** geht von einer Belohnung in Form sozialer Unterstützung oder Selbstdarstellung aus, wobei die Gratifikation höher als das mögliche Risiko eingeschätzt wird.[36] Der **Wissens- oder Kompetenzhypothese** liegt die Annahme zugrunde, dass nur ein geringes bis gar kein Wissen über Geschäftspraktiken und das Recht auf informationelle Selbstbestimmung vorliegt.[37] Bei der **sozialen Erwünschtheit-Hypothese** geht man davon aus, dass Internetnutzer einem gesellschaftlichen Druck nachgeben, „Privatheit als gängige Norm im Internet zu akzeptieren“ (Trepte und Teutsch 2016, S. 373). Sorgen um die Privatheit im Internet werden bei einer Befragung zwar angegeben, die Befragten empfinden jedoch keine Bedrohung und verhalten sich dementsprechend sorglos.[38] In (Masur 2014, S. 26) wird die sogenannte **Medienwirkungshypothese** aufgezählt. Werden datenschutzrelevante Ereignisse in Print- oder Online-Medien thematisiert, so wird durch die Medienberichterstattung eine öffentliche Meinung gebildet, die wiederum Auswirkungen auf das Privatheitsbedenken hat. Damit wird nicht die eigene Meinung, sondern ein Spiegel der medialen Wirklichkeit wiedergegeben. Die **Erfahrungshypothese**, beschrieben in (Trepte et al. 2014a), geht davon aus, dass die Nutzer Informationen von sich preisegeben, da sie noch keine schlechten Erfahrungen gemacht haben.

[35] 62 % der Deutschen sind bei der Internetnutzung um ihre Privatsphäre und 69 % über die Aufzeichnung des Surfverhaltens durch Webseitenanbieter besorgt; demgegenüber geben aber 79 % der europäischen Nutzer Sozialer Netzwerke ihren Namen an und 52 % deutscher Nutzer posten wöchentlich Kommentare und Statusupdates (Masur 2014, S. 15).

[36] Gratifikationen sind beispielsweise soziale Anerkennung, soziale Unterstützung, Selbstdarstellung und Realitätsflucht (Masur et al. 2014); zu den Vorteilen, die Nutzer in der Benutzung Sozialer Netzwerke sehen, siehe (Masur 2014, S. 19).

[37] Es betrifft insbesondere Datenschutzwissen über technische Aspekte, über Strategien und über die Gesetzeslage und Wissen über institutionelle Praktiken (Masur et al. 2017).

[38] Vgl. hierzu in Abschnitt 2.3.2 das Projekt *Privatheit im Wandel*.

Verschiedene empirische Studien sind zum Privacy Paradox durchgeführt worden (z. B. (Trepte und Teutsch 2016), (Norberg et al. 2007))[39]. Ein direkter Zusammenhang zwischen Privatheitsverhalten und Privatheitsbedenken konnte nicht festgestellt werden, aber die Untersuchung von Randbedingungen und die Identifikation von Drittvariablen zeigen, dass es durch Letztere einen Einfluss auf Einstellungen und Verhalten gibt. Andererseits existieren auch gegenteilige Studien. „In diesen Untersuchungen zeigte sich, dass Privatheit und Datenschutz betreffende Bedenken durchaus einen direkten Einfluss auf die Selbstoffenbarung der Nutzer haben“ (Trepte und Teutsch 2016, S. 374). Daher wird auch an den Studien Kritik geübt, die von falschen Annahmen und Zusammenhängen ausgehen. Des Weiteren wird in einigen Fällen die Operationalisierung als kritisch angesehen. (Dienlin und Trepte 2015) berichten von einer Untersuchung zur Überprüfung des Privacy Paradox. Wenn die Analyse den früheren Durchführungen entspricht, ist das Phänomen noch erkennbar. Wird aber zwischen Datenschutzbedenken und Einstellungen zum Datenschutz unterschieden, das *theory of planned behavior* als theoretisch orientiertes Modell zur Operationalisierung des Forschungsdesigns verwendet und werden die Datenschutzdimensionen differenziert (informativ, sozial, psychologisch), dann kann das Privacy Paradox nicht nachgewiesen werden. Somit ist das Ergebnis der Studie, dass das Verhalten der Online-Privatsphäre nicht paradox ist, sondern auf unterschiedliche Einstellungen zum Datenschutz beruht. Daher wird in der aktuellen Forschung an diesen Problemen und Annahmen weiter gearbeitet (vgl. 2.3).

„Die Präsentation des Privaten in der Öffentlichkeit ist im Internet zu einem Massenphänomen geworden, was von einer gänzlich veränderten Einstellung zur Privatsphäre zeugt“ (Wagner 2010, S. 558). Dass es im Laufe der Geschichte eine Verschiebung der Grenze zwischen Öffentlichkeit und Privatheit gab bzw. gibt, ist gesellschaftlich normal, da das Verhältnis immer neu austariert wird. „Das Irritierende an der Vernachlässigung des Privaten ist jedoch, dass sie offenbar zu einem guten Teil auf einem Missverständnis und zu einem anderen Teil auf Unkenntnis beruht“ (Wagner 2010, S. 558). Insofern muss die Behandlung des Themas *Datenschutz*, wie auch in (Wagner 2012) gefordert, sachlogisch eine Aufgabe der Schule sein.

2.1.3. Der Begriff des Vertrauens

Der Begriff ***Vertrauen*** ist ein alltäglicher Begriff[40]. Sobald ein bestimmtes Maß an Ungewissheit eine Rolle spielt, sind Handlungen und Folgeerscheinungen vom Nutzer nicht mehr vollständig steuerbar. Er vertraut dann auf Dritte (oder auch auf die Umgebung) und ist angewiesen auf das Wohlverhalten anderer. Vertrauen setzt darauf, dass die Erwartungen einen positiven Ausgang für einen selbst haben werden. Vertrauen kann sich auf verschiedene Faktoren beziehen: (a) in das Verhalten einer Person oder (b) in die Funktion eines Gegenstandes oder (c) in eine Umgebung (z. B. Familie oder eigene Wohnung). Menschen unterscheiden sich in

[39] Siehe dazu auch Abschnitt 2.3.

[40] Vertrauen = festes Überzeugtsein von der Verlässlichkeit, Zuverlässigkeit einer Person, Sache; Vertraulichkeit = Vertraulichsein, Diskretion, Vertrautheit // Quelle: www.Duden.de (zuletzt geprüft am 02.09.19)

ihrer Vertrauensneigung und „diese Unterschiede [sind] ein Produkt sowohl von genetischer Veranlagung als auch von Sozialisationserfahrungen“ (Grimm et al. 2015, S. 286).

In (Grimm und Bräunlich 2015) wird Vertrauen definiert „als eine Bereitschaft des Trustors [des Vertrauensnehmers], eine riskante Handlung in einem Kontext zu unternehmen, die er nicht vollständig kontrolliert, in der Erwartung, dass der Trustee [der Vertrauensgeber] diesen kontrolliert und den Trustor darin schützt.“ (Grimm und Bräunlich 2015, S. 289)

Anwendung von Vertrauen findet sich aus theoretischer Sicht in den Vertrauensmodellen. In (Grimm 2008) werden Beschreibungselemente für Modelle und ausgewählte Beispiele vorgestellt. Eine praktisch orientierte Anwendung ist z. B. *Trusted-Third-Party*[41] im Bereich E-Commerce (z. B. *PayPal*[42] und PK-Trustcenter).

Das Zusammenspiel zwischen Trustor und Trustee wird durch das Modell von Mayer, Davis und Schoorman beschrieben, welches in Abschnitt 3.2 vorgestellt wird.

Bei der Vertraulichkeit von Daten stehen an erster Stelle die Inhalte; aber auch ein „Schutz vor aller unautorisierter Informationsgewinnung“ gilt es zu beachten. „Man kann die Informationsvertraulichkeit daher auf folgende Bereiche beziehen: Dateninhalte …, Datensteuerung …, Kommunikationsbeziehungen [, und] … Kommunikationsverhalten“ (Grimm 2015, 129f).

Datenschutz und Vertraulichkeit sind zwei ganz unterschiedliche Grundbegriffe, die aber in einem engen Zusammenhang stehen. Die Aspekte, die durch die Prinzipien des Datenschutzes (vgl. Abschnitt 2.1.1) charakterisiert sind, verlangen Vertraulichkeit. In Artikel 5 (1) a) DSGVO wird die Verarbeitung „nach Treu und Glauben“ gefordert. Dies zeigt, dass die Vertraulichkeit eine notwendige Voraussetzung für Datenschutz ist.

2.1.4. Der Begriff der Sicherheit

Der Oberbegriff ***Sicherheit*** ist ein umfassender Begriff, der differenziert zu betrachten ist. Eckert definiert: „Unter **Funktionssicherheit** (engl. *safety*) eines Systems verstehen wir die Eigenschaft, dass die realisierte Ist-Funktionalität der Komponenten mit der spezifizierten Soll-Funktionalität übereinstimmt. Ein funktionssicheres System nimmt keine funktional unzulässigen Zustände an“ (Eckert 2013, S. 6). Es ist somit die Sicherheit von Mensch und Umgebung vor Systemfehlern und -ausfällen.

Dem gegenüber steht die Informationssicherheit. „Die **Informationssicherheit** (engl. *security*) ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen“ (Eckert 2013, S. 6). Mit diesem Begriff wird die Sicherheit von IT-Systemen und ihrer Umgebung vor Bedrohungen und Angriffen verstanden.

[41] Eine gute Beschreibung zu *Trusted-Third-Party* findet sich in (Grimm et al. 2015, S. 287f).
[42] Siehe https://www.paypal.com/de/home

(Eckert 2013) definiert weiter: „Die **Datensicherheit** (engl. *protection*) ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keinem unautorisiertem Zugriff auf Systemressourcen und insbesondere auf Daten führen. Damit umfasst die so beschriebene Sicherheit der Daten insbesondere auch Maßnahmen zur Datensicherung …, also den Schutz vor Datenverlusten durch Erstellung von Sicherungskopien“ (Eckert 2013, S. 6).

Zusammenfassend kann definiert werden: „**Sicherheit** ist die Eigenschaft eines Systems, die dadurch gekennzeichnet ist, dass die als bedeutsam angesehenen Bedrohungen, die sich gegen die schützenswerten Güter richten, durch besondere Maßnahmen [Sicherheitsmaßnahmen] soweit ausgeschlossen sind, dass das verbleibende Risiko akzeptiert wird“ (Grimm et al. 2016, S. 2).

„Sicherheit [ist somit] keine absolute Eigenschaft …, sondern [muss] stets relativ zu den spezifizierten Anforderungen bewertet werden“ (Eckert 2013, S. 716). Den ganzen Betrachtungen muss daher eine Sicherheitsstrategie zugrunde gelegt werden. Der erreichbare Grad an Sicherheit wird durch die Sicherheitsanforderungen bzw. einem Sicherheitsregelwerk[43] bestimmt, wobei auf eine sehr präzise Formulierung zu achten ist. Allgemeine Sicherheitsgrundfunktionen helfen dabei, Klassen von Anwendungen mit ähnlichen Sicherheitsbedürfnissen zusammenzufassen. Dadurch kann man ähnlich einem Baukastensystem, Grundfunktionen nach den eigenen Bedürfnissen miteinander kombinieren.

Nachdem die Sicherheitsanforderungen spezifiziert sind, ist ein Sicherheitsmodell so zu erstellen, dass geforderte sicherheitsbezogene und funktionale Eigenschaften erfüllt sind. Ein besonderes Modell stellt das Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse dar, welches in Abschnitt 3.3 genauer vorgestellt wird.

Wenn mindestens zwei Parteien miteinander kommunizieren, die jede für sich unterschiedliche Schutzziele verfolgt, die zwangsläufig nicht konträr sein müssen, dann sprechen (Pfitzmann et al. 2000, S. 5) von **mehrseitiger Sicherheit**. Es geht darum, dass alle Interessen aller (unterschiedlichen) Parteien berücksichtigt werden. Ein Beispiel dafür wäre ein E-Commerce, bei dem der Kunde möglichst wenig von sich an den Händler preisgeben möchte, aber der Händler auf der anderen Seite die Sicherheit hat, dass eine widerrechtliche Nutzung des Contents ausgeschlossen ist.

Die wichtigsten Sicherheitsanforderungen werden durch das sog. **C-I-A-Triangle** definiert. Dazu zählen die Vertraulichkeit (engl. *confidentiality*), die Integrität (engl. *integrity*) und die Verfügbarkeit (engl. *availability*). Eine nähere Beschreibung findet sich in (Eckert 2013, S. 7).

[43] Regelwerke sind Kriterienkataloge, die ein Bewertungsschema beschreiben, um die Vergleichbarkeit der Sicherheit ähnlicher Systeme sicherzustellen. Dabei definieren sie ein Maß und dienen „als Leitlinie zur Entwicklung und Konstruktion sicherer Systeme“ (Eckert 2013, S. 233). Ein Beispiel für ein solches Regelwerk ist das *Common Criteria for Information Technology Security Evaluation* (CC) zur Evaluierung und Zertifizierung von Produkten.

2.1.5. Der Kompetenzbegriff und Kompetenzmodelle

Der zweite tragende Begriff in dieser Arbeit ist der Kompetenzbegriff. Weinert definiert **Kompetenz** als „die bei Individuen verfügbaren oder durch sie erlernbaren kognitiven Fähigkeiten und Fertigkeiten, um bestimmte Probleme zu lösen, sowie die damit verbundenen motivationalen, volitionalen und sozialen Bereitschaften und Fähigkeiten, um die Problemlösungen in variablen Situationen erfolgreich und verantwortungsvoll nutzen zu können“ (Weinert 2002, S. 27).[44]

Im Zusammenhang mit Kompetenzen steht häufig der Begriff der **Schlüsselkompetenzen**. (Dörge 2012) ist im Rahmen ihrer Dissertation informatischen Schlüsselkompetenzen nachgegangen und stellt bei der Begriffsbestimmung fest, dass der Begriff *Schlüsselkompetenz*[45] wissenschaftlich nicht einheitlich definiert ist. Der Begriff wird eher als intuitiv angesehen. Jemand besitzt einen „Schlüssel“, um sich damit weitere Kompetenzen anzueignen (Dörge 2012, 11 & 114).

Neben Schlüsselkompetenzen wird auch der Begriff der **Basiskompetenzen** in der wissenschaftlichen Literatur genutzt. „Der Begriff der Basiskompetenzen wird in der internationalen Diskussion einerseits für Minimalanforderungen in Bildungsstandards und andererseits für untere Stufen eines Kompetenzmodells verwendet (vgl. Klieme et al. 2007, S. 100). Die jeweilige Grenze zwischen Basiskompetenzen und weiteren Kompetenzen wird im Allgemeinen von Expertengremien getroffen. Sie ist meist dadurch begründet, dass Schüler einer Risikogruppe zugeordnet werden, die beispielsweise den angestrebten Schulabschluss oder eine Berufsausbildung vermutlich nicht erreichen wird, wenn sie die Minimalanforderungen nicht erfüllen“ (Stechert 2009, S. 19).

Unter dem Begriff *Kompetenz* werden unterschiedliche Phänomene und Merkmale zusammengefasst.[46] Problematisch für Untersuchungen ist, dass sie nicht direkt messbar sind, sondern zu Teilen aus Äußerungen und Handlungen erschlossen werden müssen (Gapski 2006, S. 15). Im Berufsbildungsdiskurs werden unter anderem Kompetenztests, Kompetenzzertifikate, Kompetenzbilanzen und Kompetenzportfolio genutzt, um Kompetenzen zu erfassen oder sichtbar zu machen.

Im Rahmen der Kompetenzbegriffsbildung hat sich ein Kreis von grundlegenden Kompetenzen herausgebildet, der heute in der Wissenschaft als anerkannt gilt. Es wird hier zwischen soge-

[44] Diese Definition gilt inzwischen als wissenschaftlich anerkannt, wenn auch der Kompetenzbegriff seinen Ursprung rund 30 Jahre früher hat.
[45] Gerne wird auch der Begriff *Schlüsselqualifikation* genutzt.
[46] Im OECD-Bericht 2005 ist vermerkt: „Eine Kompetenz ist mehr als nur Wissen und kognitive Fähigkeiten. Es geht um die Fähigkeit der Bewältigung komplexer Anforderungen, indem in einem bestimmten Kontext psychosoziale Ressourcen (einschließlich kognitive Fähigkeiten, Einstellungen und Verhaltensweisen) herangezogen und eingesetzt werden“ (Gapski 2006, S. 16).

nannten Fachkompetenzen, Methodenkompetenzen, Sozialkompetenzen und Selbstkompetenzen unterschieden. Definitionen dieser sich fast schon selbsterklärenden Begriffe sind z. B. in (Gesellschaft für Informatik e. V. 2000, IV) zusammengefasst.

Auf Basis der Weinert-Definition des Kompetenzbegriffs sind **Kompetenzmodelle** zu unterschiedlichen Themen in vielen wissenschaftlichen Disziplinen entwickelt worden. Die Kompetenzmodelle bilden dabei die Grundlage zur Definition und Beschreibung der jeweiligen Kompetenzen, sodass Teildimensionen unterschieden werden können. Dadurch machen sie z. B. informatische Kompetenzen und deren Aufbau vorstellbar, vermittelbar, umsetzbar und diskutierbar.

„Kompetenzmodelle konkretisieren die Kompetenzbeschreibungen (Klieme et al. 2007, S. 9) und vermitteln wissenschaftlich fundiert zwischen Bildungszielen und konkreten Lehr-Lernprozessen. Ein Kompetenzmodell umfasst normative Vorgaben und empirische Validierung. Operationalisierte Kompetenzen unterscheiden sich von operationalisierten Lernzielen im Wesentlichen nicht in der Formulierung, sondern durch ihren theoretischen Hintergrund, d. h. ein Kompetenzmodell“ (Stechert 2009, S. 19).

(Friedrich 2003) hat z. B. ein Stufenmodell für informatische Kompetenzen entwickelt (vgl. Abb. 2.2). Dabei lehnt er sich an die Modelle der PISA-Studie an und benutzt die GI-Leitlinien (Gesellschaft für Informatik e. V. 2000), in denen unter dem Aspekt *Wechselwirkungen zwischen Informatiksystemen, Mensch und Gesellschaft* der Punkt *Ethische und rechtliche Aspekte* genannt ist. Das Thema *Datenschutz* setzt an dieser Stelle der Leitlinien an.

Informatische Kompetenz	**Interaktion**	**Wirkprinzipien**	**Modellierung**	**Wechselwirkung**
	Problemlösung	*Konzepte*	*Abstraktion*	*Allgemeinbildung*
Stufe I	Bedienung von Informatikanwendungen			
Stufe II	Benutzung von Informatiksystemen			
Stufe III	Kenntnis fachsystematischer Grundlagen			
Stufe IV	Verständnis von Konzepten der Informatik			
Stufe V	Entwicklung und Bewertung von Informatiksystemen			

Abb. 2.2: Stufenmodell für informatische Kompetenzen (Friedrich 2003, S. 126)

In Stufe III formuliert Friedrich als eine Kompetenz „Notwendigkeit des verantwortungsbewussten Umgangs mit Daten“, in Stufe IV „Beurteilung von Auswirkungen des Einsatzes von Informatiksystemen, besonders hinsichtlich deren Möglichkeiten und Grenzen“ und in Stufe V „Bewertung des Einsatzes von Informatiksystemen, hinsichtlich deren Möglichkeiten und deren Grenzen sowie der Beachtung deren gesellschaftlicher Dimension“ (Friedrich 2003, 128f). In diesem Kompetenzmodell sind also schon Aspekte enthalten, die eine Richtung von Datenschutzkompetenz aufzeigen, aber der Begriff ist explizit noch nicht erwähnt.

Ein Kompetenzmodell einer informatischen Allgemeinbildung stammt von (Koubek 2005b). Hier gibt es zwei getrennte Kompetenzstufungen, wobei die Eine technische Kompetenzen im Blick hat, während die Andere soziokulturelle Themen vereint. Im Unterricht sind letztendlich beide Kompetenzstufungen zu kombinieren. Jedoch schweigt der Autor sich aus, wie diese Stufungen zu verbinden sind. Er betont aber, dass die letzten Ebenen der jeweiligen Stufungen nur in Kombination miteinander erreicht werden können. Bemerkenswert an diesem Modell ist, dass durch den Aspekt soziokultureller Themen das Thema *Datenschutz* als informatische Allgemeinbildung gilt.

Ein anderes Kompetenzmodell für die Informatik stammt von (Fuchs und Landerer 2005), in denen unter dem Aspekt *Systemkompetenz* der Punkt *Sicherheit und Auswirkungen von (vernetzten) Informatiksystemen* und unter dem Aspekt *Anwendungskompetenz* der Punkt *Kommunikation und Wissensorganisation mit Informatiksystemen* genannt sind. Auch hier ist, wie im Fall von Friedrich, die Richtung für Datenschutzkompetenz angedacht, aber es findet sich keine Ausformulierung in diese Richtung. Dabei nutzen Fuchs und Landerer unter anderem den **informationsorientierten Ansatz** aus (vgl. (Hubwieser und Broy 1997), (Breier und Hubwieser 2002), (Breier 2005), (Hubwieser 2007)), der einen Ansatz neben vielen anderen didaktischen Ansätzen darstellt. Die Idee hierbei ist, die Information als weitere Grundgröße neben Materie und Energie zu betrachten und den Begriff der *Information* und den Umgang damit, in den Mittelpunkt der didaktischen Betrachtungen zu stellen. Das Paradigma der Informationsverarbeitung steht dabei im Vordergrund, denn „Informatik widmet sich der automatischen Informationsverarbeitung“ (Breier 2005, S. 70). Hieraus lässt sich der Begriff der Informationskompetenz ableiten, denn „Information ist … nicht nur eine der drei Grundgrößen, um die uns umgebende Welt zu beschreiben, sondern zugleich das wesentliche Element, um gesellschaftliche Probleme zu erfassen“ (Breier 2005, S. 71).

(Dörge 2012) hat in ihrer Dissertation über informatische Schlüsselkompetenzen einen Katalog von Kompetenzen auf der Basis von Fachdidaktikbüchern abgeleitet und dabei auch den Begriff der **Informationskompetenz** definiert. Sie versteht darunter „die Fähigkeit, nach der Idee des informationszentrierten Ansatzes agieren zu können, sowie das Erlernen des kompetenten Umgangs mit Informationen ... Dieser Punkt wird, neben ‚*Lesen, Schreiben und Rechnen*‘, von der ‚Erfurter Resolution‘ als Kulturtechnik gefordert“ (Dörge 2012, S. 214)[47]. Im weiteren Verlauf der Arbeit hat sie durch Literaturrecherche Auswertungen zum anwendungsorientierten Ansatz, zum benutzerzentrierten Ansatz und zum systemzentrierten Ansatz herausgearbeitet (Dörge 2012, S. 407, 424, 438).

Unter dem Titel *Relevanz von Informationskompetenz als Lerngegenstand* referierte Wolfgang Stock bei der 10. Tagung des wissenschaftlichen Beirats des Deutschen Philologenverbands am 10. Oktober 2017 in Göttingen und sagte dort, dass die „Informationskompetenz die grundlegende Kompetenz im 21. Jahrhundert“ sei (Langer 2017, S. 13). Zur Stoffvermittlung schlug er „ den Zugang zu Informations- und Kommunikationstechniken, zu Information und Wissen, Informationsethik und -recht, Privatheit [und] Informationsmarkt“ vor (Langer 2017,

[47] Zur *Erfurter Resolution* siehe (Schubert und Schwill 2011, S. 39).

S. 14). Bemerkenswert ist, dass der Referent von dem Begriff *Privatheit* spricht (vgl. Abschnitt 2.1.2). Er ging sogar so weit, dass er für ein Fach *Informationskompetenz* ab einem Alter von 13 Jahren plädierte. Dies zeigt die Notwendigkeit, dass sich Schüler frühzeitig mit Fragen rund um das Thema *Datenschutz* beschäftigen müssen.

Eine ausführliche Darstellung zum Thema *Kompetenzbegriff und Kompetenzmodell* findet man in (Klieme 2004).

2.2. Relevanz und Legitimation des Themas *Datenschutz* als Unterrichtsthema

Die Legitimation eines zu behandelnden Unterrichtsthemas erfolgt in der Regel im Rahmen der didaktischen Analyse[48] einer Stunde. Demzufolge muss sich ebenfalls das Thema *Datenschutz* legitimieren lassen, damit es als ein Unterrichtsthema fungieren kann. Die Legitimation erfolgt dabei einerseits auf der Grundlage von ministeriellen Rechtsvorschriften und ähnlichen Dokumenten, die Kompetenz- und Inhaltsbeschreibungen zum (Informatik-)Unterricht liefern, und andererseits auf Basis von wissenschaftlichen Modellen zur Beschreibung von Kompetenzen und informatischen Inhalten.

Aufgrund der Vielzahl an unterschiedlichen Schulformen und Lehrplänen in Deutschland schränkt der Autor sich – sofern notwendig – bei allen Betrachtungen auf das Bundesland Rheinland-Pfalz ein, in dem auch die in Kapitel 4 beschriebene Erhebung stattgefunden hat.

2.2.1. Standards zur informatischen Bildung

Für das Fach *Informatik* hat *die Ständige Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland* (*KMK*) – im Gegensatz zu Mathematik, Deutsch, modernen Fremdsprachen und Naturwissenschaften – keine Bildungsstandards herausgegeben. Ein Hauptgrund dürfte sein, dass Informatik nur in Sachsen, Sachsen-Anhalt, Mecklenburg-Vorpommern, Baden Württemberg und Bayern ein Pflichtfach ist, dessen Ausgestaltung (Anzahl der Unterrichtsstunden, Verteilung der Stunden auf die Jahrgangsstufen, …) aber sehr unterschiedlich ist[49]. Würde die KMK Bildungsstandards beschließen, dann müsste das Fach in allen

[48] Eine didaktische Analyse umfasst neben der Legitimation auch Betrachtungen zur Relevanz des Unterrichtsthemas, zur Interdependenz der Stunde im Rahmen der Unterrichtseinheit und die didaktischen Bemerkungen (Zugänge zum Thema, sachlogischer Aufbau der Stunde, Lernschwierigkeiten, …).

[49] Es gibt Bundesländer, in denen informatische Inhalte integrativ in anderen Fächern, z. B. Technik, unterrichtet werden. In einigen Bundesländern, wie z. B. Thüringen, wird das Thema Datenschutz im Rahmen der sog. *Medienkunde* behandelt (Bethge et al. 2011). Durch diese Implementierung sollen informatische Themen in die Schule eingebracht werden, da die Einrichtung eines Pflichtfachs Informatik seitens der Politik (noch) nicht vorgesehen ist. Nach der Pressemitteilung vom 17.09.19 wird Informatik in Nordrhein-Westfalen in der Orientierungsstufe Pflichtfach (vgl. https://gi.de/meldung/gi-begruesst-geplante-einfuehrung-des-pflichtfachs-informatik-in-nrw/, zuletzt geprüft am 03.10.19).

Bundesländern als Pflichtfach eingeführt werden. Daher ist der Herausgeber der Bildungsstandards für das Fach *Informatik* die *Gesellschaft für Informatik e. V.* (*GI*)[50]. Es existieren Standards für den mittleren Schulabschluss (Sekundarstufe I) (Gesellschaft für Informatik e. V. 2008) und den höheren Schulabschluss (Sekundarstufe II) (Gesellschaft für Informatik e. V. 2016), wobei letztere als Ablösung der *Einheitlichen Prüfungsanforderungen Abitur* (*EPA*) Informatik gedacht, aber von der KMK nicht verabschiedet sind. Diese von den Bundesländern unabhängigen Standards wurden in der Fachcommunity sehr gut angenommen und dienen in vielen Bundesländern als Grundlage für die Entwicklung von Lehrplänen und Curricula.

Innerhalb der Bildungsstandards für die Sekundarstufe I kann das Thema *Datenschutz* in folgenden Inhaltsbereichen verortet werden (vgl. Tab. 2.1):

Inhaltsbereich	**Kompetenz: Schülerinnen und Schüler …**
3: Sprachen und Automaten	3.1: nutzen formale Sprachen zur Interaktion mit Informatiksystemen und zum Problemlösen.
4: Informatiksysteme	4.2: wenden Informatiksysteme zielgerichtet an.
5: Informatik, Mensch und Gesellschaft	5.1: benennen Wechselwirkungen zwischen Informatiksystemen und ihrer gesellschaftlichen Einbettung.
	5.2: nehmen Entscheidungsfreiheiten im Umgang mit Informatiksystemen wahr und handeln in Übereinstimmung mit gesellschaftlichen Normen.
	5.3: reagieren angemessen auf Risiken bei der Nutzung von Informatiksystemen.

Tab. 2.1: Ausgewählte Kompetenzen der Inhaltsbereiche Bildungsstandards Sek. I (Gesellschaft für Informatik e. V. 2008, S. 16)

Insbesondere im Inhaltsbereich *Informatik, Mensch und Gesellschaft* sind konkret ausformulierte Kompetenzen benannt. Dort heißt es: „Die Schülerinnen und Schüler

- „beachten Umgangsformen bei elektronischer Kommunikation und achten auf die Persönlichkeitsrechte anderer“ (5.2 für Klassenstufe 5 – 7),
- „wenden Kriterien an, um Seriosität und Authentizität von Informationen aus dem Internet zu beurteilen, beschreiben an ausgewählten Beispielen, wann und wo personenbezogene Daten gewonnen, gespeichert und genutzt werden, bewerten Situationen, in denen persönliche Daten weitergegeben werden, erkennen die Unsicherheit einfacher Verschlüsselungsverfahren“ (5.3 für Klassenstufe 8 – 10),
- „beurteilen Konsequenzen aus Schnelligkeit und scheinbarer Anonymität bei elektronischer Kommunikation“ (5.2 für Klassenstufe 8 – 10) (Gesellschaft für Informatik e. V. 2008, S. 18).

[50] Die KMK-Standards sind für die Schulen verbindlich, während die GI-Standards nur eine Empfehlung darstellen können; siehe www.gi.de (zuletzt geprüft am 03.10.19).

Im Rahmen der ausführlichen Erläuterungen des Inhaltsbereichs *Informatik, Mensch und Gesellschaft* für die Klassenstufe 8 bis 10 heißt es: „Informationelle Selbstbestimmung ist ein Persönlichkeitsrecht, das erst einmal als solches erkannt werden muss. Schülerinnen und Schüler werden daher dafür sensibilisiert, dass sie Daten unterschiedliche Qualitäten zuweisen, dass manche Daten für sie persönlich und daher schützenswert sind. Die Weitergabe personenbezogener Daten darf nur dann erfolgen, wenn dies gesetzlich geregelt ist oder der Betroffene ihr zustimmt“ (Gesellschaft für Informatik e. V. 2008, S. 44).

Innerhalb der Bildungsstandards für die Sekundarstufe II kann das Thema *Datenschutz* in folgenden Inhaltsbereichen verortet werden (vgl. Tab. 2.2):

Inhaltsbereich	**Kompetenz: Schülerinnen und Schüler …**
4: Informatiksysteme	4.5: analysieren die Kommunikation und die Datenhaltung in vernetzten Systemen und beurteilen diese auch unter den Gesichtspunkten des Datenschutzes und der Datensicherheit.
5: Informatik, Mensch und Gesellschaft	5.2: beschreiben Chancen, Risiken und Missbrauchsmöglichkeiten von Informatiksystemen.
	5.3: diskutieren und bewerten wesentliche Aspekte des Datenschutz- und Urheberrechts anhand von Anwendungsfällen.
	5.5: verwenden und beschreiben Verfahren zur Sicherung von Vertraulichkeit, Authentizität und Integrität von Daten.
	5.6: ziehen Rückschlüsse für das eigene Verhalten beim Einsatz von Informatiksystemen.
	5.7: *analysieren und beurteilen Verfahren zur Sicherung von Vertraulichkeit, Authentizität oder Integrität von Daten in konkreten aktuellen Anwendungskontexten.*
	5.8: *konzipieren Maßnahmen zur Realisierung von Datensicherheit für konkrete Anwendungsfälle, insbesondere Zugriffskontrolle*.

Tab. 2.2: Ausgewählte Kompetenzen der Inhaltsbereiche Bildungsstandards Sek II (Gesellschaft für Informatik e. V. 2016, 11f)
kursiv geschrieben = erhöhtes Anforderungsniveau

Da in den meisten Bundesländern Informatik (speziell in der Sekundarstufe I) kein Pflichtfach ist, die Standards aber aufeinander aufbauen, können bei der Behandlung des Themas *Datenschutz* die Inhalte auf verschiedene Jahrgangsstufen, insbesondere der Oberstufe, verteilt werden.

Abschließend soll angemerkt werden, dass die am 31.01.2019 vom GI-Präsidium verabschiedeten Bildungsstandards für den Primarbereich ebenfalls schon Kompetenzen benennen, die mit dem Thema *Datenschutz* in Beziehung stehen, auch wenn diese Standards für die weiteren Betrachtungen in dieser Arbeit keine Rolle spielen. Im Inhaltsbereich *Informatik, Mensch und Gesellschaft* lauten die Kompetenzen für die Klassenstufen 2:

„Die Schülerinnen und Schüler

- nennen Maßnahmen, um Daten vor ungewolltem Zugriff zu schützen.
- halten sich an Regeln im Umgang mit Daten und Informatiksystemen.
- erläutern, dass Daten personenbezogen sein können."

(Gesellschaft für Informatik e. V. 2019, S. 16)

Für die Klassenstufe 4 sind folgende Kompetenzen gelistet:

„Die Schülerinnen und Schüler

- ergreifen Maßnahmen, um Daten vor ungewolltem Zugriff zu schützen.
- entwickeln und bewerten Vereinbarungen im Umgang mit Daten und Informatiksystemen.
- erläutern, dass mit Informatiksystemen personenbezogene Daten gesammelt und verarbeitet werden können."

(Gesellschaft für Informatik e. V. 2019, S. 16)

Die Autoren dieser Standards weisen darauf hin, dass die Schüler schon frühzeitig durch Medien mit dem Thema *Datenschutz* in Berührung kommen, sodass eine frühzeitige Vorbereitung auf den Umgang mit persönlichen Daten von Vorteil ist.

2.2.2. Lehrpläne und Handreichungen

In Rheinland-Pfalz ist Informatik kein Pflichtfach[51]. An den Gymnasien und integrierten Gesamtschulen (IGS) kann es in der Sekundarstufe I als Wahl- oder Wahlpflichtfach angeboten werden. Dies ist Voraussetzung für das Angebot eines Leistungskurses in der gymnasialen Oberstufe[52], während das Grundkursangebot in fast allen Schulen mit dem höheren Schulabschluss gegeben ist. Für alle diese Fälle existieren Lehrpläne.

An der Realschule Plus kann im Rahmen des schuleigenen Wahlpflichtpflichtangebots Informatikunterricht angeboten werden, jedoch existiert für diesen Unterricht kein Lehrplan. Als Orientierung dient der Lehrplan für das *Wahl-/Wahlpflichtfach Informatik in der Sekundarstufe I für Gymnasien und integrierten Gesamtschulen*. Aber in jedem Fach werden innerhalb

[51] Mit dem Schuljahr 2020/21 werden in Rheinland-Pfalz die ersten 21 sogenannten Informatik-Profil-Schulen starten, an denen alle Schüler ab der Klassenstufe 5 an dem Pflichtfach Informatik teilnehmen werden. Somit ist hier ein erster Schritt in die Richtung Pflichtfach getan (vgl. https://informatik.bildung-rp.de/ips.html, zuletzt geprüft am 09.01.20).

[52] In Rheinland-Pfalz gibt es nur an 16 (von 151) Gymnasien und einer (von 55) IGS dieses Angebot (vgl. https://informatik.bildung-rp.de/sek2/schulen-mit-leistungsfach.html, zuletzt aufgerufen am 15.01.18).

des Wahlpflichtbereichs[53] Inhalte und Kompetenzen des Unterrichtsprinzips der *Informatischen Bildung* vermittelt, wozu es eine Handreichung[54] gibt. Ferner ist dieses Unterrichtsprinzip auch im Unterricht der IGS umzusetzen.

Die Berufsbildenden Schulen (BBS) werden aufgrund ihrer besonderen Struktur und Ausbildungsform im Folgenden nicht betrachtet.

2.2.2.1. Der Lehrplan Informatik

Im Abschnitt *Grundlagen der Informationsverarbeitung* des Lehrplans für die Sekundarstufe I wird schon darauf hingewiesen, dass „beim Umgang mit Informationen … z.B. Fragen des Urheberrechtes oder des Datenschutzes auftauchen [können], die durch Behandlung rechtlicher Rahmenbedingungen geklärt werden müssen“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2008a, S. 8).

Dies wird durch den Beitrag ergänzt, dass „durch Zusammenführen von Daten mit geeigneten Datenbankoperationen … sich leicht neue ‚brisante‘ Daten gewinnen [lassen], deren Interpretation auch missbräuchlich genutzt werden kann. Anhand der Datenschutzproblematik lässt sich so leicht aufzeigen, welche Auswirkungen der Einsatz von Informatiksystemen auf den Einzelnen haben kann“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2008a, S. 9).

Im Abschnitt *Nutzung und Modellierung von Datenbanken* werden folgende Lernziele formuliert:

- „Datenbanken nutzen und den Einsatz unter datenschutzrechtlichen Aspekten bewerten“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2008a, S. 23).
- „Dazu gehört Datenerhebungen unter dem Aspekt Datenschutz bewerten“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2008a, 23 + 25).

Die Thematik *Datenschutz* ist ebenfalls im Lehrplan der Sekundarstufe II vertreten. Dort heißt es im Abschnitt *Inhaltsbereiche und informatische Bildung*: „Während der Komplex ‚Wechselwirkungen zwischen Informatiksystemen, Individuum und Gesellschaft‘ im Leistungsfach mit einem eigenen Inhaltsbereich ausgewiesen ist, werden diese Aspekte im Grundfach in andere Inhaltsbereiche integriert: Der Umgang mit Informationen wirft in natürlicher Weise Fragen des Datenschutzes und des rechtlich einwandfreien Umgangs mit Daten auf. Besonders das Internet beeinflusst den Einzelnen und die Gesellschaft so stark, dass neben ethischen und rechtlichen auch Sicherheitsfragen erörtert werden müssen. Unzuverlässige Software kann

[53] Dieser besteht aus *Hauswirtschaft und Soziales*, *Technik und Naturwissenschaft* und *Wirtschaft und Verbraucherbildung*.

[54] Siehe https://informatik.bildung-rp.de/fileadmin/user_upload/informatik.bildung-rp.de/Informatische_Bildung/Handreichung_Informatische_Bildung_S_I_05-09-12.pdf (zuletzt geprüft am 15.01.18)

großen individuellen und gesellschaftlichen Schaden anrichten. Umgekehrt liegt in guter Software ein großes Potenzial zur Verbesserung der Lebensqualität. Im Umgang mit fertiger oder auch selbst erstellter Software lernen Schülerinnen und Schüler Chancen und Risiken der Informationstechnik fachlich fundiert einzuschätzen“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2008b, 9).

Im Grundfach innerhalb des Themenfelds *Informationen und ihre Darstellung* heißt es „Datenerhebungen unter dem Aspekt Datenschutz bewerten“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2008b, 16 + 20). Im Leistungsfach wird die Thematik innerhalb des Themenfelds *Wechselwirkungen zwischen Informatiksystemen, Individuum und Gesellschaft* aufgegriffen. Dort heißt es „Datenerhebungen unter dem Aspekt Datenschutz beurteilen“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2008b, 71 + 73).

2.2.2.2. Bezug des Themas *Datenschutz* zu anderen Fächern

Die Wissenschaft und das Schulfach *Informatik* stellen eine Grundlagenwissenschaft[55] dar. „Über den Begriff der Information ist … die Chance gegeben, eine Brücke zwischen naturwissenschaftlichen, sozialwissenschaftlichen, sprachlichen und technischen Fächern zu schlagen und fächerverbindendes und fachübergreifendes Lernen zu ermöglichen“ (Breier 2005, S. 71).

Das Thema *Datenschutz* ist ein Thema, welches sich hervorragend für einen fachübergreifenden oder fächerverbindenden Unterricht anbietet. Bei diesem Thema spielen neben der technischen Seite auch sozialwissenschaftliche Aspekte eine Rolle. „Dabei sollen im Besonderen Themen angesprochen werden, die die Jugendlichen im täglichen Umgang mit dem Internet und den Informations- und Kommunikationsmöglichkeiten der Neuen Medien wie selbstverständlich einsetzen“ (Gesellschaft für Informatik e. V. 2006, S. 9).

Ein Thema des Fachs *Sozialkunde* ist das der Gesetzgebung und der Gesetzausübung. Hiermit wird die juristische Seite des Datenschutzes berührt. Aber auch die Betrachtung des Themas auf EU-Ebene oder weltweit unter dem Einfluss entsprechender politischer Systeme können in diesem Fachunterricht aufgezeigt werden. Das Thema *Volkszählung 1983*, in dessen Zusammenhang das Grundrecht der informationellen Selbstbestimmung abgeleitet worden ist (vgl. Abschnitt 2.1.1), ist ein entscheidender Schritt gewesen, der zudem das Fach *Geschichte* berührt.

Die Frage nach *Sicherheitsstaat oder Rechtsstaat*, die schon im 17. Jahrhundert Thomas Hobbes und John Locke beschäftigt hat, ist ein Thema, mit welchem gleichzeitig die Fächer *Sozialkunde*, *Geschichte* und *Philosophie/Ethik* angesprochen werden (Weichert 2014, 16f).

Das Fach *Philosophie/Ethik* hat die Möglichkeit, sich dem Thema *Datenschutz* aus der moralisch-ethischen Sichtweise zu nähern: Was ist bzw. bedeutet Privatsphäre bzw. Privatheit?

[55] D. h. Informatik ist eine Wissenschaft, deren Erkenntnisse und Arbeitsweisen (Methoden) in anderen Wissenschaften Verwendung finden.

Darf, kann oder muss man Grenzen ziehen? Welche Rolle spielt dabei der Staat? Diese letzte Fragestellung berührt dann auch wieder das Fach *Sozialkunde*.

Ein gutes Beispiel für einen fachübergreifenden Ansatz im Fach *Deutsch* findet sich in dem Schulbuch *deutsch.kompetent.* für die Klassenstufe 8 (Bitterer et al. 2014, S. 38). Anhand des Beispiels *Videoüberwachung* wird das Leitthema *Schreiben einer Erörterung* behandelt. Die Romane *Little Brother* von *Cory Doctorow* und *1984* von *George Orwell* sind Beispiele aus der modernen Literatur, die sich inhaltlich mit dem Thema Überwachung und Überwachungsstaat und damit im weitesten Sinne auch mit Datenschutz beschäftigen. Ferner kann hier (wie auch in einem Fach wie *Sozialkunde*) von methodischer Seite hergesehen das Debattieren und Argumentieren geschult werden. Es bietet sich z. B. an, dass Schüler sich mit Themen wie *Überwachung*, die damit verbundene *Angst* oder *Rechtsstaat* in Form z. B. eines eigenen Gedichts auseinandersetzen.

Die oben genannten Romane können natürlich auch als Originalliteratur im Fremdsprachenunterricht *Englisch* behandelt werden. Im Rahmen der Länderkunde wäre zu erarbeiten, wie andere Staaten – vorneweg die USA mit der NSA – mit dem Thema *Datenschutz* umgehen.

Das Fach *Geschichte* wiederum hat in Anlehnung an das Fach *Sozialkunde* die Möglichkeit, unter einem historischen Blickwinkel den Datenschutz zu betrachten.

Innerhalb des Fachs *Mathematik* kann die Informationsgewinnung aus statistischen Daten thematisiert werden, das insbesondere im Zusammenhang mit Big Data von Interesse ist.

Die künstlerischen Fächer *Musik, Bildende Kunst* und *Darstellendes Spiel* können einen kreativen Beitrag dazu leisten. So wurde z. B. 2011 von dem Schlagersänger Udo Jürgens der Song mit dem Namen *Du bist durchschaut* aufgenommen, der die Problematik des Datenumgangs von *Facebook* anprangert[56]. Aber Schüler können auch selbst aktiv werden, in dem sie Bilder oder Collagen zu dem Thema *Datenschutz* entwerfen oder in Form eines Theaterstückes sich der Problematik nähern (z. B. Mobbing eines Mitschülers).

Die Biologie oder besser die Psychologie kann sich Fragen der Art widmen: Wie verhalten sich Menschen? Warum verhalten sie sich so? Warum sind sie risikobereit? Warum sind sie unterschiedlich? Gibt es Erklärungsansätze, die aus der Evolution begründet werden können?

Diese Auflistung zeigt, dass das Thema *Datenschutz* nicht ausschließlich als eine Aufgabe der Informatik gesehen werden muss. Selbstverständlich wird man niemals alle der oben genannten Ansätze verfolgen können, jedoch ist die Aufzählung als ein Ideenpool zu verstehen.

[56] Vgl. http://www.laut.de/Udo-Juergens/Alben/Der-Ganz-Normale-Wahnsinn-65394 (zuletzt aufgerufen am 09.02.2018)

2.2.2.3. Richtlinie zur Verbraucherbildung

Eine Besonderheit in Rheinland-Pfalz ist, dass seitens des 2010 fachlich zuständigen Ministeriums eine Richtlinie für die Verbraucherbildung herausgegeben worden ist (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2010). Neben den Themen *Finanzkompetenz und Konsum* und *Ernährung und Gesundheit* wird als drittes Thema *Datenschutz* vorgeschrieben. Diese Richtlinie gilt für die Primarstufe und gesamte Sekundarstufe I aller allgemeinbildenden Schulen, wobei jede Schule durch hausinterne Pläne festlegen soll, in welcher Jahrgangsstufe welche Themen in welchem Fach behandelt werden. Da es sich „nur" um eine Richtlinie handelt, hat sie im Vergleich zu den Lehrplänen der einzelnen Fächer nicht den verpflichtenden Charakter.

Diese drei Themenfelder wirken ineinander, denn Online-Handel z. B. erzeugt datenschutzrelevante Daten. Bei vielen Produkten aus der Ernährungsindustrie werden gerade die jüngeren Kinder auf den Verpackungen zum Besuch der firmeneigenen Webseite mit Gewinnversprechen oder ähnlichem aufgerufen. Auf diesem Weg besteht die Möglichkeit, dass Kinder personenbezogene Daten preisgeben, da sie noch überhaupt nicht in der Lage sind, das Ausmaß und die Notwendigkeit der Datenangabe zu erkennen. Allein die Tatsache, Webseiten zu besuchen, liefert dem Produktanbieter schon Informationen. Letztendlich spielen hier die Regeln der Werbepsychologie eine Rolle. Ein anderes Beispiel sind Fitnessbänder, die zu Vitalitätsmessungen herangezogen werden. Einerseits versprechen sie die eigene Kontrolle zum Wohl der Gesundheit, andererseits sind Krankenversicherungen an den Daten interessiert, um den Kunden maßgeschneiderte Tarife anzubieten (nach der Devise „Wer sich gesund verhält, zahlt weniger Beitrag")[57].

Unter dem Kernbereich *Datenschutz* ist das Bildungsziel *Datenschutz- und Datensicherheitsrisiken erkennen und minimieren* formuliert. Die Kompetenzbeschreibung lautet: „Die Schülerinnen und Schüler sind bereit und in der Lage,

- Datenschutz als Bürger- und Menschenrecht anzuerkennen.
- die Freiheit des Internets verantwortungsbewusst und selbstbestimmt wahrnehmen zu können.
- selbstbestimmt und verantwortungsvoll medial basiert zu kommunizieren.
- mit eigenen personenbezogenen Daten reflektiert umzugehen.
- personenbezogene Daten als ein wertvolles Gut zu betrachten."

Dies wird ergänzt durch die Inhalte:

- „Recht auf informationelle Selbstbestimmung
- Selbstdatenschutz
- Urheberrechte
- Communities/Social Networks

[57] Vgl. https://www.welt.de/gesundheit/article154004816/Wenn-die-Krankenkasse-Ihre-Fitness-App-mitliest.html (zuletzt geprüft am 17.07.19)

- Selbstdarstellung im Netz
- …“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2010, S. 30)

Zu Beginn der Richtlinie wird der Kernbereich *Datenschutz* begründet: „Aufgrund der technologischen, jugend-, arbeitsmarkt-, gesellschafts- und bildungspolitischen Veränderungen kommt der Förderung von Medien-, Informations-, Kommunikations- und Datenschutzkompetenz eine entscheidende Bedeutung zu. In diesem Zusammenhang spielen das Recht auf informationelle Selbstbestimmung, die Verantwortung im Umgang mit persönlichen Daten und die Fähigkeit, verschiedene Formen kommerzieller Inhalte und Kommunikation kritisch zu bewerten und zu analysieren, eine entscheidende Rolle“ (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2010, S. 14).

Obwohl es an der reinen Bedienungskompetenz bei Schülern im Rahmen der Nutzung digitaler Medien nicht mangelt, fehlt es an dem kritischen Umgang damit, sodass insbesondere die Erzeugung digitaler Spuren und deren Folgen nicht bewusst sind. Speziell die Privatsphäre ist durch bestimmte Internetdienste gefährdet. Den Themen *Selbstdatenschutz* und *Jugendrechte* muss daher ein entsprechender Raum im Unterricht geboten werden. Daneben müssen auch die Grundsätze der Datenvermeidung und Datensparsamkeit angesprochen werden. Letztendlich gilt es, auch die Verpflichtungen, die man gegenüber Anderen und deren persönlichen Daten hat, bei der Internetnutzung zu schärfen und das eigene Verhalten ethischen Ansprüchen zu erfüllen (Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) 2010, S. 14).

2.2.3. Das Konzept *Informationstechnische Grundbildung ITG*

In den 80er Jahren wurde das Konzept der *Informationstechnischen Grundbildung* (*ITG*) mit dem Ziel einer Einführung informationstechnischer Allgemeinbildung an Schulen entworfen. Die Idee war, dass dies integrativ in anderen Fächern geschehen soll, um eine flächendeckende Einführung eines Schulfachs *Informatik* zu „vermeiden“. Obwohl entsprechend geschulte Lehrkräfte zur Verfügung standen, ist die Umsetzung in der Praxis gescheitert. Die Gründe dafür waren vielfältig, wie z. B. die Frage nach dem Zeitansatz bei den ohnehin überfüllten Curricula, nach der Stoffverteilung auf die Fächer und des Einsatzes fachfremder Lehrer. (Humbert 2006) merkt dazu an, dass „als eine Ursache für diesen Misserfolg … die fehlende Fundierung der Konzepte in der Fachwissenschaft ausgemacht werden [kann]. Der Zielkonflikt zwischen einer abnahmeorientierten Bedienkompetenz und den fachlichen grundlegenden Prinzipien kann offenbar mit diesen Konzepten nicht aufgelöst werden“ (Humbert 2006, S. 56).

In dem 1987 verabschiedeten Rahmenkonzept heißt es unter Punkt 9: „Einführung in die Probleme des Persönlichkeits- und Datenschutzes“ (Bund-Länder-Kommission für Bildungsplanung und Forschungsförderung 1987, S. 12). Dies zeigt, dass die von (Koubek 2005b) geforderte

Allgemeinbildung – nämlich dass dazu nicht nur ein technischer, sondern auch ein sozialwissenschaftlicher Aspekt gehört – auch schon in die Überlegungen für die ITG aufgenommen worden ist.

Weitere Informationen zu dem Konzept findet man in (Schubert und Schwill 2011, 28f).

2.2.4. Datenschutz im Kontext Fundamentaler Ideen

Die fundamentalen Ideen der Informatik sind nach einem Ansatz von Schwill ein Denk-, Handlungs-, Beschreibungs- oder Erklärungsschema, die folgende Kriterien erfüllen: Horizontalkriterium, Vertikalkriterium, Zielkriterium, Zeitkriterium und Sinnkriterium (Schubert und Schwill 2011, 64f). Wenn ein Thema für den Unterricht eine Relevanz hat, dann sollte es sich an diesen Kriterien messen lassen.

Das Thema *Datenschutz* erfüllt das Horizontalkriterium weniger innerfachlich, als dass es ein Thema für den fachübergreifenden Unterricht darstellt (vgl. Abschnitt 2.2.2.2). Das Vertikalkriterium ist erfüllt, da das Thema je nach Alter auf verschiedenen Niveaustufen unterrichtet werden kann. Im Sinne des Spiralcurriculums hat dies auch den Sinn, dass das schon einmal Gelernte immer wiederholt und mit weiteren Themenaspekten altersgerecht vertieft wird. Dadurch ist ein höherer Lernerfolg am Ende zu erwarten. Im Zielkriterium wird die Erziehung der Schüler zu mündigen Bürgern ausgedrückt. Ein entsprechender Bürger muss zum einen seine Rechte in Bezug auf Datenschutz kennen, um sich an der gesellschaftlichen und politischen Diskussion beteiligen und entsprechend handeln zu können. Zum anderen muss er wissen, wie Firmen mit persönlichen Daten umgehen können und welche Möglichkeiten daraus erwachsen (Big Data und Data Mining). Das Thema *Datenschutz* ist seit den 70er Jahren des letzten Jahrhunderts ein öffentlich diskutiertes Thema geworden, welches insbesondere durch den Siegeszug des Internets zu einem hochbrisanten und aktuellen Thema wird. Eine begrenzte Gültigkeit des Themas ist nicht absehbar (Zeitkriterium). Die Bedeutung des Sinnkriteriums ist offensichtlich, da die Jugendlichen schon bei der Nutzung des Internets mit dem Thema Datenschutz in Berührung kommen, sodass der entsprechende Unterrichtsinhalt gut kontextorientiert unterrichtet werden kann.

Die Kriterien aus den fundamentalen Ideen zeigen, dass das Thema Datenschutz sich durchaus daran messen lässt, auch wenn es keine Masteridee darstellt, da es sich hierbei – im Gegensatz zu den anderen Masterideen – um kein allgemeines Prinzip handelt.

2.2.5. Datenschutz im Zusammenhang des Dagstuhl-Dreiecks und des Frankfurt-Dreiecks

In der im März 2016 von der *Gesellschaft für Informatik e. V.* veröffentlichten *Dagstuhl-Erklärung: Bildung in der digital vernetzten Welt*, an der Experten der Informatik-Didaktik und Medienbildung zusammengearbeitet haben, werden drei Perspektiven der digitalen Bildung (= Bildung in der digital vernetzten Welt) herausgearbeitet, die sich gegenseitig beeinflussen und daher ganzheitlich zu betrachten sind, um eine nachhaltige und strukturell verankerte digitale Bildung zu gewährleisten. Diese Perspektiven sind im sogenannten ***Dagstuhl-Dreieck*** festgehalten (vgl. Abb. 2.3).

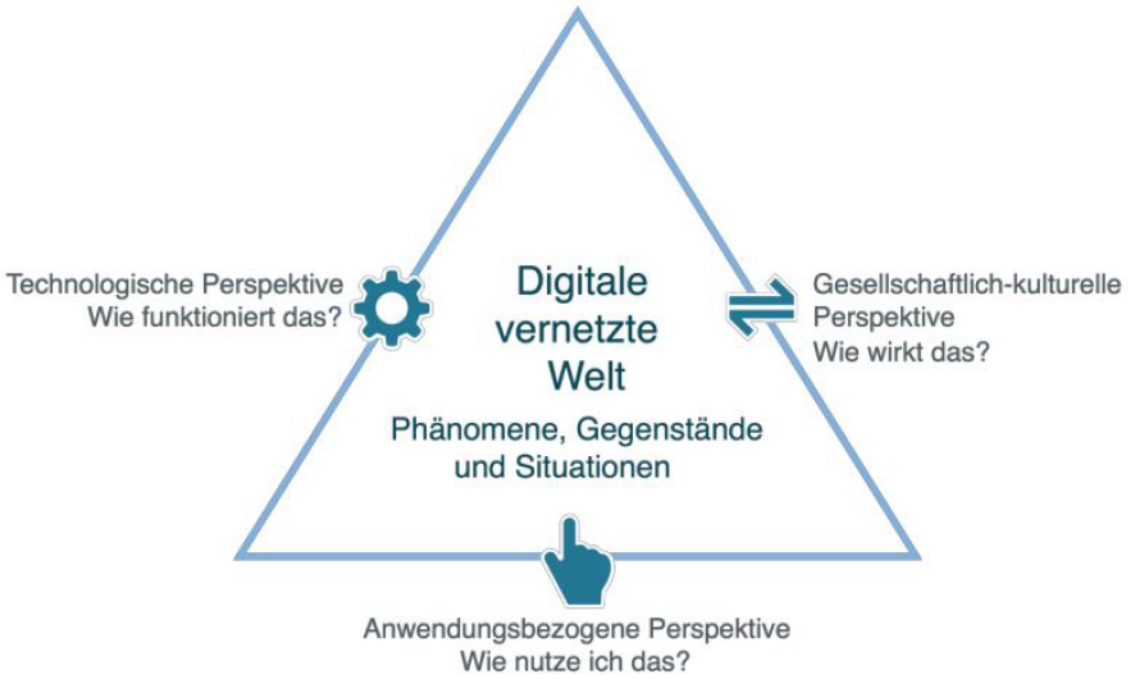


Abb. 2.3: Das Dagstuhl-Dreieck (Brinda et al. 2016, S. 3)

Die Vielseitigkeit des Themas *Datenschutz* lässt sich sehr gut anhand des Dreiecks aufzeigen. „Die gesellschaftlich-kulturelle Perspektive untersucht die Wechselwirkungen der digitalen vernetzten Welt mit Individuen und der Gesellschaft“ (Brinda et al. 2016, S. 3). Dieser Aspekt zeigt sich z. B. in dem Punkt, dass viele Menschen in Sozialen Netzwerken und ähnlichen Plattformen aktiv oder auch nur passiv tätig sind. Kontakte werden teilweise nur auf digitaler Ebene gepflegt. Der Umgang mit eigenen persönlichen Daten, aber auch mit den Daten anderer bzw. den Informationen, die man über andere kennt und als Daten speichert, spielt in dieser Perspektive eine entscheidende Rolle.

„Die anwendungsbezogene Perspektive fokussiert auf die zielgerichtete Auswahl von Systemen und deren effektive und effiziente Nutzung zur Umsetzung individueller und kooperativer Vorhaben“ (Brinda et al. 2016, S. 3). Solche Systeme sind auf der Hardware-Seite

z. B. Smartphones und Tablet-PC und auf Software-Seite z. B. Soziale Netzwerke, Lernmanagementsysteme und Cloud-Dienste. Der Nutzer muss die Angebote kennen und sie zielgerichtet einsetzen. Dabei sind die Grundsätze des Datenschutzes zu beachten.

„Die technologische Perspektive hinterfragt und bewertet die Funktionsweise der Systeme, die die digitale vernetzte Welt ausmachen" (Brinda et al. 2016, S. 3). Durch das technologische Verständnis der Systeme ist es möglich, Zusammenhänge besser zu verstehen. Daraus lässt sich erklären und erschließen, wie z. B. ein E-Mail-Versand abläuft und Daten auf dem Weg abgefangen werden können oder personenbezogene Daten unterschiedlicher Quellen miteinander verknüpft werden.

Im Juli 2019 veröffentlichte die Initiative *Keine Bildung ohne Medien!* das sogenannten ***Frankfurt-Dreieck***, welches eine „Erweiterung und Fortschreibung" des „Dagstuhl-Dreiecks" darstellt. Die Modellfunktion ist die Bereitstellung „eine[s] überfachlichen Orientierungs- und Reflexionsrahmen[s] für Bildungsprozesse im digitalen Wandel … und" der Einbezug „möglichst aller relevanten Perspektiven daran beteiligter Disziplinen" mit dem Ziel, „aus den disziplinären Perspektiven … Phänomene einer digitalen Welt und die daraus resultierenden Erfordernisse für Bildungsprozesse zu beschreiben und dadurch eine gemeinsame Reflexionsbasis zu entwickeln sowie darauf aufbauend – in künftigen Schritten – die notwendigen Kompetenzen für Partizipation in einer digital geprägten Welt zu definieren" (Brinda et al. 2019, S. 1). Im Modell werden die drei Perspektiven *technologisch-mediale Perspektive*, *Interaktionsperspektive* und *gesellschaftliche-kulturelle Perspektive* mit jeweils den Prozessen *Analyse*, *Reflexion* und *Gestaltung* beschrieben.[58] In der Modellmitte erscheint der Betrachtungsgegenstand.

Beide Modelle, die von Forschern mit einem politischen Hintergrund erstellt worden sind, zeigen, dass das Thema *Datenschutz* ein wichtiger Aspekt innerhalb der digitalen Bildung ist.

2.2.6. Das EU-Projekt *DigComp*

Ein EU-Projekt, welches wie das Dagstuhl- und Frankfurt-Dreieck (vgl. Abschnitt 2.2.5) und das KMK-Strategiepapier *Bildung in der digitalen Welt* (vgl. Abschnitt 2.2.7) einen politischen Hintergrund hat, ist der sog. *European Digital Competence Framework for citizens*. In ihm sind die zu beherrschenden Kompetenzen zur sicheren, kritischen, gemeinschaftlichen und kreativen Nutzung digitaler Technologien beschrieben. Innerhalb dieses Kompetenzrahmens gibt es einen Bereich *Safety*, in dem Kompetenzen zum Schutz persönlicher Daten und digitaler Identitäten aufgelistet sind. Somit nimmt das Thema *Datenschutz* auch in diesem Papier eine tragende Rolle ein (vgl. (Ferrari 2013) und (Carretero et al. 2017)).

[58] Im Dagstuhl-Dreieck entspricht die erste Perspektive der technologischen Perspektive und die Zweite der anwendungsbezogenen Perspektive.

Letztendlich legitimiert ein solcher Referenzrahmen, dass das Thema *Datenschutz* Inhalt eines zeitgemäßen Informatikunterrichts zu sein hat, wenn das übergeordneten Projektziel die Beschreibung der Schlüsselkompetenzen des 21. Jahrhunderts vor Augen hat.

2.2.7. Das KMK-Strategiepapier *Bildung in der digitalen Welt*

Die Kultusministerkonferenz der Länder (KMK) hat im Dezember 2016 den Beschluss *Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt"* verabschiedet (Sekretariat der Kultusministerkonferenz (Hg.) 2016), welches in dieser Arbeit im Vergleich zum EU- Projekt *DigCom* detaillierter dargestellt wird, da das Strategiepapier in den nächsten Jahren direkte Auswirkungen auf die deutschen Schulen und Lehrpläne haben wird. Diese „KMK-Strategie … [ist ein] Meilenstein in der Entwicklung des deutschen Schulsystems" (Eickelmann 2017, S. 30). In dem Papier wird zwischen Schule, beruflicher Bildung und Hochschule unterschieden, wobei im Folgenden nur die Schule betrachtet wird.

Die Strategie verfolgt hierbei zwei Ziele:

(1) „Die Länder beziehen in ihren Lehr- und Bildungsplänen sowie Rahmenplänen, beginnend mit der Primarschule, die Kompetenzen ein, die für eine aktive, selbstbestimmte Teilhabe in einer digitalen Welt erforderlich sind."
(2) „Bei der Gestaltung von Lehr- und Lernprozessen werden digitale Lernumgebungen entsprechend curricularer Vorgaben dem Primat des Pädagogischen[59] folgend systematisch eingesetzt." (Sekretariat der Kultusministerkonferenz (Hg.) 2016, S. 11)

Es ist nicht angedacht, dass die zu erwerbenden Kompetenzen in einem eigenen Fach (mit eigenständigem Curriculum), sondern im Zusammenhang mit spezifischen Fachkompetenzen unterschiedlicher Fächer vermittelt werden.[60] Dadurch entstehen vielseitige Erfahrungs- und Lernmöglichkeiten, wobei durch digitale Lernumgebungen eine individuelle Lerngestaltung und Förderung der Schüler und eine Eigenverantwortung für den Lernprozess ermöglicht wird.

Ab dem Jahr 2021 soll jeder Schüler jederzeit eine digitale Lernumgebung nutzen und einen Zugang zum Internet haben, wenn dies im Rahmen des Lernprozesses pädagogisch sinnvoll ist. Dazu sind jedoch folgende Voraussetzungen notwendig:

(1) „Eine funktionierende Infrastruktur …,
(2) die Klärung verschiedener rechtlicher Fragen …,
(3) die Weiterentwicklung des Unterrichts und
(4) vor allem auch eine entsprechende Qualifikation der Lehrkräfte."
(Sekretariat der Kultusministerkonferenz (Hg.) 2016, S. 11)

[59] Dies meint, dass das Lehren und Lernen einem Bildungs- und Erziehungsauftrag folgen müssen.
[60] Es sei an dieser Stelle noch angemerkt, dass in dem Strategiepapier die digitale Bildung auf die Nutzung und kritische Reflexion digitaler Medien reduziert wird. Dadurch wird das Papier der Bedeutung eines digitalen Bildungsbegriffs nicht gerecht, da digitale Bildung weiter zu fassen ist (vgl. Abschnitt 2.2.5).

Es werden in dem Kompetenzmodell der KMK insgesamt sechs Kompetenzbereiche vorgegeben (Sekretariat der Kultusministerkonferenz (Hg.) 2016, S. 15–18):

(1) Suchen, Verarbeiten und Aufbewahren
(2) Kommunizieren und Kooperieren
(3) Produzieren und Präsentieren
(4) Schützen und sicher agieren
(5) Problemlösen und Handeln
(6) Analysieren und Reflektieren.

„Neben den klassischen Bereichen von bekannten Medienkompetenzmodellen werden auch neue Bereiche mit in das Rahmenkonzept aufgenommen. Datensicherheit und Aspekte des Schützens bekommen hier sicherlich zu Recht eine besondere Relevanz“ (Eickelmann 2017, S. 26). Somit muss das Themas *Datenschutz*, welches schon in den Richtlinien der Verbraucherbildung ausformuliert worden ist (vgl. Abschnitt 2.2.2.3), in die Umsetzung der KMK-Strategie übernommen werden. Dazu schreibt die KMK, dass Lehrende „durch ihre Kenntnisse über … Datenschutz und Datensicherheit … die Schülerinnen und Schüler … befähigen [sollen], bewusst und überlegt mit Medien und eigenen Daten in digitalen Räumen umzugehen und sich der Folgen des eigenen Handelns bewusst zu sein“ (Sekretariat der Kultusministerkonferenz (Hg.) 2016, S. 27).

Für das Thema der vorliegenden Arbeit sind die folgenden Teilbereiche aus dem Strategiepapier von Interesse (Sekretariat der Kultusministerkonferenz (Hg.) 2016, S. 16):

„3.3. rechtliche Vorgaben beachten
3.3.3 Persönlichkeitsrechte beachten
4.1. Sicher in digitalen Umgebungen agieren
4.1.1. Risiken und Gefahren in digitalen Umgebungen kennen, reflektieren und berücksichtigen
4.1.2. Strategien zum Schutz entwickeln und anwenden
4.2. Persönliche Daten und Privatsphäre schützen
4.2.1. Maßnahmen für Datensicherheit und gegen Datenmissbrauch berücksichtigen
4.2.2. Privatsphäre in digitalen Umgebungen durch geeignete Maßnahmen schützen
4.2.3. Sicherheitseinstellungen ständig aktualisieren
4.2.4. Jugendschutz- und Verbraucherschutzmaßnahmen berücksichtigen“

Diese Teilbereiche und Unterpunkte sind inhaltlich klar beschrieben und so ausdifferenziert, dass nur ein geringer inhaltlicher Spielraum zur Ausgestaltung zur Verfügung steht. Gestaltungsmöglichkeiten und ein Gestaltungsbedarf besteht jedoch darin, wie die Kompetenzen über die unterschiedlichen Schulstufen aufgebaut werden sollen. Um den Umgang mit einer heterogenen Schülerschaft und Schulformen zu ermöglichen, sind bewusst keine unterschiedlichen Kompetenzstufen definiert worden.

Der Kompetenzrahmen ist kein statisches Modell, sondern ist aufgrund der schnelllebigen Entwicklungen den jeweiligen Anforderungen und Bedürfnissen anzupassen. Eine „Auswertung

des Erreichten“ soll die weitere Entwicklung des Modells begleiten (Sekretariat der Kultusministerkonferenz (Hg.) 2016, S. 53).

Das Kompetenzmodell ist eine Synthese aus drei anderen Modellen, die zur Formulierung der oben genannten Kompetenzen herangezogen worden sind:

(1) der EU-Referenzrahmen *DigComp* (vgl. Abschnitt 2.2.6),
(2) das empirisch ermittelte Kompetenzmodell computer- und informationsbezogener Kompetenzen, das aus der ICIL-Studie (vgl. Kapitel 1) erwachsen ist, und
(3) das *Kompetenzorientierte Konzept für die schulische Medienbildung* der Länderkonferenz MedienBildung (vgl. Abschnitt 3.1).

Alle Schüler, die ab dem Schuljahr 2018/19 eingeschult oder in die weiterführende Schule eintreten werden, sollen bis zum Ende ihrer Pflichtschulzeit die oben genannten Kompetenzen erworben haben.

2.3. Existierende Forschungsarbeiten und Studien zum Thema *Datenschutz und Unterricht*

Der folgende Abschnitt gliedert sich in zwei Teile. Im ersten Teil werden Forschungsarbeiten und -ergebnisse vorgestellt, wobei der Schwerpunkt der Recherche auf Bezüge zu Wissen, zur Wahrnehmung, zum Nutzungsverhalten (insbesondere bei Kindern und Jugendlichen) und zur Didaktik im Bezug zu Datenschutz liegt. Veröffentlichungen zur Modellbildung im Zusammenhang mit Datenschutzkompetenz wurden keine gefunden. Im zweiten Teil des Abschnitts findet eine detaillierte Betrachtung ausgewählter Studien statt, die das Verhalten und die Kompetenzen von Jugendlichen im Umgang mit Computer (Smartphone, Tablet, …) und Internet und das Online-Verhalten untersuchen. Bei der Recherche hat der Autor jedoch keine Studie ausfindig gemacht, die speziell und ausschließlich Datenschutz oder Datenschutzkompetenz untersucht. Jedoch gibt es Untersuchungen, in deren Rahmen diese Aspekte mehr oder weniger ausführlich mitbetrachtet worden sind. Es wird an dieser Stelle kurz über die Ergebnisse dieser Studien berichtet. Dabei fand bewusst eine Beschränkung auf deutschsprachige Studien statt, um zum einen eine Vergleichbarkeit mit den Ergebnissen der im Rahmen dieser Arbeit durchgeführten Untersuchung zu ermöglichen und zum anderen sind die Rahmenbedingungen z. B. US-amerikanischer Erhebung andere, da US-Amerikaner ein anderes Datenschutzverständnis haben und der Stellenwert ein anderer ist[61]. Einzige Ausnahme bildet die Studie *Difference between young and older adults in relation to information privacy* über die (Hoofnagle et al. 2010) berichtet, da aus dieser Studie Items für die Untersuchung des Autors (vgl. Kapitel 4) verwendet worden sind. Am Ende dieses Teilabschnitts gibt es eine Zusammenfassung über alle betrachteten Studien.

[61] Vgl. dazu (Weichert 2012, S. 718).

2.3.1. Forschungsarbeiten im Zusammenhang mit Datenschutz

In (Gross und Acquisti 2005) werden Muster der Informationsoffenbarung in Sozialen Netzwerken und deren Auswirkungen auf den Datenschutz untersucht. Dazu wurden 4000 Studierende der Carnegie Mellon University, die *Facebook* nutzen, beobachtet, wobei die Autoren darauf hinweisen, dass ihre Ergebnisse auch für andere Plattformen gelten. Während personenbezogene Daten großzügig bereitgestellt werden, werden einschränkende Datenschutzeinstellungen kaum genutzt. Nur eine geringe Anzahl von Mitgliedern ändert die Standardeinstellungen für den Datenschutz, um die Sichtbarkeit der Benutzerprofile zu maximieren. Aufgrund der bereitgestellten Informationen setzen sich Benutzer Risiken aus und machen es Dritten extrem leicht, digitale Dossiers ihres Verhaltens zu erstellen. Durch Influencer wird das Informationsoffenbarungsverhalten beeinflusst. Ferner geben die Nutzer sachbezogen persönliche Informationen an, da der von ihnen erwartete Nutzen aus der Veröffentlichung die wahrgenommenen Kosten übersteigt. Gruppenzwang und Herdenverhalten können ebenfalls Einflussfaktoren sein und so auch zu kurzsichtigen Einstellungen der Privatsphäre führen. Letztendlich könnte ein Schutzgefühl, das die (wahrgenommenen) Grenzen einer Campusgemeinschaft bietet, ein weiterer Einflussfaktor sein. In (Acquisti und Gross 2006) wird eine Studie beschrieben, bei der eine repräsentative Stichprobe von *Facebook*-Mitgliedern (78 % im Alter von 17 bis 24 Jahren und 15 % im Alter von 25 bis 34 Jahren) an einer US-amerikanischen Einrichtung befragt worden ist. Die Ergebnisse wurden mit den aus *Facebook* selbst abgerufenen Informationen verglichen. Unter anderem wurden auch die Auswirkungen von Datenschutzbedenken auf das Verhalten der Mitglieder untersucht. Ein Vergleich zwischen den Einstellungen der Mitglieder und deren tatsächlichem Verhalten und der Verhaltensänderungen nach der Veröffentlichung datenschutzrelevanter Informationen zeigt, dass die Datenschutzbedenken wenig Einfluss auf eine Mitgliedschaft haben. Auch Personen mit Bedenken geben eine große Menge persönlicher Informationen preis. Einige Mitglieder vertrauen darauf, dass sie die von ihnen bereitgestellten Informationen und den externen Zugriff kontrollieren können. Es wurde beobachtet, dass Missverständnisse der Mitglieder über die tatsächliche Größe und Zusammensetzung der Online-Community und über die Sichtbarkeit der Mitgliederprofile herrschen.

(Schulz 2012) führte eine Studie zum Selbstdatenschutz durch, bei der die Gründe für die Nutzung von *studiVZ* und die Datenschutzpräferenzen untersucht wurden. Durch die Online-Umfrage konnte gezeigt werden, dass bei der Nutzung Sozialer Netzwerke ein Unterschied zwischen Datenschutzkompetenz und Medienkompetenz messbar ist.[62] Zudem spielt die Regelung und Ausgestaltung des Datenschutzes durch die Anwendungen eine Rolle. Er kommt zu

[62] „Medienkompetenz ist als Konzept gedacht, das auf einen Bildungsgrad beruht, der die Kenntnisse, die Anwendung, die Kritik und die Anpassung bzw. Veränderung von Medien wie dem Internet fördert. Datenschutzkompetenz basiert demgegenüber nicht nur auf der Kenntnis der anwendungsbezogenen Datenschutzeinstellungen und deren Nutzung im Rahmen einer Selbstdatenschutz-Kompetenz." (Schulz 2012, S. 269)

dem Schluss, dass ein hoher Datenschutz weder von der Medienkompetenz noch vom individuellen Bildungs- oder Sozialniveau abhängt. „Ein guter Datenschutz [basiert] auf gesetzlichen Regelungen, technischer Programmierung (privacy by design) sowie individuellen Schutzmaßnahmen. Letztere umfassen nicht nur Datenschutzkompetenzen, sondern auch ein Bewusstsein für die sozialen, politischen und ökonomischen Gefahren, die von einem ungenügenden Datenschutz ausgehen“ (Schulz 2012, S. 269).

Eine Untersuchung der Praktiken Jugendlicher in Sozialen Netzwerken zur Aufdeckung eines Zusammenhangs zwischen Online-Risiken und Online-Chancen stellt (Livingstone 2008) vor. Sie diagnostiziert, dass jüngere Teenager sich ein „hoch-dekoriertes“ und ein stilistisch ausgefeiltes Profil erstellen, während die älteren Teenager nur eine schlichte Ästhetik für ihr Profil wählen, da für sie die Verbindung zu den Anderen im Netzwerk von Bedeutung ist und die Identität durch authentische Beziehungen mit den Anderen gelebt wird. Daher hat die Verschiebung der Identitätsentwicklungsphasen Auswirkungen auf das Erleben der Online-Chancen und Online-Risiken von Teenagern. Einfluss auf das Gleichgewicht zwischen Chancen und Risiken hat zudem das Freunde-Konzept in Sozialen Netzwerken und die Bereitstellung von Datenschutzeinstellungen. Jugendliche arbeiten mit einer geschickten Klassifizierung von Freunden, die in Bezug auf Intimität gesehen wird, aber nichts mit öffentlich und privat im Sinne Sozialer Netzwerke zu tun hat. Teenager wünschen eine passende Abstufung der Intimität, die eine Herangehensweise an Datenschutz im Internet darstellt, während es jedoch Mängel in der Internetkompetenz gibt. Für die Jüngeren kann es zu Online-Risiken wegen der Selbstdarstellung kommen. Bei den Älteren können Online-Risiken im Vertrauen liegen. Risiken können zudem durch eine eingeschränkte Internetkompetenz und verwirrende und schlecht gestalte Webseiten gefördert werden. Auch wenn Nutzer – um online präsent zu sein – sich selbst ihre Freundschaften und Gemeinschaften wählen, heißt das nicht, dass alles von sich auch preisgegeben werden muss. Die Entscheidung darüber ist für viele Teenager eine Handlung, um ihre Identität und ihre Intimsphäre zu schützen.

Der Beitrag (Dey et al. 2013) nimmt sich des Problems der Nutzung Sozialer Netzwerke durch Minderjährige an. Netzwerkanbieter treffen Vorkehrungen zum Schutz der Kinder (wie die Anzeige minimaler oder keiner Informationen in öffentlichen Profilen oder Untersagung des Beitritts kleiner Kinder), damit Dritte die Dienste nicht missbrauchen, um Kinder zu finden oder gar zu profilieren. Jedoch können Angreifer diese Vorsichtsmaßnahmen durch effiziente Crawling- und Data Mining-Methoden umgehen, wie die Autoren anhand von *Facebook* zeigten. Es wurden nicht nur die meisten Schüler einer ausgewählten Schule gefunden, sondern das jeweils ausgegebene Profil enthielt mehr Informationen als im öffentlichen Profil der registrierten Minderjährigen verfügbar war, sodass dadurch sogar schlimmstenfalls kriminelle Handlungen vorbereitet werden könnten. Ein US-Gesetz zum Schutz der Online-Privatsphäre Minderjähriger erleichtert ironischerweise den gezeigten Ansatz. Da ein erheblicher Teil der Minderjährigen über ihr Alter (was von den Anbietern nicht überprüft wird) lügt, konnte gezeigt werden, wie viele Vorsichtsmaßnahmen umgangen werden können, wodurch

sowohl lügende als auch wahrheitsgemäße Minderjährige gefährdet werden. Die Untersuchung hat letztendlich gezeigt, dass es deutlich weniger Datenschutzverletzungen geben würde, wenn *Facebook* keine Altersbeschränkungen hätte.

In (Youn 2008) wird eine Untersuchung zu der Rolle des Elterneinflusses bei der Entwicklung der Datenschutzbedenken von Jugendlichen und ihre spätere Einstellung zu Datenschutzmaßnahmen vorgestellt. Die Autorin schließt aus ihren Beobachtungen, dass elterliche Vermittlungsmaßnahmen problematisch sein könnten, da den Eltern keine umfassende Liste von Online-Aktivitäten zur Verfügung steht, über die Jugendliche und Eltern diskutieren könnten. Während Eltern sich auf E-Commerce-bezogene Handlungen kommerzieller Webseiten konzentrieren, beschäftigen sich Jugendliche mit Sozialen Netzwerken und sind in Chatrooms unterwegs. Daher sind die Auswirkungen des Elterneinflusses auf Jugendliche schwach.

(Norberg et al. 2007) beschreiben eine Studie zur Untersuchung des Privacy Paradox. In vorangegangener Forschung wurde immer davon ausgegangen, dass Risiko und Vertrauen sowohl Verhaltensabsichten als auch tatsächliches Verhalten beeinflussen können. Die Autoren argumentieren nun, dass die Verhaltensabsicht nicht das tatsächliche Verhalten vorhersagt, da das Risiko die Offenlegungsabsicht beeinflusst, während eine Vertrauensheuristik auf den tatsächlichen Offenlegungskontexten wirkt. Sie betonen aufgrund ihrer Überlegungen, dass nicht nur die Politik durch Gesetze eingreifen muss, sondern dass auch der Verbraucher sich anstrengen und verstehen muss, wem sie ihre Daten anvertrauen. Auch wenn Rosenberg[63] fordert, dass der beste und effektivste Weg, die Nutzung von Informationen zu kontrollieren, ohne das Verhalten andere zu beeinträchtigen, darin besteht, zu verhindern, dass sie jemals in die Hände anderer gelangen, kann dies nicht das Ziel sein. Die Erhebung und Verwendung von Daten kann nur auf Grundlage von Berechtigungen erfolgen. Eine Gefahr sehen die Autoren darin, dass politische Entscheidungen getroffen werden, die nur einen Teil des Problems betreffen und ggf. negativ für die Unternehmen werden könnten. Wichtiger ist es, die Verbraucher für den Schutz ihrer eigenen Privatheit zu gewinnen, das wohl das effizienteste Mittel darstellt, um die Bedenken der Menschen zu zerstreuen.

In dem Beitrag von (Brüggen und Wagner 2017) werden Ergebnisse aus vier Studien betrachtet, von denen die JFF-Studie *Persönliche Informationen in aller Öffentlichkeit* in Abschnitt 2.3.2 ausführlich betrachtet wird. Die Autoren leiten aus Untersuchungen zum Privacy Paradox ab, dass Jugendliche trotz starker Bedenken Angebote nutzen, „da die digitalen Dienste eng mit ihrer Lebensführung verknüpft sind“ (Brüggen und Wagner 2017, S. 132). Jugendliche erkannten 2010 die Risiken, dass Betreiber von Internetplattformen auf personenbezogene Daten zugreifen und auswerten, noch nicht, jedoch neuere Studien zeigen, dass sich diese Ansicht geändert hat. Vor allem die Bedeutung persönlicher Daten im Zusammenhang mit Auswertungsverfahren ist den Befragten nicht klar. Einerseits sind die Jugendlichen bereit, sich der Aufgabe des Selbstdatenschutzes anzunehmen, andererseits „sind sie mit dieser Aufgabe auf mehreren Ebenen überfordert“ (Brüggen und Wagner 2017, S. 136). Das Recht auf

[63] Rosenberg, Alexander (2000): Privacy as a Matter of Taste and Right. In: *Social Philosophy and Policy* 17 (2), S. 68 – 90

informationelle Selbstbestimmung wird zur Verhandlungssache. Statt sich, z. B. bei der Veröffentlichung eines Fotos, das Einverständnis der Betroffenen einzuholen, trifft der Nutzer selbst die Entscheidung, sodass an diese Stelle die eigene Einschätzung tritt. Diese Verhandlungssache „impliziert einen Kontrollaufwand", wobei „diese Dynamik … vermutlich Interessen von Anbietern digitaler Dienste in die Hände" spielt (Brüggen und Wagner 2017, S. 139). Dies führt am Ende dazu, dass eine Resignation gegenüber den Unternehmen eintritt. Informationelle Selbstbestimmung kann nur dann ausgeübt werden, wenn der Nutzer auch Entscheidungsoptionen (Einflussnahme und Partizipation) hat. „Die Gestaltung von Technologien [ist] eine wichtige Stellgröße, mit der ein Ermöglichungsrahmen für informationelle Selbstbestimmung und (Selbst-)Datenschutz auch als soziale Praxis gestärkt werden kann" (Brüggen und Wagner 2017, S. 143). Die Autoren vertreten die Ansicht, dass ein neues Privacy Paradox entsteht, wenn die Nutzer die Verantwortung für einen (Selbst-)Datenschutz erkennen, aber sie gleichzeitig keine Optionen sehen, darüber selbst bestimmen zu können, und letztendlich resignieren (Brüggen und Wagner 2017, S. 144).

(Bonneau und Preibusch 2009) haben eine Analyse von Datenschutzpraktiken und Datenschutzrichtlinien in Sozialen Netzwerken durchgeführt und kommen zu dem Schluss, dass der Datenschutz in den Netzwerken insofern unpraktisch ist, als die Datenschutzkontrollen, Datenerfassungsanforderungen und gesetzlichen Datenschutzrichtlinien der Websites erheblich voneinander abweichen und dem Nutzer keine angemessene Kontrolle über den Datenschutz bietet. Daher wäre eine standardisierte Datenschutzkennzeichnung (ähnlich einer Nährwertkennzeichnung) notwendig, mit denen Datenschutzpraktiken in einem nicht-textuellen Format kommuniziert werden können, damit Benutzer fundierte Entscheidungen zum Datenschutz treffen können.[64]

Über die Messung von Datenschutzlecks in Sozialen Netzwerken berichten (Srivastava und Geethakumari 2013). Weil Nutzer Informationen an ihre „digitalen Freunde" in den Netzwerken weitergeben, entsteht ein Datenschutzrisiko. Durch die Berechnung eines von den Autoren vorgeschlagenen Datenschutzquotienten (eine Metrik zur Messung des Datenschutzes eines Nutzerprofils), den der jeweilige Nutzer kennen soll, kann er anhand einer Skala sein Datenschutzrisiko selbst ablesen und letztendlich einschätzen.

(Liu et al. 2011) berichten in ihrem Beitrag zu den Privatsphäre-Einstellungen von *Facebook* im Kontext der Nutzererwartungen und der Realität, dass die Häufigkeit falscher Datenschutzeinstellungen oder die Schwierigkeiten der Benutzer bei der Verwaltung ihrer Datenschutzeinstellungen sich kaum quantifizieren lässt. Ziel war es, die Diskrepanz zwischen den gewünschten und den tatsächlichen Datenschutzeinstellungen zu messen und das Ausmaß des

[64] Da davon ausgegangen werden kann, dass Datenschutzerklärungen von Anbietern nicht ernsthaft gelesen werden und zudem die Mini-Displays von Smartphones für die langen Texte ungeeignet sind, beschreibt Hansen Lösungsvorschläge, entweder durch standardisierte Piktogramme oder durch „Mehrebenen-Policies" oder durch „maschinell übertragene Policies" den Verbraucher bei den Entscheidungen zu unterstützen. Und „vertrauenswürdige Gütesiegel können auch im Datenschutzbereich Verbraucher_innen darin unterstützen, die guten Produkte zu erkennen, und für Unternehmen Marktanreize für eingebaute und gelebten Datenschutz schaffen" (Hansen 2015a, S. 3f).

Problems der Datenschutzeinstellung durch Zahlen zu beschreiben. Dazu wurde eine als *Facebook*-Anwendung implementierte Umfrage 200 *Facebook*-Nutzern bereitgestellt. Es konnte festgestellt werden, dass 36 % des Inhalts mit den standardmäßigen Datenschutzeinstellungen geteilt werden und dass die Datenschutzeinstellungen insgesamt nur in 37 % der Fälle den Erwartungen der Benutzer entsprechen.

Aktuelle Projekte zur Erforschung der Privatheit sind *Strukturwandel des Privaten I + II*, welche von der Volkswagenstiftung finanziert wurden/werden. „Ziel … ist es, mit Informatik, Politik-, Rechts- und Medienwissenschaft vier zentrale Disziplinen zusammenzuführen, die mit der Reflexion um Bedeutung, Wert und Grenzen des Privaten befasst sind. Interdisziplinär soll dabei das Bedingungsverhältnis von Privatheit, Freiheit und Demokratie im Zusammenwirken mit informationstechnischen Entwicklungen untersucht werden.“[65] Aus Sicht der Informatik zeigte sich, dass Privatheit in der Informatik (fälschlicherweise) meist mit informationeller Selbstbestimmung gleichgesetzt und durch Werkzeuge zum Selbstdatenschutz realisiert wird. Weiterhin wurde Privatheit vertiefend analysiert – erstens in seinem Verhältnis zu Interessenkonflikten und Machtasymmetrien und zweitens in seinem Verhältnis zu Vertrauen. Parallel dazu wurde durch eine empirische Untersuchung zum Webtracking gezeigt, dass sich dieses in den letzten 15 Jahren verfünffacht und zu einer Monopolisierung geführt hat. In Ergänzung dazu wurde ein Verfahren zur Webtracking-Erkennung entwickelt, das nicht den Quellcode des Webservices, sondern sein Verhalten analysiert (Wambach 2018). Kernerkenntnis des Projektes war es, dass sich das Verständnis von Privatheit von einem Individualrecht wandelt und Privatheit in seiner Bedeutung für Demokratie und Freiheit interpretiert werden muss. Aus Sicht der Informatik bedeutet dies, dass Privatheitsschutz nicht einzig den Nutzern in Sinne von Selbstdatenschutz auferlegt werden kann und darf, sondern mittels einer geeigneten Symbiose von Selbst- und Systemdatenschutz erfolgen muss. Das Ziel des noch laufenden Projektes *Strukturwandel des Privaten II* ist es, die Erkenntnisse des Vorgängerprojekts in Form eines interdisziplinären Theoriemodells zu konsolidieren und eine Übertragungsmöglichkeit auf den Kontext Europa zu prüfen (Bräunlich et al. 2019). Durch die Ergebnisse des Projekts können einerseits Hinweise zur Gestaltung von IT-Systemen und andererseits zur Nutzeraufklärung erwachsen.[66]

[65] Siehe https://strukturwandeldesprivaten.wordpress.com/privatheit-und-freiheit/ (zuletzt geprüft am 09.09.2019)

[66] Über die „Neubestimmung der Privatheit“ siehe auch (Hill 2014). Eine „Post-Privacy“ wäre dann nach seiner Auffassung eine „Welt ohne Privatsphäre“ (S. 250f). Auf S. 256 merkt der Autor die Bildung von *Social Capital* an, eine Form sozialer Zusammenkünfte, die durch *Linking*, *Bonding* und *Bridging* entstehen. „Dem Urteil, der Bewertung und dem Rat von ‚Freunden‘ wird oft mehr Vertrauen geschenkt als klassischen Institutionen oder Autoritäten. Neue Plattformen des Austauschs und der Diskussion entstehen. Menschliches Verhalten, menschliche Überzeugungen und menschliche Beziehungen organisieren sich damit neu in einem ‚Age of Connection‘.“ Schon 1999 sagte Scott McNeally (Chef von Sun Microsystems): „You have zero privacy anyway. Get over it“ (zitiert nach (Weichert 2012, S. 718)) und prägte damit schon die Post-Privacy-Denkweise.

2.3.2. Studien im Zusammenhang mit Datenschutz

Im Folgenden werden ausgewählte Studien in Form einer Zusammenfassung vorgestellt.

JIM-Studie 2018. Jugend, Information, Medien. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland (Stuttgart, November 2018)[67]:

Die seit 1998 jährlich veröffentliche Studie hat das Ziel, die Mediennutzung Jugendlicher zu untersuchen und Fachleuten in unterschiedlichen Institutionen und Fachverbänden im Rahmen ihrer Arbeit (Forschungsvorhaben, Argumentationshilfe, …) zu dienen.

Es zeigt sich, dass fast jeder Jugendliche ein Smartphone mit Internetanbindung besitzt, welches dann auch meist täglich zur Internetnutzung und zum Musikhören (vor allem Streaming-Dienste und *YouTube*) genutzt wird. Im Rahmen der Internetnutzung haben nicht alle Jugendlichen uneingeschränkten Zugang im heimischen WLAN. Öffentliche WLAN-Hotspots werden unabhängig vom Alter von mehr als 70 % genutzt. Die Bereiche Kommunikation, Unterhaltung und Gaming spielen unabhängig vom Alter die entscheidende Rolle, wobei hier geschlechterspezifisch Mädchen die Kommunikation und Unterhaltung präferieren und Jungen den Spielen mehr zugeneigt sind. Zur Informationssuche wird nur 10 % der Zeit aufgewendet. Von den Internetangeboten liegt *YouTube* weit abgeschlagen vorne, gefolgt von *WhatsApp* und *Instagram*; *Facebook* hat massiv an Aktualität verloren[68] und wird nur von Älteren genutzt. Durch Fotos und Videos findet bei *Instagram* die Teilhabe des Alltags von Personen des persönlichen Umfelds statt, die dann von einem Viertel der Follower kommentiert wird. Gut 10 % der Befragten posten eigene Inhalte bei *Instagram*. Eine ganz eindeutige Mehrheit der Videos wird bei *YouTube* mobil abgerufen, wobei Favoriten nicht diagnostiziert werden, aber Musik und Spielen stark vertreten sind. Ein Fünftel der Befragten konsumieren Erklärvideos zu Themen aus Ausbildung und Schule. Trotz der regen Nutzung laden andererseits 92 % keine eigenen Videos hoch. Bei der Internetrecherche ist *Google* der absolute Favorit, gefolgt von *YouTube* und *Wikipedia*. Interessanterweise nutzen ein Viertel der Befragten auch *Twitter* und *Facebook*. Von falschen und beleidigenden Inhalten waren schon 20 % betroffen (Jungen eher als Mädchen), wobei der größte Anteil zwischen 14 und 15 Jahren alt ist und es die bildungsfernen eher als die bildungsnahen Jugendlichen betrifft. Von den Befragten (vor allem 16- bis 17-Jährige) gaben 11 % zu, dass Bildmaterial (beleidigend oder peinlich) verbreitet wurde, wobei es keinen geschlechterspezifischen Unterschied gibt. Über Cybermobbing im Bekanntenkreis konnten ein Drittel berichten (eher Mädchen als Jungen) und es vor allem die 16- bis 17-Jährigen betrifft. Opfer waren 8 % der Befragten, die eher dem niedrigeren Bildungsniveau zuzurechnen sind. Zur Verbreitung werden die oben genannten beliebten Portale genutzt. Aufgrund vorangegangener JIM-Studien kann schlussgefolgert werden, dass Jugendliche ihre eigene Datenschutzkompetenz umso höher einschätzen, je weniger Erfahrung sie mit Sozialen Netzwerken haben.

[67] Quelle der Zitate: Feierabend et al. 2018

[68] Laut (Kramer und Spaeing 2014, S. 373) waren 2014 Viert- und Fünftklässler keine Exoten, die mehr als einhundert *Facebook*-Freunde hatten.

KIM-Studie 2018. Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger in Deutschland (Stuttgart, Mai 2019)[69]:

Die seit 1999 alle zwei Jahre veröffentliche Studie hat – wie die JIM-Studie – das Ziel, die Mediennutzung von Kindern zu untersuchen und Fachleuten in unterschiedlichen Institutionen und Fachverbänden im Rahmen ihrer Arbeit (Forschungsvorhaben, Argumentationshilfe, …) zu dienen. Insbesondere die Relevanz der Fragen nach der Smartphone-Nutzung und dem Einstieg in die Kommunikation mit Sozialen Medien sowie die Frage der Nutzungsintensität stehen im Fokus.

Das Interesse für Handy/Smartphone bzw. Internet/Computer liegt in dieser Altersgruppe an dritter bzw. fünfter Stelle. Für 98 % ist ein Internetzugang und für 97 % das Handy/Smartphone fester Medienbestandteil, wobei die Jungen (im Gegensatz zu den Mädchen) eher im Besitz von Mediengeräten sind (Ausnahme: Smartphone/Handy jeweils 50 %). Mit 39 % führt das Smartphone die Liste der täglichen Internetzugänge an. Das heimische WLAN nutzen 65 %, während 35 % auf frei zugängliche WLAN-Netze zurückgreifen (betrifft vor allem zehn Jahre und älter). Am Beliebtesten ist *WhatsApp* (52 %), gefolgt von *YouTube* (26 %) und *Facebook* (13 %). Eine zentrale Rolle spielen auch Suchmaschinen, wobei *Google* die Favorisierteste ist; es wird vor allem nach Musik, Information für den Unterricht und zum Sport, zum Einkauf und nach Prominentenseiten gesucht. Die Kommunikation stellt einen zentralen Punkt der Internetnutzung dar, wobei *WhatsApp* mit steigendem Alter immer wichtiger wird. Den Weg ins Internet findet knapp die Hälfte und ein Drittel kann alleine Apps installieren. Immerhin 10 % sind schon auf für Kinder ungeeignete Inhalte gestoßen, 5 % kamen in Kontakt damit, 4 % erlebten Ängste und 3 % unangenehme Bekanntschaften. Eltern sehen Gefahren im Internet, die Spieldauer mit Smartphones wird reglementiert, aber nur ein Drittel der Eltern wenden technische Hilfsmittel zum Jugendschutz an.

DIVSI U25-Studie - Euphorie war gestern. Die „Generation Internet" zwischen Glück und Abhängigkeit (Hamburg, November 2018)[70]:

Ziel der Studie war, „das aktuelle Spektrum der digitalen Lebenswelten von Jugendlichen und jungen Erwachsenen in Deutschland abzubilden. Im Fokus der Untersuchung stehen … neben der Nutzung digitaler Medien vor allem die Einstellungen der jungen Menschen zum Internet, ihre Haltung zu Fragen rund um Datenschutz und Privatsphäre, zu Sozialen Medien und aktuell wahrgenommenen Trends im Netz. Einen besonderen Schwerpunkt bilden die Themen Vertrauen und Sicherheit sowie die damit verbundenen Verhaltenskonsequenzen bei den 14- bis 24-Jährigen" (S. 10).

Unter den Befragten nutzen 99 % täglich das Internet, aber nur 69 % macht das Internet glücklich, 64 % sehen eine Zeitverschwendung darin und 19 % fühlen sich sogar genervt. Sorge und

[69] Quelle der Zitate: Feierabend et al. 2019
[70] Quelle der Zitate: Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) 2018

Ängste einer Internetabhängigkeit werden in diesem Zusammenhang angesprochen. In den letzten fünf Jahren hat sich die Wahrnehmung und Nutzung Sozialer Medien stark verändert. *Facebook* verliert an Bedeutung (weniger posten, eher Andere beobachten), jedoch für 99 % ist *WhatsApp* „nicht mehr wegzudenken" (S. 13). Trotz generell vorhandener Chancen in der Internetnutzung werden auch die Risiken deutlicher wahrgenommen, was aber nicht zu einer Verstärkung an Sicherheitsmaßnahmen führt. Angriffe und Falschinformationen sind gefürchteter als die Angst vor Datensammlungen. Die Schule bereitet nicht ausreichend auf die digitale Welt vor, obwohl Themen wie Schutz und Sicherheit als wichtig erachtet werden. Kenntnisse werden autodidaktisch oder mit Hilfe des Freundeskreises angeeignet. „Datenschutz ist für alle relevant, gilt aber als ein zu komplexes Thema, dessen tatsächliche Auswirkungen (positiv wie negativ) unklar sind. Daher steigen viele aus, wenn es um eine intensivere Auseinandersetzung mit dem Thema geht, indem sie aktuelle Gegebenheiten schlicht akzeptieren oder das Problem verdrängen" (S. 105). Risikoaspekte werden von Frauen eher als von Männern wahrgenommen. Das „Thema Datenschutz wird als immer komplexer wahrgenommen. Nur noch 57 Prozent der 14- bis 24-Jährigen glauben, gut über die Möglichkeiten zum Schutz der eigenen Daten im Internet informiert zu sein, während sich im Jahr 2014 noch fast drei Viertel der Befragten gut informiert fühlten. In diesem Zusammenhang ist das Interesse am Thema Schutz der Privatsphäre tendenziell rückläufig, zumindest in Bezug auf den Aspekt, sich über Möglichkeiten zum Schutz der Privatsphäre zu informieren. Hier stimmen nur noch 60 Prozent zu, sich für die entsprechenden Möglichkeiten zu interessieren (2014: 69 Prozent)" (S. 86).

DIVSI U9-Studie. Kinder in der digitalen Welt (Hamburg, April 2015)[71]:

„Ziel der Studie ist es, aus der Perspektive sowohl der Kinder als auch der Eltern die Zugänge und Zugangsweisen zur digitalen Welt zu erfassen und Einstellungen und Verhaltensmuster in ihrer ganzen Bandbreite abzubilden."

In diesem Altersspektrum von drei bis acht Jahren überwiegen Internetrisiken die Chancen einer Internetnutzung, wobei vor allem die Gefahr von den nicht kindgerechten Inhalten und dem Schutz persönlicher Daten ausgeht (besonders durch eine unkontrollierte Kommunikation, da mit acht Jahren die Nutzung von online-Communities steigt („unüberschaubares Gefahrenfeld")). Ergebnis ist daher das Internetverbot, insbesondere bei deutlicher Risikowahrnehmung der Eltern. Die Internetkompetenz der Kinder erwächst aus der Kompetenz der Eltern, wobei der Bildungsgrad der Eltern eine entscheidende Rolle spielt. Sicherheitsmaßnahmen bei der Internetnutzung von Kindern anzuwenden, ist keine Selbstverständlichkeit, wobei das Maß umso größer ist, je gebildeter die Eltern sind. Die Sicherheitskonzepte sind jedoch unterschiedlich.

[71] Quelle der Zitate: Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) 2015

Studie „How different are young adults from older adults when it comes to information privacy attitudes and policies?“ (Berkeley/California, Juli 2009)[72]:

In (Hoofnagle et al. 2010) wird eine Studie beschrieben, bei der 2009 im Rahmen einer telefonischen Umfrage das Datenschutzverhalten junger und älterer Erwachsener miteinander verglichen wird. Hierbei geht es um die Einstellungen zum Schutz der Online-Privatsphäre, um die Ausführung bestimmter Verhaltensweisen zum Schutz der Privatsphäre, um ihre öffentlichen Präferenzen in Bezug auf die Privatsphäre und ihre Kenntnis der Datenschutzgesetze, die sie in ihrem täglichen Leben beeinträchtigen könnten. Dabei wurde festgestellt, dass die zum Ausdruck gebrachten Einstellung der Jüngeren (18 – 24 Jahre) sich nicht, wie vermutet, so stark denen der Älteren unterscheiden, wenn es um Sensibilität in Bezug auf Online-Datenschutz und Richtlinienvorschläge geht. Die Kosten-Nutzen-Analyse bezogen auf das Risiko gehen die Jüngeren anders an, da die 18- bis 24-Jährigen zu Unrecht glauben, dass das Gesetz ihre Privatsphäre (online und offline) mehr schützt, als dies tatsächlich der Fall ist. Dieser Mangel an Wissen in einem attraktiven Umfeld und nicht die mangelnde Sorge um die Privatsphäre können ein wichtiger Grund dafür sein, warum sich eine große Anzahl von ihnen scheinbar unbefangen mit der digitalen Welt auseinandersetzt.

In der Zusammenfassung wird festgehalten, dass im Rahmen politischer Diskussionen berücksichtigt werden sollte, dass das aktuelle Geschäftsumfeld zusammen mit anderen Faktoren junge Erwachsene manchmal dazu ermutigt, personenbezogene Daten freizugeben, um soziale Eingliederung zu genießen, auch wenn sie in ihren rationalsten Momenten möglicherweise konservativere Normen vertreten. Daher ist die Bildung ein wichtiger Faktor, bei der Informationssicherheit und Datenschutz im Mittelpunkt stehen, da die Jüngeren sich darin von den Älteren unterscheiden. Aber Bildung allein reicht wahrscheinlich noch nicht aus, um ein angestrebtes Maß an Privatsphäre zu erreichen. Sie benötigen wahrscheinlich mehrere Formen der Hilfe aus verschiedenen Seiten der Gesellschaft, einschließlich der Behörden, um mit den komplexen Entwicklungen fertig zu werden, die darauf abzielen, im Widerspruch zu ihren besten Datenschutzinstinkten zu stehen.

JFF-Studie „Persönliche Informationen in aller Öffentlichkeit“ (München, September 2010)[73]:

Ziel der Studie war der „Aufschluss über die Motive und Regeln, nach denen Jugendliche ihr Handeln in Online-Netzwerken ausrichten und die auch ihren Umgang mit persönlichen Informationen und Persönlichkeitsrechten mitbestimmen … Insbesondere geht die Studie der Frage nach, wie die Jugendlichen sich zu Fragen des Datenschutzes und der Persönlichkeitsrechte positionieren“ (S. 2).

[72] Quelle der Zitate: Hoofnagle et al. 2010
[73] Quelle der Zitate: Wagner et al. 2010

Die Wenigsten der Befragten haben sich mit den Themen *Datenschutz* und *Persönlichkeitsrechte* beschäftigt, weshalb der Wissensstand heterogen ist, aber je älter und je gebildeter sie sind, desto besser sind sie informiert. Das notwendige Wissen erarbeiten sie sich selbst oder sie fragen in der Peergroup; Medien, Eltern und Lehrer sind weitere Optionen. Eine Selbstverantwortung für die betreffenden Daten bringen die Befragten mit, vertrauen aber dagegen den Netzwerkanbietern eine entsprechende Sorgfalt und einen korrekten Umgang mit den Daten. Über einen Missbrauch der Daten durch Fremde und Auswertung und Aggregation der Daten durch Anbieter Sozialer Netzwerke sind sich die Jugendlichen kaum bewusst oder ihre Vorstellung ist vage. Daher gilt es, die Privatsphäre zu schützen, wobei von den Älteren und Gebildeteren erkannt wird, dass neben dem eigenen Handeln auch die Kontrolle des Handelns Dritter (z. B. Freunde) dazu gehört, was aber nicht zu leisten ist. Kritisch Denkende merken an, dass durch eine Änderung der sozialen Normen ein sozialer Druck entsteht, der die Offenlegung persönlicher Informationen fordert.

LfM-Studie „Digitale Privatsphäre. Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen“ (Düsseldorf, Oktober 2012)[74]:

Ziel der Studie war die Erkundung des Privatsphäreverständnisses junger Nutzer und das Aufdecken von „Einflüsse[n] auf das Selbstoffenbarungsverhalten in Sozialen Netzwerkplattformen“ (S. 5). Im Rahmen der Untersuchung standen folgende vier Gesichtspunkte der Selbstoffenbarung im Vordergrund: (1) Veröffentliche Informationen in Nutzerprofilen, (2) die bei der Kommunikation entstehenden dynamischen Inhalte, (3) Privatsphäre-Einstellungen und (4) die Kontakte (S. 17). Dazu wurde einerseits eine quantitative Befragung Jugendlicher im Alter von zwölf bis 24 Jahre und „qualitative Interviews mit jungen Menschen und Experten aus den Domänen Schule, Jugendarbeit und Medien“ durchgeführt (S. 6).

Das Privacy-Paradox zeigt deutlich, wie Jugendliche ihre Zugänglichkeit einerseits kanalisieren, andererseits sich wegen des Selbstwertgefühls aber auch ihre Einzigartigkeit offenbaren. Dass mit Sozialen Netzwerken Chancen und Risiken verbunden sind, ist allen bewusst, jedoch hängt die Gewichtung von Sach-, Handlungs- und Begründungswissen ab. Eine Nutzung von Sozialen Netzwerken ist nur unter Selbstoffenbarung möglich, wobei Umfang und Tiefe ja nach Nutzer sich unterscheiden (im Profil angelegte Informationen werden selektiert). Die Aufklärungsmaßnahmen medienpädagogischer Initiativen scheinen – wenn man die Ergebnisse mit früheren Studien vergleicht – erfolgreich angelaufen zu sein. Trotzdem gibt es einen Aufklärungsbedarf bei Jugendlichen mit niedriger formaler Bildung und/oder Jüngeren. Gerade im Alter von 15 und 16 Jahren spielt das Selbstoffenbarungsverhalten und die Teilhabe wegen der sozialen Identitätssuche in diesem Alter eine entscheidende Rolle. Um die Privatsphäre im Internet wird sich Sorgen gemacht, wobei im Rahmen der Veröffentlichung persönlicher Informationen Digital Natives offener als Digital Immigrants sind, was am leicht unterschiedlichen Ver-

[74] Quelle der Zitate: Schenk et al. 2012b

ständnis von öffentlichen und privaten Informationen liegen könnte. „Die Einschätzung dessen, was privat und was öffentlich ist, orientiert sich zunächst an der Familie, an Eltern und älteren Geschwistern. Im Verlauf der Adoleszenz werden die Peers dafür zunehmend relevanter. Die Schule prägt die Einstellungen der Nutzer hingegen kaum“ (S. 70). In Sozialen Netzwerke, die einen dauerhaften Kontakt zur Peergroup gewährleisten können, spielen Unterhaltung und Beziehungspflege die größere Rolle gegenüber Selbstdarstellung, sodass eine rezeptive Nutzung neben Kommunikationsmöglichkeiten vorherrscht. Im Rahmen der Kommunikation sind privaten Mitteilungen (vor semi-öffentlichen) vorherrschend. Dabei wird über die Konsequenz kommunikativer Handlungen nicht nachgedacht, weil die Wirkung auf Andere im Vordergrund steht. Die älteren Nutzer sind bei der Auswahl ihres Freundes-, der eher einem erweiterten Bekanntenkreis gleicht, gründlicher. Mehr als die Hälfte (56 %) der 12- bis 24-Jährigen sind mit Leuten online vernetzt, die sie noch nie persönlich getroffen haben. „Die nuancierte Wahl der Einstellungsmöglichkeiten“ in Sozialen Netzwerken wird „nur von sehr wenigen Nutzern wahrgenommen … Möglicherweise ist diese [Ausgestaltung der Schutzmechanismen] zu komplex oder der Aufwand, den ein solch differenziertes Privatsphäre-Management bedeuten würde, wird als zu hoch eingestuft“ (S. 71). Nur selbst hinzugefügte oder bestätigte Kontakte haben Zugriff auf das Profil. „Diese Einstellung scheint sich mittlerweile auch in Deutschland zum einem Standard etabliert zu haben“ (S. 71). Die Wahrscheinlichkeit, dass die Privatsphäre dramatisch verletzt wird, wird für gering angesehen, aber immerhin 14 % der Befragten haben schon negative Erfahrungen gemacht. Den meisten Jugendlichen ist zwar bewusst, dass sie z. B. beim Teilen von Fotos für die Daten der anderen Freunde verantwortlich sind, aber nicht immer handeln sie danach. Die Studie bestätigt das Privacy-Paradox. „Die jungen Nutzer haben ein klares Bild davon vor Augen, was sie von sich zurückhalten möchten und welche Daten über sie öffentlich sein dürfen. Was privat ist und was nicht, wandelt sich im Laufe der Zeit“ (S. 73). Beobachtungen zeigen, dass auch Kinder sich zunehmend auf den Plattformen anmelden, bei denen die notwendige Medienkompetenz und die Auffassungsgabe zur Unterscheidung zwischen Freundschaft und Bekanntschaft fehlt.

BITKOM-Studie „Jung und vernetzt“ (Berlin, März 2014)[75]:

Der Großteil der Befragten besitzt einen PC und/oder ein Smartphone/Handy, bei dem die Funktionen SMS/Kurznachrichten-Schreiben, Spielen, Musikhören, Fotografieren/Filmen, Internetsurfen und Video-Schauen im Vordergrund stehen. Die Internetnutzung ist unter den zehn- bis elf-Jährigen für 94 % eine Selbstverständlichkeit. Unter den 16- bis 18-Jährigen geben 59 % an, mit Sicherheitsprogrammen umgehen zu können; unter den zehn- bis 18-Jährigen können 22 % der Jungen und 13 % der Mädchen Dateien oder E-Mails verschlüsseln. Chatten mit Freunden (48 %), Nutzen Sozialer Netzwerke (45 %) und Verschicken/Hochladen eigener Fotos (25 %) sind Internetanwendungen, bei denen der Datenschutz eine herausragende

[75] Quelle der Zitate: BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2014

Rolle einnimmt. Insbesondere die Älteren der Befragten haben schon bewusst falsche Altersangaben gemacht. Während bei den zehn- bis elf-Jährigen nur 32 % darauf achten, welche Informationen sie über sich selbst ins Netz stellen, steigt ab den zwölf-Jährigen der Anteil (mit 71 % beginnend) über das Alter an. Ein gleiches Bild gilt für die Beachtung, welche Informationen über einen selbst im Internet sichtbar sind. Die im Internet gemachten negativen Erfahrungen steigen mit dem Alter und der daraus resultierenden Nutzungshäufigkeit. Bei den Sozialen Netzwerken rangiert *WhatsApp* mit 72 % ganz oben, *Facebook* 56 %, *Skype* 46 %, *Google+* 19 %, *Instagram* 18 % und *Twitter* 8 %. Spitz-/Benutzernamen, Vor- und Nachnamen, Geburtsdatum/Alter und Porträtfotos werden von mehr als der Hälfte im Netz veröffentlicht; aber auch mit E-Mail-Adressen (42 %), Wohnort (31 %) und Fotos (29 %) wird nicht sparsam umgegangen. In den am meist genutzten Sozialen Netzwerken haben 62 % der Jungen und 57 % der Mädchen die Privatsphäre-Einstellungen geändert, wobei diese Option weitaus mehr von den Älteren als den Jüngeren genutzt wird.

Studie „Privatheit im Wandel" (Stuttgart, Juni 2015)[76]:

Durch die von den Nutzern preisgegebenen persönlichen Informationen in Sozialen Netzwerken erhöht sich das Risiko der Identifizierbarkeit und des Datenmissbrauchs durch Dritte, sodass der Nutzer vor neuen Herausforderungen gestellt ist. Ziel der Studie war die Klärung der Frage: „Führen diese Veränderungen auch zu einem veränderten Verhalten hinsichtlich der Privatsphäre?" (S. 4)

Von den rund drei Stunden täglicher Internetnutzung verbringen die Deutschen ca. die Hälfte der Zeit in Sozialen Netzwerken. Ungefähr 92 Minuten pro Tag werden von Smartphone-Nutzern für die Kommunikation aufgebracht, wobei Instant-Messenger die am „häufigsten genutzten Smartphone-Anwendungen" sind (S. 3). In der deutschen Bevölkerung gibt es eine starke Ausprägung an Privatheitsbedenken (Masur 2014, S. 10) und sie sieht „Privatheit … als wichtiges und schützenswertes Gut" an (98 %), welches selbst „bei Verdacht auf Kriminalität [noch] geachtet werden" sollte, meint 37 % der Befragten, wo hingegen 18 % „zum Schutz … der Bürger es dem Staat erlaubt sein [sollte], jeden Menschen zu überwachen" (S. 3 + 8). Da „ein hohes Bedürfnis an informationeller Privatheit" existiert, ist die öffentliche Zugänglichkeit der Daten unerwünscht (S. 3). Gut drei Viertel der Befragten wünschen sich, dass „wenig über sie bekannt ist"; die öffentliche Zugänglichkeit persönlicher Daten wünschen 82 % der Befragten nicht; und 94 % „finden, dass jeder Mensch selbst bestimmen können sollte, welche Informationen über ihn öffentlich zugänglich sind" (Trepte et al. 2014b, S. 12).

Weil es für die Nutzer keinen Einblick gibt, „was mit ihren Daten geschieht", machen sie sich „gerade in Online-Kontexten … erhebliche Sorgen um ihre Privatheit" (S. 3). Im Vergleich Vielmit Wenignutzern des Internets sorgen sich Vielnutzer im online- wie im offline Bereich eher um ihre Privatheit (Trepte et al. 2014b, 14f). Es ist den Befragten nicht bekannt, „welche Da-

[76] Quelle der Zitate: Trepte und Masur 2015a

tensammlungspraktiken von Anbietern durchgeführt werden und welche konkreten Strategien sie dagegen einsetzen können“ (S. 3). Trotzdem ist im Zeitraum von 2011 bis 2014 ein Anstieg der Veröffentlichung von Daten im Internet erkennbar, die insbesondere medizinische Informationen, Telefonnummern und Beruf/Ausbildung betreffen (Trepte et al. 2014b, S. 16).

Zusammenfassend kann beobachtet werden, dass die Diskrepanz zwischen Privatheitswünschen und Privatheitsverhalten weiter wächst: Generell ist den Deutschen die Privatheit sehr wichtig, weshalb sie sich online wie offline um ihre Privatheit sorgen; die Akzeptanz der Freigabe persönlicher Daten im Internet ist im Verlauf der Jahre zurückgegangen, jedoch konnte gleichzeitig ein gravierender Anstieg der Preisgabe privater Informationen beobachtet werden (Trepte et al. 2014b, S. 22).

Studie „Online Privacy Literacy Scale (OPLIS)“ (Stuttgart, November 2015)[77]:

Ziel der Studie ist es, die Diskrepanz zwischen dem Bedenken über die Offenlegung persönlicher Daten und dem Veröffentlichen intimer Details im Internet zu erforschen.[78] Zum einen wurde die Online-Datenschutzkompetenz erfasst, die schon im Mittelpunkt der Studie *Privatheit im Wandel* stand, zum anderen die Umsetzung konkreter Datenschutzmaßnahmen erforscht.

In (Trepte et al. 2015b) beschreiben die Autoren die Entwicklung einer Datenschutzkompetenzskala (OPLIS), um die Diskrepanz zwischen dem Bedenken über die Offenlegung persönlicher Daten und dem Veröffentlichen intimer Details im Internet zu erforschen. Obwohl in der Vergangenheit schon empirische Untersuchungen zu Online-Datenschutzverhalten und Online-Datenschutzeinstellungen gemacht worden sind, kritisieren die Autoren von OPLIS, dass (1) die meisten Skalen nicht multidimensional sind und (2) nur auf Selbstberichten der Probanden beruhen und damit kein Wissen objektiv erfassen (Trepte et al. 2015b, S. 347). Die vorgeschlagene Skala umfasst fünf Dimensionen, die sich alle um den Bereich des Wissens konzentrieren: „(1) Knowledge about practices of organizations, institutions and online service providers; (2) Knowledge about technical aspects of online privacy and data protection; (3) Knowledge about laws and legal aspects of online data protection in Germany; (4) Knowledge about European directives on privacy and data protection; and (5) Knowledge about user strategies for individual privacy regulation“ (Trepte et al. 2015b, S. 333). Hier liegt ein entscheidender Unterschied zu dem Datenschutzkompetenzmodell, welches der Autor in Kapitel 3 vorstellen wird. Datenschutzkompetenz kann nach seiner Auffassung nicht ausschließlich auf Wissen beruhen. In der Zusammenfassung des oben genannten Beitrags schreiben die Autoren, dass eine Erklärung für das paradoxe Verhalten der Internetnutzer mangelndes Wissen über individuelle Strategien zur Kontrolle des Online-Datenschutzes, rechtliche und technische Aspekte sowie institutionelle Praktiken sein kann. Sie wissen nicht, wie sie ihre persönlichen Daten schützen sollen. Es gibt nur wenige Informationen über Geschäftspraktiken und über die

[77] Quelle der Zitate: Trepte und Masur 2015b
[78] Ausführliche Informationen zur Motivation und zum Ziel der Studie finden sich in Abschnitt 2.3.1 dieser Arbeit.

Gesetze und Vorschriften, die sich auf den Datenschutz auswirken. Zurzeit befindet sich die Welt in einer Krise, da das bisherige Verständnis von Datenschutz durch Online-Praktiken weitgehend untergraben wird. Es bleibt jedoch die Frage, ob den Internetnutzern tatsächlich dadurch geholfen wird und damit zu einer besseren „Online-Welt" beigetragen wird, indem Verbesserungen des Wissens und der Bildung als Lösung vorschlagen werden. Der Beitrag endet mit der Frage, ob eine Online-Datenschutzkompetenz nicht ein patriarchalisches Argument ist, das sich an Datenschutzstandards hält, die für Benutzer möglicherweise veraltet erscheinen (Trepte et al. 2015b, S. 362).[79]

Zwischen der Online-Privatheitskompetenz und konkreten Datenschutzstrategien können folgende Zusammenhänge aufgedeckt werden: Mit einem höheren Wissen im Bereich des Datenschutzrechts entscheiden sich Nutzer eher, einen Dienst nicht zu nutzen; jedoch wird die Nichtnutzung eines Dienstes durch ein höheres Maß an technischem Wissen weggemacht.

Datenschutzmaßnahmen werden dann umgesetzt, je höher das Wissen über Datenschutzstrategien und technische Maßnahmen ist. Der Schutz der Privatheit wird durch eine Software-Lösung nur dann genutzt, wenn der Nutzer Kompetenzen im Bereich des Datenschutzrechts hat; Wissen über institutionelle Praktiken, technisch Aspekte oder Datenschutzstrategien spielen für den Software-Einsatz keine Rolle. „Je höher das Wissen über die eigenen Rechte, desto häufiger werden diese Rechte auch in Anspruch genommen; je höher jedoch das Wissen in den anderen Bereichen [Wissen über institutionelle Praktiken, technisch Aspekte oder Datenschutzstrategien], desto seltener werden rechtliche Schritte unternommen" (Trepte und Masur 2015b, S. 16).

Kompetentere Nutzer verwenden unterschiedliche Strategien zum Schutz der Daten im Internet. Hierbei kommen Anonymisierung, Pseudonymisierung und unterschiedliche Software zum Einsatz. Zwischen Online-Privatheitskompetenz und passiven Datenschutzmaßnahmen (Vermeidung bestimmter Angebote) konnte kein Zusammenhang bestätigt werden. Daraus könnte geschlossen werden, dass die kompetenteren Nutzer ihre Daten so glauben schützen zu können, „dass sie es nicht mehr für notwendig halten, einen bestimmten Dienst zu nutzen." Es wird ferner auch keine Notwendigkeit gesehen, gegen entsprechende Anbieter juristische Schritte einzuleiten (Masur et al. 2017, S. 12).

Die Autoren der Studie geben jedoch auch zu bedenken, dass erstens in fünf bis zehn Jahren für die Regulierung der Online-Privatheit neuartige und weitere Kompetenzen erforderlich sein werden und dass zweitens in einer digitalen Umgebung, die immer komplexer wird, es dem Nutzer überhaupt nicht mehr möglich sein wird, sich gegen alle möglichen Privatheitsverletzungen zu schützen (Masur et al. 2017, S. 12).

[79] Diese Frage stellen sich auch (Berendt et al. 2014) am Ende der dort vorgestellten Unterrichtsreihe (vgl. Abschnitt 2.4).

Studie zu Privatheitsbedürfnissen verschiedener Kommunikationstypen on- und offline:

(Trepte et al. 2015a) stellen eine Untersuchung zu Privatheitsbedürfnissen vor. Viele bis dahin veröffentlichte Studien dazu orientierten sich am Online-Bereich. Da Kommunikation auch offline stattfindet und man mit denselben Menschen on- und offline verkehrt, scheint es für ein vollständiges Bild notwendig, beide Kontexte zu betrachten. Für die Untersuchung wurden vier Kommunikationstypen definiert und deren Ergebnisse miteinander verglichen. Die Autoren kommen zu folgenden Ergebnissen: „Privatheit steht als schützenswertes Gut hoch im Kurs“, „Wer sich um Privatheit sorgt, nutzt weniger Soziale Medien“, „Weniger Online-Kommunikation geht mit weniger schlechten Erfahrungen einher“, „Kommunikation in vielen Kanälen bringt emotionale Unterstützung“, „Online-Vielnutzer wissen mehr über Privatheit im Internet“ und „Bedürfnis nach Selbstoffenbarung [ist] im persönlichen Gespräch am höchsten“ (Trepte et al. 2015a, S. 255). Nutzer machen sich Sorgen und sehen Privatheit als ein sehr wichtiges Thema an. Die Preisgabe der Daten im Internet verursacht auch bei Usern ohne konkrete Verletzungen der Privatheit ein mulmiges Gefühl, da das Wissen darüber, was mit den Daten geschieht, fehlt und Datenströme im Netz immer schlechter zu durchschauen sind. Die Bedenken der Nutzer müssen ernst genommen werden. „User mit Bedenken fühlen sich nicht gewappnet, die juristischen, ökonomischen und technischen Rahmenbedingungen so einzuschätzen, dass sie ihre Privatheit sinnvoll schützen können.“ Ziel muss es daher sein, „nicht die Sorgen auszuräumen, sondern die Wissensvermittlung soweit voranzutreiben, dass Menschen ihren Sorgen mit konkretem Wissen – zum Beispiel über Maßnahmen zum aktiven Datenschutz – begegnen können“ (Trepte et al. 2015a, S. 256). Daher fordern die Autoren, dass das Thema Privatheit stärker in der Schulbildung und in der Medienberichterstattung berücksichtigt wird. Ferner sind die Praktiken der Datenverwerter auf den Prüfstand zu stellen. „Es ist zu vermuten, dass negative Erfahrungen zur gängigen Internetnutzung gehören und dass andauernde negative Erfahrungen zu einer Habitualisierung führen. Es erscheint angeraten, hier eine öffentliche Debatte darüber anzustoßen“ (Trepte et al. 2015a, S. 257).

Studie zu Schülervorstellungen über die Suchmaschine Google:

In (Seifert et al. 2013) wird eine qualitative Ministudie[80] beschrieben, in der Schülervorstellungen über die Suchmaschine *Google* vorgestellt werden. Ein Untersuchungsaspekt war der Punkt *Datenschutz*, zum dem Folgendes festgestellt wird: „Das Thema *Datenschutz* ist den befragten Schülern bekannt. Sie erklären, dass Google ‚über alles und jeden‘ Daten sammelt, das Verhalten der Benutzer mit Hilfe der Suchfunktion im Internet mit verfolgt und jederzeit weiß, welche Person welche Website besucht … Die befragten Schüler bewerten Googles Kenntnis über das eigene Such- und Surfverhalten dennoch insgesamt als positiv … [Ein] Schüler betont auch sein Vertrauen in Google und dass die Datensammlung den Suchergebnissen

[80] Die Untersuchung erntete auf der Konferenz Kritik, da nur fünf Schüler im Alter von 13 bis 15 Jahren befragt worden sind. Dennoch, so sieht es auch der Autor, dürfen die Antworten aus den Interviews als schülertypisch angesehen werden.

zugutekommt. Ein anderer Schüler sieht darin auch einen Eingriff in die Privatsphäre. Möglichkeiten zum Schutz der eigenen Daten sind den Schülern bekannt“ (Seifert et al. 2013, S. 51). „Auffällig war, dass die Interviewten Googles Datensammlung als potentiell ungefährlich einstuften. Sie wussten zwar, dass Daten von Google gesammelt werden und dass diese personenbezogen sein können, glaubten insgesamt jedoch nicht, dass sie selbst oder ihre Daten dadurch gefährdet sein könnten“ (Seifert et al. 2013, S. 52).

Zusammenfassung:

Fast jeder Jugendliche besitzt ein Smartphone und nutzt so gut wie täglich das Internet, wobei beides mit dem Alter steigt. Unterhaltung, Kommunikation und Gaming sind die Hauptmotive für den Gebrauch. Die Wahrnehmung und Nutzung Sozialer Medien hat sich in den letzten Jahren stark verändert. Nur ein geringer Anteil der älteren Jugendlichen nutzt inzwischen noch *Facebook*, im Gegenzug ist *WhatsApp* kaum mehr wegzudenken. Durch *Instagram* und *Snapchat* wird inzwischen die Teilhabe am Leben anderer geregelt, wobei die Mehrheit eher beobachtend statt produzierend ist. Gleiches gilt für *YouTube*, das eine sehr wichtige Rolle einnimmt, indem der Konsum vor allem in Unterhaltung, Musik (neben Streaming-Dienste), aber auch in Beiträgen für die Schule/Unterricht besteht. Unter den Suchmaschinen ist *Google* der absolute Favorit.

Die Chancen und Risiken der Internetnutzung werden wahrgenommen, was aber nicht zu einer Verstärkung der Sicherheitsmaßnahmen führt. Die Datenschutzkompetenz wird umso höher von den Befragten eingeschätzt, je weniger Erfahrung sie haben. Die Schule bereitet auf Themen wie *Datenschutz* und *Sicherheit* die Jugendlichen nicht (ausreichend) vor, ihr Wissen eignen sie sich autodidaktisch oder über Freunde, aber weniger über Eltern und Lehrer an. Die Angst vor Fake News ist größer als vor der Datensammlung. Jedoch das Interesse an Privatheit nimmt immer mehr ab, obwohl dennoch eine Sorge – eher bei den Digital Immigrants statt den Digital Natives – besteht. Im Laufe der Zeit wandelt sich aber die Einsicht, was auch in dem unterschiedlichen Verständnis für öffentliche und privaten Informationen besteht.

Das Privacy Paradox wird insofern bestätigt, dass die Zugänglichkeit schon kanalisiert wird, aber wegen des Selbstwertgefühls die Einzigartigkeit offenbart wird.[81] Dass die Nutzung Sozialer Netzwerke nur unter Selbstoffenbarung erfolgt, ist bewusst, wobei dies aber je nach Umfang und Tiefe unterschiedlich ist. Während bei den Jüngeren die Selbstdarstellung im Vordergrund steht, ist es bei den älteren Jugendlichen vor allem die Teilhabe wegen einer sozialen Identitätssuche. Die Chance der Wahl an Einstellungsmöglichkeiten wird kaum genutzt, weil dies eventuell zu komplex oder der Aufwand zu groß ist. Inzwischen ist es ein Standard, dass

[81] In Abschnitt 2.1.2 wird beschrieben, dass das Privacy Paradox so nicht mehr haltbar ist, denn das Verhalten der Online-Privatsphäre ist nicht paradox, sondern beruht auf unterschiedliche Einstellungen zum Datenschutz. Der obige Satz bezieht sich jedoch auf die Aussagen der zusammengefassten Studien.

nur bestätigte oder hinzugefügte Kontakte auf das Profil zugreifen können. Je älter die Befragten sind, desto eher werden Änderungen vorgenommen, wobei dies eher die Jungen statt die Mädchen tun.

Über Konsequenzen kommunikativer Handlungen wird kaum nachgedacht, weil die Wirkung auf Andere im Vordergrund steht. Gerade die Älteren (ab 12 Jahren aufwärts) achten darauf, welche Informationen sie über sich hochladen, verletzen aber trotzdem (teilweise wissentlich) das Recht am eigenen Bild. Der Wissensstand zu Datenschutz und Persönlichkeitsrechten ist recht heterogen (aber je älter und je gebildeter, desto besser sind sie informiert). Eine Selbstverantwortung für eigene Daten ist vorhanden, aber es wird auch ein Vertrauen in den sorgfältigen und korrekten Umgang mit Daten durch die Netzwerkanbieter geschenkt. Es herrscht nur eine vage Vorstellung vom Datenmissbrauch Dritter oder von der Datenaggregation durch Anbieter. Die Gebildeten erkennen den Schutz der Privatsphäre durch das eigene Handeln und gleichzeitiger Kontrolle im Handeln Dritter, was aber nicht zu leisten ist. Durch die Änderung der sozialen Norm entsteht sozialer Druck, der die Offenlegung persönlicher Informationen fordert.

Mit falschen oder beleidigen Inhalten oder mit Cybermobbing, welches vor allem im Alter von 15 bis 17 Jahren anzutreffen ist, sind schon bis zu einem Fünftel (insbesondere wenn sie aus einer bildungsfernen Schicht kommen) in Kontakt gekommen. Je älter die Jugendlichen sind, desto mehr negative Erfahrungen wurden gemacht, was an der höheren Nutzungshäufigkeit liegt.

Die Aufklärung durch medienpädagogische Initiativen zeigen inzwischen einen erfolgreichen Anlauf (im Vergleich zu früheren Untersuchungen), aber ein Aufklärungsbedarf existiert weiterhin bei den jüngeren und bildungsferneren Jugendlichen. Aber Bildung allein ist noch nicht ausreichend, sondern Unterstützungen durch Behörden, Gesetzgeber und anderen Seiten der Gesellschaft sind notwendig, denn der Datenschutzinstinkt ist gut ausgeprägt, aber den komplexen Entwicklungen kann kaum Stand gehalten werden. Der Vergleich von jüngeren mit älteren Erwachsenen zeigt, dass die Einstellungen zum Datenschutz so unterschiedlich nicht sind, jedoch sieht die Kosten-Nutzen-Analyse der Jüngeren anders aus, da sie fälschlicherweise glauben, dass durch das Gesetz ihre Privatsphäre bereits geschützt sei. Wegen eines Wissensmangels gehen Jüngere daher unbefangener mit der digitalen Welt um.

Beobachtungen zeigen, dass sich inzwischen vermehrt Schüler auf Sozialen Netzwerken anmelden, denen die notwendige Medienkompetenz oder die Auffassungsgabe, zwischen Freund und Bekanntem zu unterscheiden, fehlt. Eltern sind vor allem besorgt wegen nichtkindgerechter Inhalte und einer unkontrollierten Kommunikation, nutzen aber auch so gut wie keine Sicherheitsmaßnahmen für das Internet.

Untersuchungen, die über alle Altersschichten hinweggehen (ab 16 Jahre aufwärts), zeigen, dass die Privatsphäre als ein schützenswertes und wichtiges Gut angesehen wird. Das Bedürfnis an informationeller Privatheit ist hoch. Keine öffentliche Zugänglichkeit zu persönlichen Daten, über deren Freigabe jeder einzelne selbst zu bestimmen hat, wird gefordert. Weil kein

Einblick vorhanden ist, was mit den Daten geschieht, herrscht eine große Sorge bis zur Angst (vor allem bei Vielnutzern). Es ist keine Strategie bekannt, um sich den Datensammelpraktiken der Anbieter entgegen zu stellen, jedoch werden durch Anonymisierung, Pseudonymisierung und Einsatz von Softwarelösungen Strategien implementiert, um den Datenschutz im Internet zu fördern. Ein höheres Wissen an Datenschutzstrategien und technische Maßnahmen führt auch eher zu einer Umsetzung von Datenschutzmaßnahmen. Ein höheres Wissen im Bereich des Datenschutzrechts führt auch eher zur Nutzung von Diensten und dem Einsatz von Softwarelösungen zum Schutz der Privatheit. Obwohl die Preisgabe privater Informationen im Laufe der Zeit weiter gestiegen ist, ist umgekehrt die Akzeptanz der Datenfreigabe zurückgegangen.

2.4. Existierende Materialien und Beiträge für den Unterricht

Das älteste Unterrichtsmaterial, welches der Autor zum Thema *Datenschutz* recherchiert hat, stammt von (Bosse und Fleischhut 1986). Es ist bemerkenswert, dass zu einer Zeit, als es weder das World Wide Web gab, noch PC für die Privathaushalte erschwinglich waren und Rechner nur in Behörden und großen Firmen standen, dieses gesellschaftswissenschaftliche Thema in einem Informatikunterricht der Mittelstufe behandelt wurde. Die Unterrichtsreihe beginnt mit der Befragung innerhalb der Lerngruppe, deren Daten letztendlich unter Verwendung eines Computers ausgewertet werden. In einem zweiten Teil werden Themen wie „Verknüpfung unterschiedlicher Dateien und Diskussion der möglichen Gefahren“, „Datensammlungen und die Notwendigkeit eines Schutzes personenbezogener Daten“, „Das Datenschutzgesetz“, „Die Möglichkeit der Wahrnehmung von Rechten aus dem Datenschutzgesetz“, „Datensicherung – notwendige Maßnahmen und Schwachstellen“ und „Aktuelle Fragen zum Datenschutz“ behandelt (Bosse und Fleischhut 1986, S. 23). Trotz des Alters des Materials sind die hier angesprochenen Fragen hochaktuell. Diese Unterrichtsreihe ist ein sehr schönes Beispiel für die Anwendung des Kompetenzmodells einer informatischen Allgemeinbildung (Koubek 2005b).

Im Rahmen des Unterrichtskonzepts *Informatik im Kontext* (*IniK*) (Koubek o. J.) wird ein Planspiel zum Thema *Datenschutz* vorgestellt. Auf der Seite *www.it-lehren.de* beschreibt Gramm die historische Entwicklung. Der Ursprung des IniK-Projekts geht auf die Planspiele *Datenschutz in vernetzten Informationssystemen* (1987) und *Jugend im Datennetz* (1991) zurück, bei denen die Entwicklung eines Bewusstseins für Datenspuren im Netz (z. B. beim bargeldlosen Zahlen) im Mittelpunkt steht. Beide Rollenspiele werden mit Papier und Bleistift gespielt. Im Jahr 2005 erfolgte neben der Nutzung des Computers im Spielverlauf u. a. eine Anpassung der Währung und der inzwischen genutzten technischen Geräte (z. B. MP3-Player). Um die Installation einer Software auszuschließen, wurde eine Online-Version veröffentlicht (Dorn et al. 2005), die später an die Web 2.0-Welt angepasst worden ist. Eine Papierversion wurde am Studienseminar Oberursel (unter der Leitung von Poloczek) und eine Online-Variante (unter der Leitung von Oppermann und Dietz) im Rahmen der AG *IniK* in Berlin entwickelt (Dietz und Oppermann 2011). Dieses Online-Spiel steht zwischenzeitlich aus unterschiedlichen Gründen

nicht mehr zur Verfügung.[82] Ferner sind die Rollenbeschreibungen in der heutigen Zeit nicht mehr realistisch, wie die Erprobung der Unterrichtsreihe in einem GK Informatik an einem Gymnasium im Februar 2015 zeigte. Die Schüler konnten sich nicht mit den Rollen identifizieren. Ferner bemerkten sie auf die Frage, ob sie nach dieser Unterrichtseinheit ihr Verhalten ändern würden, sinngemäß: „Da sie ja noch jung seien, über kein Girokonto verfügen würden 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“ (Berendt et al. 2015, S. 35). Dies deckt sich mit den Beobachtungen aus (Berendt et al. 2014). Aus diesem Grund ist im Winter 2018/19 im Rahmen einer Masterarbeit dieses Rollenspiel technisch und inhaltlich unter der Leitung des Autors überarbeitet worden (Noll 2019). Die detaillierte Vorstellung erfolgt in Abschnitt 5.1.5.

Ein jüngerer Vorschlag für eine Unterrichtseinheit ist das von (Diethelm 2011) beschriebene Beispiel aus dem Kontext von Datenschutz, Internet und Urheberrecht, welches sich der Methode des forschend-entdeckenden Lernens bedient und dabei ebenfalls den IniK-Ansatz verfolgt. Themen der Unterrichtseinheit in Bezug auf Datenschutz sind „Kurszählung – Mikrozensus: Fragen zum Datenschutz“, „Datenschutz als Grundrecht?“, „Alltag Überwachung – Kameras und RFID“, „Die Macht einer Suchmaschine“ und „Vorratsdatenspeicherung“. In Bezug auf die zu erwerbenden Kompetenzen orientiert sich die Autorin an den Bildungsstandards (Gesellschaft für Informatik e. V. 2008), wobei der Inhaltsbereich *Informatik, Mensch und Gesellschaft* und die Prozessbereiche *Begründen und Bewerten* und *Strukturieren und Vernetzen* im Fokus stehen. Insgesamt beurteilt der Autor diesen Beitrag als einen sehr guten Vorschlag und teilt die Meinung mit Diethelm, dass dies insbesondere für den Anfangsunterricht geeignet ist, da jeder Schüler eine gewisse Vorerfahrung mitbringt (Heterogenität nutzen), die gesamte Reihe kontextorientiert ist und aufzeigt, dass Informatik nicht nur Technik ist (Diethelm 2011, S. 29).

Eine Unterrichtsreihe mit dem Titel *Kostenlos ist nicht kostenfrei oder „If you’re not paying for it, you are the product“* wird von (Berendt et al. 2014) beschrieben, in der die Datenauswertung in Sozialen Netzwerken und den sich daraus ergebenden Folgen für Datenschutz und Privatsphäre thematisiert werden. Die Autoren kritisieren, dass die in vielen Materialien und Handreichungen für den Unterricht darin formulierten Appelle kaum Gehör finden, da sie „aufgrund von Erkenntnissen aus der interdisziplinären Privacy-Forschung zu kurz … greifen“ (Berendt et al. 2014, S. 42). Ihnen geht es in ihrem Vorschlag um „Tragweite und Konzept“ (soziale Privacy und institutionelle Privacy[83], Beschädigung von Meinungsfreiheit und Demokratie), „Verständnis von Datensammlung und -verarbeitung" (Tracking, Data Mining, Big Data

[82] Unter http://www.opman.de/planspiel/index.php war das Planspiel bis Anfang Mai 2018 abrufbar. Aufgrund der in Kraft getretenen DSGVO (die Schüler mussten sich auf dem Server mit ihren Daten anmelden) und des Umstands, dass die php-Version, in der das Planspiel programmiert war, und die php-Version vom Anbieter nicht mehr unterstützt wurde, hat Oppermann das Planspiel abgeschaltet.

[83] Die Autoren schlagen diese Unterscheidung vor. Fälschlicherweise wird Privacy hier als Privatsphäre verstanden. Soziale Privacy ist demnach die „Privatsphäre“, die durch die Kommunikation mit Freunden und Nutzern in Sozialen Netzwerken charakterisiert ist. Im Rahmen der institutionellen Privacy werden die Betreiber Sozialer Netzwerke zu Mitwissern. Sie erhalten durch Posts, Fotos, usw. Zugang zu persönlichen Informationen.

und Schlussfolgerungen), „erweitertes Verständnis von Datensparsamkeit als Lösungsansatz“ (effektive Nutzung von Softwarewerkzeugen), „Kompetenzen“ (fundiertes Verständnis von Privacy, Risiken und Chancen von Internet und Sozialen Netzwerken, Kompetenzen zur Gestaltung), „Interessenkonflikte und politische Lösungen“ (im Zusammenhang mit Datenschutz) und „Interdisziplinarität“ (wegen der Komplexität des Themas ist eine fächerverbindende Behandlung der Themen notwendig). Die Unterrichtsreihe wurde einmal in einer 8. Klasse und einmal in einer 11. Jahrgangsstufe im Rahmen des Fachs *Politik/Gesellschaft/Wirtschaft* durchgeführt. Im ersten Teil werden die Folgen auf eine rechtsstaatliche Ordnung und die freie Persönlichkeitsentfaltung betont und durch Datenauswertung der Datensammelindustrie und Tracking im Internet diskutiert, während die zweite Hälfte den Blick auf die Auswirkungen auf die Privatsphäre und „den daraus resultierenden Rechtsgarantien“ behandelt. Ziel ist es, dass die „Schüler … Sensibilität gegenüber der Problematik Datenschutz und SNS (**S**oziale-**N**etzwerk-**S**ites) [entwickeln] … [,] Kenntnisse über moderne Methoden der Datensammlung im Internet und ihrer Analyse mithilfe von statistischen Verfahren des Data Mining [erwerben] … [und] ein staatsrechtliches Bewusstsein als ‚Grundrechtssubjekte‘ und mündige Bürger [entwickeln]“ (Berendt et al. 2014, S. 43). Gefolgt von einer ausführlichen Beschreibung der Unterrichtsreihe und einer Reflexion folgt eine Stellungnahme einer Schülerin, die aus ihrer Sicht das Resümee zieht, dass (1) ihr einerseits die gesamte Unterrichtsreihe und andererseits auch die Folgen der aus Data-Mining-gewonnen Informationen zu abstrakt sind (und damit keinen Einfluss auf ihr Verhalten im Alltag hat), (2) ihr „Online-Verhalten zum Teil purer Bequemlichkeit geschuldet und Datensparsamkeit nicht nur aus Sicht der institutionellen Privacy empfehlenswert ist“ und (3) weder bei ihr noch bei ihren Freunden „Konsequenzen aus der Reihe im Umgang mit Sozialen Netzwerken für … [sie] ersichtlich“ sind. Dies gelte auch für „den Zusammenhang [zwischen] Privatsphäre, freie Meinungsäußerung [und] Demokratie“. „Zusammenfassend würde … [sie] sagen, [dass ihre] … Haltung … zwischen indifferent, irritiert und entsetzt“ schwankt (Berendt et al. 2014, S. 54). Aus diesem Grund stellen sich die Autoren die Frage, „ob [sie] … mit diesem Ansatz heutige Schülerinnen und Schüler überhaupt noch erreichen können“ (Berendt et al. 2014, S. 54) und unterbreiten Vorschläge für überarbeitete Ansätze.

In (Berendt et al. 2015) wird neben der Vorstellung dreier Projekte, die hier schon weiter oben beschrieben sind, ein möglicher Weg durch einen Einstieg über Messenger-Dienste skizziert.[84] Der Beginn stellt eine Diskussion über Leitfragen zur Produktnutzung, deren Häufigkeit und deren Vorteile (gegenüber anderen Kommunikationsmöglichkeiten) dar. Eine Einigung auf einen Dienst für die weitere schriftliche Kommunikation wird vorgeschlagen, um die theoretische Ebene zu verlassen. Unverschlüsselte Kommunikation und die Verknüpfung diverser Dienste (wie z. B. *WhatsApp* und *Facebook*) stehen im nächsten Schritt im Vordergrund und sollen letztendlich zu der Einsicht führen, dass in der digitalen Welt ein zweites „Ich“ entsteht, dem Eigenschaften zugewiesen werden, deren Gültigkeit zu hinterfragen ist. Durch den Ein-

[84] Als einen weiteren alternativen Zugang schlagen die Autoren die *Crypto-Wars* vor, ohne dies jedoch weiter zu vertiefen.

satz eines Trackers wird wieder eine praktische Phase eingeschoben, bevor sich dem eine Diskussion über Privatsphäre und den Vor- und Nachteilen Sozialer Netzwerke anschließt. Das Fazit könnte lauten: „If you‘re not paying for it, you are the product" (Berendt et al. 2015, S. 40). Durch eine gruppendifferenzierte Untersuchung der AGB diverser Anbieter mit anschließender Diskussion führt dies unweigerlich zu Begriffen wie *Datenschutz*, *Datenschutzgesetz* und *informationelle Selbstbestimmung* (in Verbindung mit dem Volkszählungsurteil 1983). „Die Lauschangriffe im Netz haben eine andere Dimension: Der Meinungspluralismus, der ein Kennzeichen der Demokratie ist, geht verloren und Uniformität gewinnt die Oberhand" (Berendt et al. 2015, S. 41). Es gilt daher, Möglichkeiten des Selbstdatenschutzes nachzuweisen.

Mit einem speziell für den Unterricht programmierten Sozialen Netzwerk, welches zu Beginn den Namen *friendzone* und inzwischen den Namen *InstaHub* trägt, thematisiert Dorn den Unterrichtsinhalt *Datenbanken*. In (Dorn 2017) beschreibt er ganz knapp die Verknüpfung zu Aspekten wie *Datenschutz*, *Big Data* und *Datensicherheit*. In der weiterentwickelten Reihe in (Dorn 2019) wird ein ausführlicherer Vorschlag (als im ersten Artikel) zum Einbezug des Themas *Datenschutz* in den Unterricht (mit und ohne vorherige Behandlung des Themas *Datenbanken*) vorgestellt. Durch einen Wechsel von der Benutzerperspektive zur Administratorperspektive soll eine Sensibilisierung der Schüler angestoßen werden. Um dem Thema *Datenschutz* einen noch größeren Raum innerhalb des Projekts zu geben, sind unter der Betreuung des Autors drei Masterarbeiten 2019 entstanden, in denen *InstaHub* um weitere Module zum Thema *Datenschutz* erweitert worden ist. Die Arbeiten werden in Kapitel 5 vorgestellt.

Um mit Jugendlichen gesellschaftswissenschaftliche Themen der Informatik, die nach der Erfahrung des Autors eher eine untergeordnete Rolle im Schulunterricht spielen, zu bearbeiten, wurde im Schuljahr 2005/06 an der Humboldt-Universität Berlin eine Schüler-Arbeitsgruppe *Computer – Mensch – Gesellschaft* eingerichtet, denn „ein selbstbestimmter, verantwortungsvoller und sicherer Umgang mit Informatiksystemen bedingt … neben technischem Sachverstand auch Kenntnisse um gesellschaftlichen Verknüpfungen und Wechselwirkungen dieser Techniken", so die Autoren (Koubek und Kurz 2007, S. 126). Es ist ein mehrstufiges Programm erstellt worden, sodass „Materialien zur Sach- und Methodenschulung in ausreichender Menge, modularem Aufbau, vertikaler Differenzierung sowie in verknüpfbarer Form geschaffen und bereitgestellt wurde" (Koubek und Kurz 2007, S. 126). Dabei wurden die AG-Ziele einerseits durch die *Informatik-Mensch-Gesellschaft*-Kompetenzen der Bildungsstandards auf der Unterrichtsebene beschrieben und andererseits nach dem Prinzip Proof-of-Concept die Projektebene bedient. Als Unterrichtseinheiten wurden *Geschichte der Informatik*, *Geistiges Eigentum*, *Datenschutz*, *Ökologie*, *Kryptographie*, *Sicherheit*, *Ethik*, *Multimediarecht* und *Digitale Medien* behandelt.

In (Schubert et al. 2005) wird das Problem von Phishing-E-Mails mit dem Ziel thematisiert, dass Schülerinnen und Schüler „sicherheitstechnisch problematische E-Mails erkennen" und „über das Fälschen von E-Mail-Absendern" informiert sind (Schubert et al. 2005, S. 66). Hierzu werden Beispiele für die Lehrkraft vorgestellt.

In (Koubek 2005a) befinden sich ebenfalls Unterrichtsbeispiele zur Förderung von E-Mail-Kompetenzen. Über die Jahrgangsstufen der Sekundarstufe I verteilt fordert der Autor, dass „systematisch … die Kompetenzen aufgebaut werden, E-Mails auf ihre Absichten zu befragen und kritisch mit den erhaltenen Sendungen umzugehen“ (Koubek 2005a, S. 61).

In (Peters 2008) wird über die Ergebnisse einer Arbeitsgruppe der 15. Königsteiner Gespräche[85] berichtet, die einen möglichen Unterrichtsverlauf zum Inhaltsbereich *Informatik, Mensch und Gesellschaft* aus den Standards für die informatische Bildung (Gesellschaft für Informatik e. V. 2008) vorschlägt. Die Idee ist, soziale Netze zur Zeit des Mittelalters mit den sozialen Netzen von heute zu vergleichen, um „die Formen heutiger Kommunikation transparent werden zu lassen und auch neu schätzen zu lernen“ (Peters 2008, S. 42). Hierzu wird ein fächerverbindender Ansatz vorgeschlagen.

In dem Projekt *Virtual:Stories* von (Petko et al. 2017) stehen negative Online-Erfahrungen Jugendlicher im Vordergrund, die durch einen narrativen und fallbasierten Ansatz der Medienbildung zur Sensibilisierung dieser in Bezug auf typische Problemsituationen in der Online-Welt beitragen sollen. Ziel ist es, durch die im Rahmen von anonymen Interviews vorgestellten Fälle in eine Unterrichtsdiskussion über mögliche Strategien der Vermeidung und Bewältigung und zu einer Enttabuisierung der Probleme und Themen zu kommen. Die Autoren gehen davon aus, dass „das Risikoverhalten von Jugendlichen im Internet bei vielen Themen vermutlich weniger auf ein Informationsdefizit zurückzuführen, sondern vielmehr auf ein aktives Austesten von Grenzen … und ein bewusstes und teilweise auch provokantes Infrage-Stellen von Normen der Erwachsenenwelt“ ist (Petko et al. 2017, S. 53). Die Interviews, die über eine Webseite[86] zur Verfügung stehen, sind mit einer Filmkamera oder einem Audiorecorder aufgenommen und im Nachgang anonymisiert worden. Jeder Beitrag endet mit Tipps und Hilfestellungen für Jugendlichen. Ferner besteht die Möglichkeit, über ein Forum Kommentare zu den Beiträgen zu hinterlassen.

Dadurch, dass jeder Nutzer heute nicht mehr nur Datennutzer, sondern gleichzeitig Datenproduzent ist, ist das Datenmanagement eine herausfordernde Aufgabe, die es auch im Informatikunterricht zu thematisieren gilt. (Grillenberger und Romeike 2017) stellen in ihrem Beitrag ausgewählte Themen vor und bemerken, dass Aspekte wie Datenschutz und Datensicherheit, die in der Vergangenheit im Unterricht eher vernachlässigt worden sind, in diesem Zusammenhang aber an Bedeutung gewinnen. Die Themen, die mehr oder weniger ausgearbeitet sind, lauten: „Verwaltung und Nutzung großer Datenmengen: Big Data“, „Verteilte Datenspeicher“, „Datenanalyse durch Data Mining“, „Datenauswertung in Echtzeit – Datenstromsysteme“ und „Metadaten“. Den Autoren ist wichtig, dass ausgehend von den klassischen Datenbanken Big Data als Ausgangspunkt dient, um vor allem auch den „Wandel von kausalitätsbasierter zu immer häufiger korrelationsbasierter Datenanalyse“ darzustellen und den häufig genannten „Paradigmenwechsel im Bereich der Datenverwaltung und -analyse“ zu betonen

[85] Siehe https://tu-dresden.de/ing/informatik/smt/ddi/schulinformatik/koenigsteiner-gespraeche (zuletzt geprüft am 27.04.18)
[86] Siehe www.virtualstories.ch (zuletzt geprüft am 09.09.2019)

(Grillenberger und Romeike 2017, S. 45). Es geht letztendlich nicht nur darum, das Bewusstsein für Gefahren zu thematisieren, sondern den Schülern auch die Möglichkeiten des Selbernutzens und Profitierens aufzuzeigen. Erste Ideen zur Umsetzung finden sich bei (Grillenberger und Romeike 2015). Die Autoren schlagen vor, einerseits Data Mining und Big Data und andererseits Datenstromanalysen zu betrachten. Jedoch liegen zu diesem Thema zum jetzigen Zeitpunkt noch keine Erfahrungen in der unterrichtlichen Umsetzung vor, die dem Autor bekannt sind.

Von der Siemens-Stiftung wurde eine Webseite[87] mit Materialien zum Thema Big Data implementiert, die sich in mehrere Themenfelder (z. B. „Big Data in der Praxis", „Internet der Dinge", „Staatliche Überwachung" und „Personalisierte Online-Werbung") gliedert. Je nach Themenfeld werden Medienpakete bestehend aus Bildern, Videos, Tondokumenten, Textbeiträgen und sogenannten Interaktivem angeboten. Die Hintergrundinformationen für die Lehrkräfte sind so ausgearbeitet, dass sie auch für Nicht-Informatiker verständlich sind.

Mit dem Stationsspiel *Big Up 4 Big Data* stellt (Gmeinwieser 2017) eine Unterrichtsprojekt vor, dessen Ziel es ist, „Bewusstsein für den Wert und den Schutz persönlicher Daten zu entwickeln (Gmeinwieser 2017, S. 64). Die Schüler werden so in den Themenkomplex miteingebunden, dass sie selber erleben, wie personenbezogene Daten gesammelt, überwacht, analysiert und ausgewertet werden. Die Gruppen werden in drei Teams geteilt, von denen die ersten beiden Teams sich an den Stationen anhand der Arbeitsaufträge, die „einen mehr oder weniger offensichtlichen Alltagsbezug zum Themenkomplex *Big Data*" haben (Gmeinwieser 2017, S. 66), duellieren und das dritte Team das Verhalten und die Preisgabe persönlicher Daten festhält. Nur das dritte Team kennt den Hintergrund des Spiels. Auf der Basis der Beobachtungen (Datenspuren) wird am Spielende ein Profil des „potentiellen" Duellgewinners erstellt. „Wichtig ist, im Anschluss … einen Bezug von den Stationen zum Alltag der Jugendlichen herzustellen … Ziel ist es nicht, den Hintergrund jeder einzelnen Station aufzudecken, sondern punktuell an den Interessenfeldern der Teilnehmenden anzusetzen und das Gespräch zu fördern" (Gmeinwieser 2017, S. 68).

Im Rahmen des Promotionsprojekts ist im Frühjahr 2019 unter Betreuung des Autors eine Masterarbeit erstellt worden, in der vorhandene Unterrichtsmaterialien zum Erwerb von Datenschutzkompetenz qualitativ untersucht worden sind. Dazu hat (Makosch 2019) auf der Basis zweier, existierender Kataloge[88] – dem sog. Bielefelder Raster (Makosch 2019, S. 11) und dem sog. Reutlinger Raster (Makosch 2019, S. 10) – zur Beurteilung von Schulbüchern und Unterrichtsmaterialien eine eigene Kriterienliste entwickelt (Makosch 2019, 85f). Anhand dieser Liste, die neben formalen Angaben wie Autor, Titel, Materialart, Jahrgangsstufe usw. Faktoren zur Einschätzung von Sachrichtigkeit, Schülergemäßheit, Kompetenzorientierung, Lernprozesssteuerung und ähnlichem enthält, hat sich die Autorin insgesamt 22 Materialien vor-

[87] Siehe https://medienportal.siemens-stiftung.org/111955 (zuletzt aufgerufen am 09.09.2019)

[88] Es sind auch weitere Verzeichnisse angeschaut worden, jedoch haben die beiden oben Genannten den maßgeblichen Einfluss gehabt.

genommen. Diese Sammlung sind Beiträge von Printmedien, Arbeitsmaterialien, Unterrichtsreihen, Webseiten usf., deren Auflistung sich in Anhang A2.1 befindet. Aus der Beurteilung der Materialien folgert (Makosch 2019, S. 69–70), dass

- Aufgaben ohne notwendige Informationen/Materialien gestellt werden, sodass vieles erst selbst recherchiert werden muss,
- häufig gleiche Themen und Aufgabenstellungen zu finden sind (z. B. Rechte in Bezug auf das eigene Bild oder in Bezug auf personenbezogene Daten, …), weshalb neue Themenbereiche erschlossen werden könnten,
- Themen vielfach nur theoretisch ausgearbeitet werden, sodass keine Handlungskompetenz gefördert werden kann, und
- Themen singulär (anstatt aufeinander aufbauende Unterlagen) betrachtet werden.

Bei allen Forderungen nach verbesserten Materialien hängt der Nutzen vor allem vom Einsatz im Unterricht ab, weshalb die Lehrkraft eine entscheidende Rolle spielt. Eine sehr gute Qualität von Materialien ist zwecklos, wenn die Lehrer damit nicht arbeiten können (Gräsel 2010).

Im Rahmen der hier beschriebenen Arbeit ist die Webseite *YoungData*[89] beurteilt worden, auf die an dieser Stelle besonders eingegangen werden soll. Es ist ein Jugendportal, welches von den unabhängigen Datenschutzbehörden des Bundes und der Länder sowie des Kantons Zürich (alle vertreten mit eigenen Unterseiten) angeboten und vom LfDI Rheinland-Pfalz gehostet wird. Es dient als Informationsseite zum Thema *Datenschutz* und *Informationsfreiheit* mit Tipps für ein sinnvolles Verhalten im Internet und der Nutzung von (Smartphone-)Apps. Zu den Inhalten zählen Themen wie *DSGVO*, *Digitale Selbstverteidigung* (z. B. Passworterstellung, Phishing-Mails, Browser-Einstellungen), *Soziale Netzwerke*, *Konsolenspiele*, *Smartphones*, *Video-Überwachung* und *Cybermobbing*. Anbieter wie *Google*, *Facebook*, *WhatsApp*, *Skype* und *Spotify* werden mit ihren Geschäftspraktiken ebenso vorgestellt, wie die Sprachdienste *Siri* und *Alexa*. Ein Bereich widmet sich dem Aspekt *Datenschutz und Schule*. Der große Bereich *Internet* beinhaltet Themen wie *Cloud-Computing*, *Internet of Things*, *Big Data*, *Fake-News*, *Netiquette* und *Datenspuren*. Für rheinland-pfälzische Schulen existiert seit 2010 zudem das Angebot der Buchung für Schülerworkshops, die in der Regel vier Unterrichtsstunden umfassen und zu denen ausgebildete Referenten an die Schule fahren. Das Angebot reicht von Grundschulen (Klassenstufe 3 und 4) bis zu Sekundarschulen. Die Workshopthemen orientieren sich an den Themen der Webseite. Die Konzepte und die Materialien stehen auf der Homepage zur Verfügung, sodass fachlich fundierte Lehrer diese auch selber im Unterricht einsetzen können.

Auch in wenigen der doch recht übersichtlichen Anzahl an Informatik-Schulbüchern wird das Thema *Datenschutz* aufgegriffen, aber nicht in einem so ausreichenden Maß behandelt, dass damit eine Datenschutzkompetenz bei den Schülern ausgebildet werden kann. Die betrachteten Schulbücher für die weiterführenden Schulen, erschienen im Zeitraum 2006 bis 2015, behandeln das Thema *Datenschutz*, welches häufig mit dem Thema *Datensicherheit* verknüpft

[89] Siehe https://www.youngdata.de (zuletzt geprüft am 27.09.19)

ist, im Schnitt auf vier Buchseiten. Neben einer didaktisch reduzierten Definition des Datenschutzes werden vor allem das Bundesdatenschutzgesetz, die Funktion des Datenschutzbeauftragten und das Recht auf informationelle Selbstbestimmung (in einigen Fällen in Verbindung mit dem Volkszählungsurteil 1983) angesprochen. In den neueren Büchern werden auch die Themen *Soziale Netzwerke* und *E-Commerce* aufgenommen.

In Rheinland-Pfalz wurde vor rund zehn Jahren als elektronisches Schulbuch die Seite *infschule.de* eingerichtet, die sich im Laufe der Zeit über die Landesgrenzen hinaus zu einem beliebten Portal für den Informatikunterricht entwickelt hat und wissenschaftlich von der Universität Siegen evaluiert wurde[90]. In Kapitel 12 *Informatik und Gesellschaft* findet sich ein Unterkapitel *Datenschutz*, in dem neben der Klärung von Grundbegriffen und Datenschutzrechten auch die Anwendung von Beispielen aus dem Schulleben thematisiert werden. Ein Verweis auf den Selbstdatenschutz (durch Verlinkung auf die Informationsseite des LfDI), die Webseite Yo*ungData* und die Hambacher Erklärung zu Datenschutz und Künstliche Intelligenz runden den Abschnitt ab.

Für Schüler der Primarstufe existiert die Webseite *www.internet-abc.de*, die Lernmodule zu unterschiedlichen Themen enthält. Innerhalb des Moduls *Achtung, die Gefahren! – So schützt du dich* ist eine Sequenz mit dem Thema *Datenschutz – das bleibt privat!* integriert, die durch Informationstexte, mehrere Quiz und einen Videofilm interaktiv die Kinder im Umgang mit persönlichen Daten im Netz vorbereitet. Zudem gibt es für (fachfremde) Lehrkräfte ein Arbeitsheft mit didaktischen und methodischen Erläuterungen und ergänzenden Arbeitsblättern. Eine nähere Betrachtung der Seite findet nicht statt, da in der vorliegenden Arbeit die Jugendlichen der Sekundarstufe im Fokus stehen.

Der Vollständigkeit halber wird abschließend noch erwähnt, dass im Netz durch Verbraucherschutzzentralen, durch Initiativen wie *Klicksafe* und *internet-abc* und durch Ministerien Materialien für Eltern herausgegeben werden, um sie bei der Ausbildung ihrer eigenen Datenschutzkompetenz und der ihrer Kinder zu unterstützen. Da diese jedoch keinen Einsatz im Unterricht finden, werden sie an dieser Stelle auch nicht weiter betrachtet.

[90] Siehe MNU Deutscher Verein zur Förderung des mathematischen und naturwissenschaftlichen Unterrichts e. V. (Hg.) (2017): Tagungsband 108. MNU-Bundeskongress. 06. bis 10. April 2017, Aachen. S. 73

2.5. Ausblick

Zusammenfassend kann festgehalten werden:

1. Ein Mangel an Datenschutzkompetenz bei Kindern und Jugendlichen kann (trotz vorhandener (Unterrichts-)Materialien) aus Studien und Untersuchungen abgeleitet werden.
2. Es existieren Kompetenzmodelle, aber keines, welches ausschließlich Datenschutzkompetenz beschreibt. Ferner ist der Begriff *Datenschutzkompetenz* als solcher auch nicht differenziert genug definiert.
3. Datenschutz ist ein fachübergreifendes Thema, sodass auch andere Fächer in die Behandlung der Thematik mit eingebunden werden können.
4. Es existiert eine größere Anzahl an Unterrichtsmaterialien und Unterrichtsreihen (z. T. auch für fachfremde Lehrkräfte und andere Unterrichtsfächer), die teilweise an Aktualität eingebüßt haben oder didaktisch unzureichend ausgearbeitet sind.

Aus diesen Erkenntnissen kann man die Forderung ableiten, dass das Thema *Datenschutz* Bestandteil eines zeitgemäßen Informatikunterrichts sein muss, woraus sich das Motiv für die vorliegende Arbeit ergibt. Im folgenden Kapitel werden im ersten Schritt ein Datenschutzkompetenzmodell und eine Definition für Datenschutzkompetenz hergeleitet und abschließend Datenschutzkompetenzen formuliert.

„Wer auf *die* Kompetenzdefinition hofft, hofft vergeblich."
Erpenbeck, zitiert nach (Gapski 2006)

3. Ein Datenschutzkompetenzmodell

Eine datenschutzkonforme Nutzung des Internets beruht auf dem Zusammenspiel zwischen einer Form von Selbstdatenschutz, Systemdatenschutz und dem Vertrauen in das technische System, deren Entwickler und den Dienstanbietern. Nur auf diesem Weg ist eine Internetnutzung überhaupt möglich (vgl. Abschnitt 1.2). Dabei ist Vertrauen eine notwendige Voraussetzung dafür, nach einer Risikoabschätzung das (bewusst kalkulierte) Risiko einzugehen. Diesen Zusammenhang klärt das Vertrauensmodell von Mayer, Davis und Schoorman (Mayer et al. 1995) auf, indem es die Risikowahrnehmung deutlich macht und das Zusammenspiel zwischen Vertrauen und Kontrolle in einer risikobehafteten Kooperation (hier zwischen Internet-Nutzern und dem Internet mit seinen Anwendungen) beschreibt (vgl. Abschnitt 3.2). Um eine Risikobewertung vornehmen zu können, werden Methoden der IT-Sicherheit angewendet, wie sie im Referenzmodell der IT-Sicherheitsanalyse beschrieben sind (Grimm et al. 2016) (vgl. Abschnitt 3.3).

In dem ersten Abschnitt wird zunächst ein Medienkompetenzmodell vorgestellt (Six und Gimmler 2013) und gezeigt, dass Anforderungen an eine datenschutzbezogene Kompetenz der Mediennutzung durch das Modell durchaus beschrieben werden können. Aber Datenschutzkompetenz ist zudem wesentlich von der Fähigkeit geprägt, Risiken zu erkennen und zu bewerten und zugehörige Handlungsstrategien (etwa Vermeidung oder Anwendung von Tools) abzuleiten.[91] Diese Fähigkeit ist im vorhandenen Medienkompetenzmodell jedoch nicht abgebildet. Das Modell ist daher entsprechend zu erweitern, indem die vorhandenen Kompetenzen ausgewählt und interpretiert werden. Auf diese Weise wird ein Weg zur Risikobewertung und ihrer Einbettung in datenschutzriskante Kooperationen ausgeführt (vgl. Abschnitt 3.4).

Damit ist schließlich ein sogenanntes *Datenschutzkompetenzmodell* abgeleitet. Es liefert eine Vorlage, die es ermöglicht, Untersuchungen zum Datenschutz und zur Risikobewertung bei Schülern durchzuführen (vgl. Kapitel 4). Aus den Ergebnissen lassen sich Hinweise für die Ausprägung von Lehrinhalten zur Verbesserung der Datenschutzkompetenz ableiten.

3.1. Medienkompetenz und Medienkompetenzmodelle

Weinert definiert Kompetenz als „die bei Individuen verfügbaren oder durch sie erlernbaren kognitiven Fähigkeiten und Fertigkeiten, um bestimmte Probleme zu lösen, sowie die damit verbundenen motivationalen, volitionalen und sozialen Bereitschaften und Fähigkeiten, um

[91] Ähnliches formuliert (Baacke 1996, S. 25), wenn er zur Medienkompetenz schreibt, dass „das Konzept ‚Medienkompetenz' … nicht auf ‚Fähigkeit' oder ‚Qualifikation' [zu verkürzen sei], sondern … in seiner begrifflichen Reichweite ein Stück Demokratie- und Kommunikationstheorie [umgreift]".

die Problemlösungen in variablen Situationen erfolgreich und verantwortungsvoll nutzen zu können“ (Weinert 2002, S. 27).[92]

Auf Basis dieser Definition sind seit dieser Zeit Kompetenzmodelle zu unterschiedlichen Themen in vielen wissenschaftlichen Disziplinen entwickelt worden – so auch im Fall der Medienkompetenz. Wie Gimmler schon in (Gimmler 2012) zeigt, ist das Medienkompetenzmodell, welches in (Six et al. 2007) vorgestellt wird, geeignet, um in einem gewissen Maß Datenschutzkompetenz zu beschreiben. Dieser Aspekt soll der Ausgangspunkt für die nun weiteren Überlegungen sein. Doch zuvor wird in einem ersten Schritt der Begriff der *Medienkompetenz* erläutert.

Dieser Begriff ist vielschichtig und wird aus unterschiedlichen Ansätzen abgeleitet (Gapski 2006, S. 17). (Neumann-Braun 2000) schreibt z. B. dazu: „Hier liegen eine Fülle von Definitionen vor – weiter wie enger gefasste.“ Dabei umfasst eine engere Sicht, dass „Menschen … in beruflichen wie in privaten Handlungskontexten mit den neuen Medien- und Informationstechniken *wissend* umgehen können [sollen]“. Betrachtet man den Begriff der Medienkompetenz in einem weiteren Sinn, so gehört zusätzlich dazu, „mit den neuen Medien auch *gestaltend* sich selbst, die Mitwelt und Umwelt *zu reflektieren* … Diese Sichtweise impliziert, dass Medienkompetenz zu einem *Teil* der allgemeineren Schlüsselqualifikationen der *kommunikativen Kompetenz* wird, über die moderne Subjekte in der modernisierten Informationsgesellschaft verfügen müssen“ (Neumann-Braun 2000, S. 1).[93] Nuissl schreibt in der Vorbemerkung von (Rein 1996) ebenfalls, dass man von dem reinen Wissen bzw. der reinen Wissensvermittlung wegkommen muss, hin zu einer Form von Orientierung (Rein 1996, S. 7).

Zur Definition von Medienkompetenz findet man z. B. in (Baacke 2004) und (Rein 1996) verschiedene Ausführungen.[94] Diese Definitionen decken sich inhaltlich im Allgemeinen gut mit kleinen Abstufungen, sodass der Autor sich im Folgenden auf die Definition von Six und Gimmler konzentriert, da darauf auch das später folgende Medienkompetenzmodell fußt.

Laut (Six et al. 2007) ist **Medienkompetenz** (angelehnt an (Gapski 2001, S. 58)) „die Fähigkeit für einen kritischen, selbstbestimmten, kreativen und verantwortlichen Medienumgang […] Kompetenter Medienumgang zeichnet sich dadurch aus, dass er selbstbestimmt, reflektiert und selbstreguliert sowie an eigenen Anliegen orientiert, zielgerichtet und funktional gleichzeitig aber auch persönlich sowie sozial verträglich und angemessen ist“ (Six et al. 2007, S. 281).[95]

[92] Dadurch werden „sieben ‚Facetten‘ [umfasst]: Fähigkeit, Wissen, Verstehen, Können, Handeln, Erfahrung und Motivation“ (Schecker und Parchmann 2006, S. 46). Diese Facetten stehen nicht getrennt nebeneinander, sondern Wechselwirken miteinander und bedingen sich gegenseitig (vgl. Weinert 2001).

[93] Das Medienkompetenz eine „Schlüsselqualifikation in der Informationsgesellschaft“ ist und „im Spiel der politischen, rechtlichen, pädagogischen oder wirtschaftlichen Diskurs … je nach Akteur und Kontext ein anderes Verständnis von Medienkompetenz“ vorherrscht, betont auch (Gapski 2006, S. 14).

[94] Hamm schlägt in (Rein 1996) sogar vor, eher den Begriff Informationskompetenz statt Medienkompetenz zu nutzen, da er ihr passender erscheint. Auf eine Überschneidung der beiden Begriffe weist (Gapski 2006, S. 26) hin. Zum Begriff *Informationskompetenz* siehe Abschnitt 2.1.5.

[95] (Dörge 2012) schreibt, dass seit Einführung in den 70er Jahren der Begriff Medienkompetenz sehr populär ist, sodass eine Forderung zur Aufnahme in Unterrichtspläne immer wieder laut wird. Jedoch ist dabei der Abstrak-

Bei der Entwicklung eines Medienkompetenzmodells geht das Konzept von (Six und Gimmler 2013, S. 104) von einem Ressourcen-orientierten Ansatz aus. Der „Stellenwert individueller Ressourcen als eine wesentliche Einflussgröße des Handelns und Verhaltens und damit auch für den Umgang mit verschiedenen Medien“ steht im Mittelpunkt der Ausgangsüberlegungen (Six und Gimmler 2013, S. 104). Dabei stellen Kompetenzen wichtige Ressourcen dar, da Kompetenzen Wissensbestände, Fähigkeiten und Fertigkeiten beschreiben. Eine Anzahl von Basiskompetenzen (z. B. Lesekompetenz, Kommunikationskompetenz, Selbstkontrollkompetenz) werden bei der Entwicklung des Modells vorausgesetzt, wobei die Grenzen zwischen Basiskompetenzen und der eigentlichen Medienkompetenz als fließend bezeichnet werden.

(Six und Gimmler 2013, S. 105) postulieren acht Dimensionen der Medienkompetenz, wobei die ersten vier als *Medienwissen* und die anderen vier als *Fähigkeiten und Fertigkeiten* angesehen werden.

Medienwissen	**Fähigkeiten und Fertigkeiten**
1. Orientierungswissen (OW)	5. Urteilskompetenz (UK)
2. Hintergrundwissen (HW)	6. Auswahl- und Nutzungskompetenz (ANK)
3. Gestaltungswissen (GW)	7. Rezeptions- und Verarbeitungskompetenz (RVK)
4. Prozedurales Wissen (PW)	8. Kommunikatorkompetenz (KK)

Tab. 3.1: Dimensionen der Medienkompetenz (Six und Gimmler 2013, S. 105)

Bei dem Orientierungswissen handelt es sich um Wissen in Bezug auf Medienangebote und deren Kennzeichen und Spezifika. Dabei stehen die funktionale Einsetzbarkeit, deren Grenzen und auch die Wirkungen im Vordergrund. Wissen über technische Bedingungen und besonderen Anforderungen spielt bei elektronischen Medien eine zusätzliche Rolle. Das Hintergrundwissen „umfasst Kenntnisse über Rahmenbedingungen, die für die Medienbewertung und -auswahl wie auch für die Produktion eigener Medien(-inhalte) und deren Verbreitung relevant sind“ (Six und Gimmler 2013, S. 106). Die Dimension des Gestaltungswissens beschreibt Wissen über Kenntnisse von Symbolen, von Gestaltungsstrategien und die technische Manipulierbarkeit von Inhalten. Das prozedurale Wissen ist gekennzeichnet durch „theoretisches Knowhow bezüglich der Mediennutzung/-einsatz, -produktion und -distribution“ (Six und Gimmler 2013, S. 106). Handlungsabläufe (hardware- wie softwareseitig) und dabei zu beachtende Regeln stehen im Vordergrund dieser Dimension.

Unter Urteilskompetenz wird die Urteilsbildung sowohl der Angebote an Medien als auch der eigenen Weise, die Medien zu nutzen, verstanden. Neben dem Wissen aus den ersten beiden Dimensionen spielt auch „die persönliche und soziale Verträglichkeit und Angemessenheit“ eine Rolle (Six und Gimmler 2013, S. 106). Als formale Kriterien für die Bewertung von Medien sind die Handhabbarkeit und die Sicherheit ebenso wichtig wie inhaltliche und formale Aspekte. Durch „die Fähigkeit zur selbstbestimmten, zielorientierten und reflektierten Auswahl

tionsgrad so offen, dass keine Operationalisierung angegeben wird. Da für eine sinnvolle und erfolgreiche Mediennutzung informatisches Verständnis notwendig ist, liegt hier logischerweise ein Problem vor (S. 91). Mithilfe des Dagstuhl- bzw. Frankfurt-Dreieck soll diesem Problem entgegengewirkt werden (vgl. Abschnitt 2.2.5).

und Nutzung von Medien(-angeboten)“ wird die Auswahl- und Nutzungskompetenz beschrieben (Six und Gimmler 2013, S. 107). Mit der Rezeptions- und Verarbeitungskompetenz werden „Fähigkeiten und Fertigkeiten einer funktional angemessenen und persönlich verträglichen Rezeption und Verarbeitung der Medieninhalten“ angesprochen (Six und Gimmler 2013, S. 107). Da ein „Komplex psychischer Prozess“ hierbei stattfindet, ist die Rezeptions- und Verarbeitungskompetenz notwendig, damit dies „in einer persönlich verträglichen Weise“ geschieht (Six und Gimmler 2013, S. 107). Die Kommunikatorkompetenz beschreibt „spezielle Fähigkeiten und Fertigkeiten […], [die] die Entwicklung und Veröffentlichung bzw. Verbreitung von Medieninhalten [erfordert]. Dabei kann es sich um eigene Medienprodukte handeln […] oder um Inhalte, die man per Kommunikationsmedien anderen übermittelt“ (Six und Gimmler 2013, S. 107).

In dem Modell von (Six und Gimmler 2013) kommt als ein weiterer wichtiger Aspekt der motivationale Faktor ins Spiel, der schon in der Definition von Weinert eine Rolle spielt. „Hierzu gehört zunächst einmal die Einsicht in die Notwendigkeit von Medienkompetenz und die Bereitschaft, mit Medien möglichst kompetent umzugehen“ (Six und Gimmler 2013, S. 108). Dies verlangt bei der Mediennutzung, auf seine Ressourcen in Verbindung mit vorhandener Medienkompetenz zurückzugreifen und die Erfahrungen mit dem eigenen Medienumgang zu nutzen.

Die Abb. 3.1 fasst das Gesagte noch einmal zusammen.

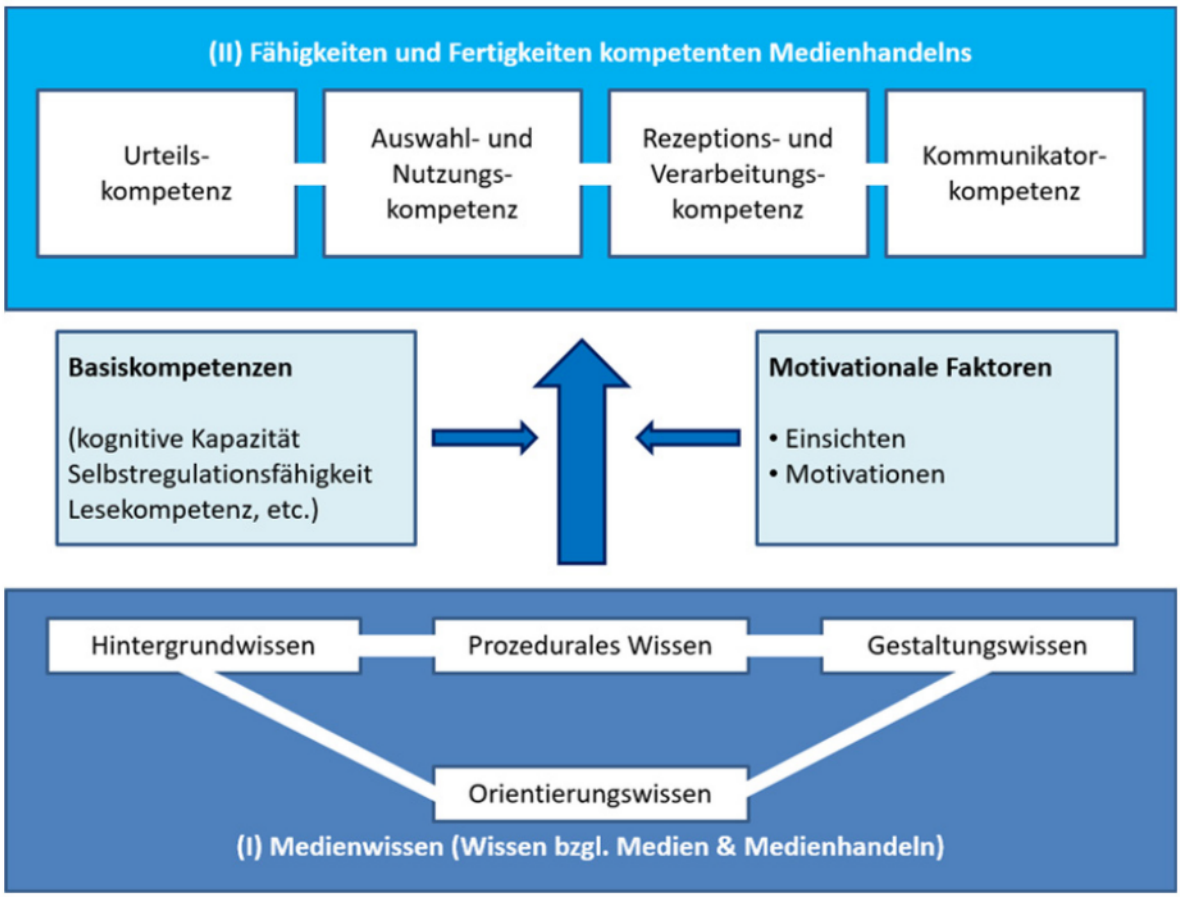


Abb. 3.1: Ressourcenorientiertes Modell der Medienkompetenz (Six und Gimmler 2013, S. 108)

Zwischen der Medienkompetenz, den motivationalen Faktoren und dem Medienumgang wirkt eine Wechselwirkung, die (Six und Gimmler 2013, S. 109) durch folgende Abbildung ausdrücken.

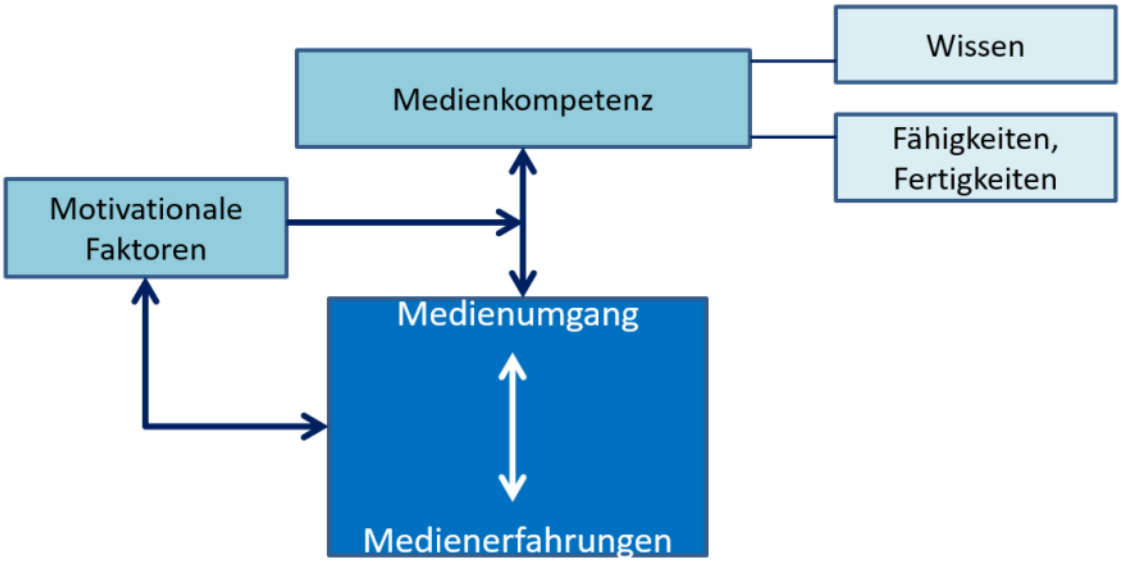


Abb. 3.2: Wechselwirkungen zwischen Medienkompetenz, motivationalen Faktoren und Medienumgang (Six und Gimmler 2013, S. 109)

„Dass es sich bei Medienkompetenz um eine Handlungskompetenz handelt", betonen schon (Vollbrecht und Mägdefrau 1999, S. 56). Dieser Aspekt ist für die Entwicklung des Datenschutzkompetenzmodells und den später abgeleiteten Handlungsempfehlungen sehr wichtig, da Datenschutzkompetenz ein Handeln verlangt.[96]

Ein weiteres Modell, das ebenfalls zur Beschreibung von Medienkompetenz genutzt wird, ist das von (Baacke 1996).[97] Baacke geht dabei von dem Begriff der Medienkompetenz aus (S. 114) und leitet daraus vier Dimensionen ab, die wiederum in Unterdimensionen geteilt sind.[98]

[96] Wie schon bei dem informatischen Verständnis des Medienkompetenzbegriffs gibt es eine ähnliche Problematik bei den Medienkompetenzmodellen. (Zorn 2010) schreibt, „dass die Integration des Computers in eine medienpädagogische Perspektive vor allem durch Subsumierung in bestehende Modelle erfolgte: Auf den Computer und Digitale Medien wird in den Medienkompetenzmodellen selten Bezug genommen, und wenn, dann ohne Berücksichtigung ihrer spezifischen softwarebasierten Eigenschaften" (S. 42). Der Computer wird von Medienwissenschatlern nur als ein Werkzeug gesehen, sodass Informatikkonzepte außer Acht gelassen werden. Eine klare Abgrenzung der Begriffe *Medienkompetenz* und *informatischer Bildung* liegt nicht vor (Dörge 2012,S. 91). Mithilfe des Dagstuhl- bzw. Frankfurt-Dreieck soll diesem Problem entgegengewirkt werden (vgl. Abschnitt 2.2.5).

[97] Das Modell ist auch beschrieben in (Baacke 1998) und (Baacke 2004).

[98] Das gleiche Modell mit anderen Begriffen nutzt (Schorb 1998), nur spricht er von den Dimensionen „Kritische Reflexivität", „Orientierungs- und Strukturwissen", „Handlungsfähigkeit" und „Kreative, soziale Interaktion" (Zacharias 2004).

Die folgende Tabelle fasst diese zusammen. In der dritten Spalte sind den Dimensionen von Baacke die Dimensionen des Six/Gimmler-Modells zugeordnet.

Dimension n. Baacke	Unterdimension nach Baacke	Gegenüberstellung Six/Gimmler
Medienkritik	analytisch	OW, HW, GW, UK
	reflexiv	
	ethisch	
Medienkunde	informativ	OW, HW, GW, PW, ANK
	instrumentell-qualifikatorisch	OW, PW, ANK
Zielorientierung	rezeptiv, anwenden	RVK, KK
	interaktiv, anbieten	
Mediengestaltung	innovativ	GW, PW, ANK, KK
	kreativ	

Tab. 3.2: Medienkompetenzmodell nach Baacke und Gegenüberstellung zum Six/Gimmler-Modell

Die Dimensionen der Medienkritik und der Medienkunde fasst Baacke auch zur Dimension der Vermittlung zusammen.

Ordnet man den Unterdimensionen bei Baacke die Dimensionen des Six/Gimmler-Modells zu[99], so stellt man fest, dass die Dimensionen des Six/Gimmler-Modells (teilweise mehrfach) vorkommen. D. h. beide Modelle sind bemüht die Medienkompetenz umfassend zu beschreiben. Jedoch ist das Modell von Baacke im Vergleich zu dem Modell von Six/Gimmler viel konkreter an Medien orientiert. Zudem sind das Six/Gimmler-Modell und dessen Dimensionen weiter gefasst, damit unabhängiger vom Medienbegriff und deutlicher an Kompetenzen – also Wissen, Fähigkeiten und Fertigkeiten – ausgerichtet, sodass es dem Autor geeigneter als Ausgangspunkt für ein Datenschutzkompetenzmodell erscheint. Zudem ist zu berücksichtigen, dass das Modell von Six/Gimmler gut zehn Jahre aktueller ist und daher den Kompetenzbegriff von Weinert berücksichtigt, der den hier gemachten Überlegungen zugrunde liegt.

(Gimmler 2012) sieht in dem von ihm beschriebenen Medienkompetenzmodell eine ausreichende Beschreibung von Datenschutzkompetenz. Der Autor widerspricht dem, da in keiner Form der wichtige Aspekt des Risikos betrachtet wird. Somit ist dieses Modell unzureichend. In den folgenden Abschnitten wird dieser Aspekt aufgegriffen.

Abschließend sei erwähnt, dass die (Länderkonferenz MedienBildung 2015) ein Medienkompetenzmodell veröffentlicht hat, das folgende Kompetenzbereiche umfasst:

- „Informationen recherchieren und auswählen
- Mit Medien kommunizieren und kooperieren
- Medien produzieren und präsentieren
- Medien analysieren und bewerten
- Mediengesellschaft verstehen und reflektieren“ (S. 3)

[99] Zu den Abkürzungen in Spalte 3 siehe Tabelle 3.1.

Diese Bereiche stehen in gewünschten „vielfältige[n] Wechselbeziehungen und Zusammenhänge[n]“ zueinander, „wobei der Kompetenzbereich ‚Mediengesellschaft verstehen und reflektieren‘ als umfassende Bezugsebene zu sehen ist. Das sachgerechte *Bedienen und Anwenden* ist als Voraussetzung für medienkompetentes Handeln stets mitgedacht“ (Länderkonferenz MedienBildung 2015, S. 3).

Diese Gruppe betont, dass ebenfalls „die Relevanz juristischer Aspekte im Umgang mit digitalen Medien“ eine Rolle spielt. Ein Aspekt der für die Datenschutzkompetenz entscheidend ist. Medienkompetenz „gewinnt“ insgesamt gesehen „den Status einer unverzichtbaren Kulturtechnik“ (Länderkonferenz MedienBildung 2015, S. 2).

Ab Seite 6 des Positionspapiers sind die Kompetenzerwartungen, die sich an einer 10. Klasse orientieren, nach den Bereichen gegliedert ausformuliert (Inhalte, erforderliches Grundwissen und methodische Hinweise). Dabei sollen Querverweise aufzeigen, dass „die einzelnen Bereiche keinesfalls als abgeschlossen zu betrachten sind, sondern Medienkompetenz vielmehr als systemische Qualität begriffen werden sollte, deren Erwerb durch die Schülerinnen und Schüler zugleich Voraussetzung für ihre selbst bestimmte, aktiv handelnde, sozial verantwortliche und kreativ gestaltende Teilhabe an der Gesellschaft ist“ (Länderkonferenz MedienBildung 2015, S. 5). Im Folgenden werden nur die Bereiche zitiert, die für das Thema *Datenschutz* eine Rolle spielen; zur Gegenüberstellung mit dem Six/Gimmler-Modell sind die Dimensionen dieses Modells als blaugeschriebene kursive Einträge gleichzeitig mit in die Tabellen aufgenommen worden[100]:

Kompetenzbereich: Mit Medien kommunizieren und kooperieren	
Kompetenzerwartungen in Bezug auf …	Inhalte und Grundwissen:
… Verantwortungsbewusstsein, Angemessenheit und Adressatenbezug	
• ergebnisorientiert sowie verantwortungsbewusst kommunizieren *(HW, OW, UK, ANK, KK)*	Grundlagen des Urheber- und Persönlichkeitsrechts *(HW)*
… Medienunterstützte Kommunikation und Kooperation beim Lernen	
• digitale Lernumgebungen in ihren Grundfunktionen beherrschen und zur Gestaltung individueller wie kollaborativer Lernprozesse nutzen *(HW, OW, GW, PW, UK, ANK)*	Datenschutz *(HW)*
… Kommunikationsbedingungen in der Mediengesellschaft	
• die nationale wie globale Mediengesellschaft hinsichtlich ihrer kommunikativen Angebote, Möglichkeiten und Potenziale untersuchen und reflektieren *(HW, OW, UK, ANK, RVK)*	Recht auf informationelle Selbstbestimmung *(HW)*

Tab 3.3: Ausschnitt Kompetenzbereich *Mit Medien kommunizieren und kooperieren* (Länderkonferenz MedienBildung 2015, 7-8)

[100] Zu den Abkürzungen der Dimensionen siehe Tabelle 3.1.

Kompetenzbereich: Medien analysieren und bewerten	
Kompetenzerwartungen in Bezug auf …	Inhalte und Grundwissen:
… Bedeutung und Wirkung von Medienangeboten	
• medialen Angeboten und Identifikationsfiguren mit kritischer Distanz begegnen *(OW, HW, GW, PW, UK, ANK, RVK, KK)*	jugendgefährdende Inhalte/Angebote, Persönlichkeitsrechte, Datenschutz; Chancen und Risiken Sozialer Netzwerke *(HW, GW)*

Tab 3.4: Ausschnitt Kompetenzbereich *Medien analysieren und bewerten* (Länderkonferenz MedienBildung 2015, S. 13)

Kompetenzbereich: Mediengesellschaft verstehen und reflektieren	
Kompetenzerwartungen in Bezug auf …	Inhalte und Grundwissen:
… Eigener Mediengebrauch	
• Bewusstsein für Datensicherheit und Datenmissbrauch entwickeln und anwenden *(HW, GW, UK, ANK, RVK, KK)*	Big Data, Open Data, Datenspuren im Internet, Datenschutz Privat-/Intimsphäre vs. Öffentliches Interesse; Schutz der Persönlichkeit durch Aufklärung, Prävention, Reglementierung und eigenes kompetentes Verhalten *(OW, HW, GW, PW)*

Tab 3.5: Ausschnitt Kompetenzbereich *Mediengesellschaft verstehen und reflektieren* (Länderkonferenz MedienBildung 2015, S. 14)

Die Gegenüberstellung zeigt, dass in den ausgewählten Bereichen sich die Dimensionen des Six/Gimmler-Modells wiederspiegeln, sodass sich das Medienkompetenzmodell von Six/Gimmler als Ausgangspunkt für die weiteren Betrachtungen eignet.

3.2. Das Vertrauensmodell von Mayer, Davis und Schoorman

Im Zusammenhang mit Datenschutzkompetenz spielt die Betrachtung des Risikos eine entscheidende Rolle, weil durch die Internetnutzung Daten preisgegeben werden, die bei einem möglichen Missbrauch von anderer Seite eine Gefährdung der Privatheit des Nutzers bedeuten. Damit begibt er sich in Gefahr und muss ein Risiko tragen, der Gefahr zu entgehen, die Gefahr abzuwehren oder sie zu ertragen. Risiko steht wiederum in einem Zusammenhang mit Vertrauen, sodass in diesem Abschnitt das Vertrauensmodell von Mayer, Davis und Schoorman vorgestellt wird.

Eine datenschutzkonforme Nutzung des Internets ist ohne eine Kooperation mit verschiedenen Parteien, denen man Vertrauen entgegenbringen muss, gar nicht möglich (vgl. Abschnitt 1.2). So muss man z. B. dem Datenempfänger vertrauen, dass er diese nicht missbraucht, oder dass z. B. zwischen dem Rechner des Nutzers und dem Server der Bank eine verschlüsselte Verbindung aufgebaut ist. Das Vertrauensmodell von Mayer, Davis und Schoorman „modelliert das Luhmannsche Verständnis von Vertrauen als Entscheidung einer vertrauenden Person („Trustor“) sich auf eine Beziehung mit einer Vertrauensperson („Trustee“)

einzulassen und dabei das Risiko von Nachteilen in Kauf zu nehmen, deren Abwendung nicht in der Hand des Vertrauenden, sondern der Vertrauensperson liegt. Den Grund dieser Entscheidung sieht Luhmann in der Reduktion der Komplexität, mit der sich die vertrauende Person andernfalls auseinandersetzen müsste, wenn sie das Risiko selbst steuern oder seine Steuerung jedenfalls prüfen wollte“ (Grimm 2015, S. 138)[101]. Das Zusammenspiel zwischen Trustor und Trustee wird durch ein relationales Vertrauensmodell beschrieben (Mayer et al. 1995), wobei als Vorteil die Vertrauensbeziehung im Zentrum des Modells darstellt (s. Abb. 3.3).

Weil der Trustor den gesamten Kontext nicht vollständig kontrollieren kann, vertraut er dem in diesem Kontext handelnden Trustee, dass dessen Handlungen eine für die Zukunft positive Auswirkung hat.

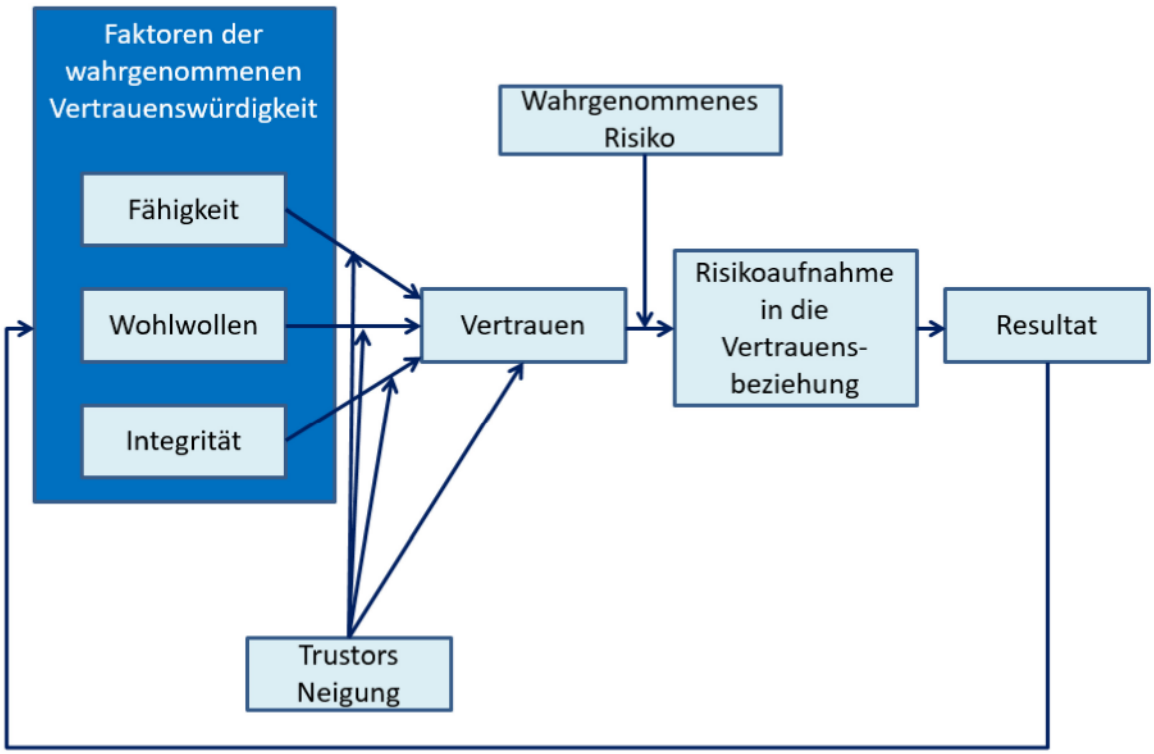


Abb. 3.3: Das Vertrauensmodell nach Mayer, Davis und Schoorman (Mayer et al. 1995, S. 715)

Nach dem Modell von Mayer, Davis und Schoorman, welches die Vertrauensbeziehung zwischen Trustee und Trustor beschreibt, schenkt der Nutzer (also Trustor) den Anbietern (also Trustees) aufgrund deren Kompetenz, deren Wohlwollen und deren Integrität sein Vertrauen. Liegt nun ein zu erwartendes Risiko vor, dann wird dieses in die Vertrauensbeziehung mit aufgenommen, sofern der Nutzer das Risiko nicht durch Maßnahmen des Selbstdatenschutzes

[101] Zum Begriffsverständnis von Vertrauen nach Luhmann siehe:
Luhmann, Niklas (1973): Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. 2. Aufl. Stuttgart: Ferdinand Enke Verlag.
Luhmann, Niklas (2001): Vertrautheit, Zuversicht, Vertrauen. Probleme und Alternativen. In: Hartmann, M.; Offe, C. (Hg.): Vertrauen – Die Grundlage des sozialen Zusammenhalts. Frankfurt: Campus Verlag, S. 143 – 160.

beherrschen kann. Aufgrund der Auswirkung in diese Vertrauensbeziehung wächst oder fällt mit der Zeit das Vertrauen, da die Ergebnisse wiederum die wahrgenommene Vertrauenswürdigkeit des Trustees darstellen. Dies stellt ein rückkoppelndes Element dar und beschreibt damit die dynamische Komponente im Modell.

(Söllner et al. 2012) haben die Eigenschaften, die der Trustor von dem Trustee fordert, auf digitale Artefakte übertragen. Sie kristallisieren die Aspekte *Performanz*[102], *Zweckorientierung*[103] und *Prozessangemessenheit*[104] heraus. Auf diese muss sich der Internetnutzer verlassen können (Grimm 2015).

Die verschiedenen Parteien, denen der Nutzer bei der Internetnutzung gegenübersteht, sind zunächst die Softwarehersteller (von Betriebssystemen, Browsern, ggf. Plug-ins, usw.), in der aktuellen Sitzung der Provider, der ihm den Zugang zum Netz ermöglicht und Verbindungsdaten speichert, und letztendlich die Anbieter von den gewünschten Diensten, die er nutzen möchte. Diese Kooperation ist insgesamt risikobehaftet, denn der Nutzer kann nur bis zu einem gewissen Grad seine Daten kontrollieren. Eine vollständige Kontrolle liegt beispielsweise dann vor, wenn der Nutzer bewusst entscheidet, ob er ausgewählte Daten z. B. im Profil eines Sozialen Netzwerkes oder an einen Anbieter (z. B. beim Online-Einkauf) weitergibt oder nicht. Eine andere Kontrollmöglichkeit ist die Verschlüsselung im Rahmen der Kommunikation, wobei diese Kontrolle an der Stelle endet, an der ein vertrauensbedürftiger Partner diese Daten wieder entschlüsselt. Hierbei ist zu beachten, dass der Nutzer dem Anbieter der Verschlüsselungstechnologie vertrauen muss, dass das Tool seine Funktion mit Wohlwollen und Integrität gegenüber dem Benutzer ausführt. Ganz allgemein zählt man Schutzmechanismen, die vom Nutzer aus bewusst angewendet werden, zum sogenannten Selbstdatenschutz (vgl. Abschnitt 2.1.1).[105]

Gibt der Nutzer jedoch seine Daten preis, dann vertraut er fortan der anderen Seite, dass diese bestimmungsgemäß mit den Daten umgeht. Dies ist in den von den Anbietern formulierten Datenschutzerklärungen geregelt, die wiederum auf der Basis von Datenschutzgesetzen ausgearbeitet worden sind. An dieser Stelle gibt der Nutzer (als Trustor) die Kontrolle an die anderen Parteien (Trustees) ab. Die Ziele, die die unterschiedlichen Gruppen (Provider, Software- und Dienstanbieter) verfolgen, sind jedoch in der Regel unterschiedlich.

Der Nutzer kann den Selbstdatenschutz zusätzlich durch passende Tools (z. B. Adblock Plus[106] oder PassSec+[107]) verbessern. Aber auch in diesem Fall muss er dem Tool, welches er einsetzt und in der Regel nicht selbst programmiert hat, Vertrauen entgegenbringen, dass es seine

[102] „Die Fähigkeit, die Funktion zu erfüllen“ (Grimm 2015, S. 139)
[103] „Die wohlwollende Intention beim Systemdesign“ (Grimm 2015, S. 139)
[104] „Die Integrität der korrekten und angemessenen Ausführung“ (Grimm 2015, S. 139)
[105] Roßnagel argumentiert ausgehend von der informationellen Selbstbestimmung, dass es dem Staat nicht möglich ist, alles zu kontrollieren, sodass jeder Bürger selbst aktiv werden muss. Aber dazu müssen die technischen Möglichkeiten und die rechtlichen Rahmenbedingungen geschaffen werden (Roßnagel 2003, S. 327ff).
[106] Diese Software ist ein Werbefilter und unterdrückt Werbung auf den Webseiten (https://adblockplus.org/de/, zuletzt aufgerufen 22.12.17).
[107] Diese Software warnt vor der Eingabe von Zugangsdaten u. Ä. auf unsicheren Webseiten (https://www.secuso.informatik.tu-darmstadt.de/de/secuso/forschung/ergebnisse/security-extensions/passsec/, zuletzt aufgerufen am 22.12.17).

Funktion mit Wohlwollen und Integrität gegenüber dem Benutzer erfüllt. Hier gilt es ebenfalls abzuwägen, wie viel Vertrauen man den Anderen – in diesem Fall der Infrastruktur, die diese Tools trägt – gegenüber bringt.

Selbstdatenschutzkontrolle und Vertrauen sind eng in der risikobehafteten Situation miteinander verbunden und stehen in Wechselwirkung zueinander. Die geringste Form der Abhängigkeit ist, dass der Nutzer keine Daten angibt (also Datenvermeidung) und damit auch kein Tool nutzt. Die nächst höhere Form ist, dass der Nutzer Selbstdatenschutztools nutzt, wobei hier Vertrauen in die Werkzeuge von Nöten ist. Die stärkste Abhängigkeitsform ist, dass der Nutzer ohne weitere Maßnahmen seine Daten weitergibt und damit dem Empfänger der Daten vertraut. Die beiden letzten Formen finden häufig gemeinsam statt.

In einer risikobehafteten Situation gilt es nun das Risiko abzuschätzen, sodass daraus eine Handlungsstrategie folgt. Wenn der Nutzer in der Kooperation Selbstdatenschutzkontrolle ausüben kann, dann verringert sich das Risiko, wobei er jedoch in die eingesetzten Tools Vertrauen schenken muss. Ist ein Restrisiko vorhanden, dann hat der Nutzer zwei Möglichkeiten: Entweder er verlässt die Situation oder er geht das für ihn akzeptable Restrisiko ein, indem er Vertrauen (sowohl in die Selbstdatenschutztools als auch in den Datenempfänger) schenkt, welches dafür notwendig ist. Diese Entscheidung verlangt in besonderem Maße Kenntnis und Bewusstsein (engl. Awareness) und muss wesentlicher Teil einer Datenschutzkompetenz sein.

Am Max-Planck-Institut für Bildungsforschung, Berlin, wird am Harding-Zentrum über Risikokompetenz geforscht. „Risikokompetenz bezeichnet die Fähigkeit, informiert, kritisch und reflektiert mit Risiken umzugehen … Zu den einzelnen Kompetenzen zählen statistisches Denken, heuristisches Denken, Systemwissen … und psychologisches Wissen“ (Jenny 2017, S. 225). Eine herausragende Rolle spielt nach Meinung des Autors das heuristische Denken, weil es die Fähigkeit im Umgang mit unbekannten Risiken beschreibt. Ein Verständnis für Wahrscheinlichkeiten und Risiken ist bei vielen Menschen nicht gut ausgebildet, sodass sogar die Existenz von Unsicherheiten gerne außer Acht gelassen wird. „Die Allgemeinbevölkerung ist sich ihrer zu geringen Risikokompetenz wenig bewusst“ (Jenny 2017, S. 227), sodass eine Förderung einer Risikokompetenz in der Schule gefordert wird.

Dies ist jedoch nicht ausschließlich eine Aufgabe des Informatikunterrichts, sondern hier hat insbesondere auch der Mathematikunterricht mit kritischen Betrachtungen auf Statistiken und statistischen Verfahren seine Aufgabe. Risiken zu erkennen, ist die eine Seite im Handlungsprozess, jedoch ist die Bewertung die andere, mindestens genauso wichtige Seite. Eine Hilfe dazu bietet das Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse.

3.3. Das Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse

Handlungen, die im Zusammenhang mit der Internetnutzung vollzogen werden, sind – wie schon in Abschnitt 3.2 beschrieben – risikobehaftet, da es dem Nutzer bei einer solchen komplexen Struktur nicht möglich ist, alle Teilprozesse und Teilschritte zu kontrollieren. Bevor der Nutzer jedoch den Trustees Vertrauen schenkt, muss er zuerst einmal das Risiko, ein Produkt aus Schadenshöhe und Eintrittswahrscheinlichkeit, wahrnehmen und anschließend bewerten.

Mit Hilfe des Referenzmodells für ein Vorgehen bei der IT-Sicherheitsanalyse (Grimm et al. 2016) kann eine Bewertung des Risikos vorgenommen werden. Das Modell ist in erster Linie für die Entwickler von Sicherheitssystemen gedacht und kann in abgewandelter Form auch zur Einschätzung eines Nutzungsrisikos genutzt werden. Die Abbildung 3.4 beschreibt das vierschrittige Modell anschaulich.

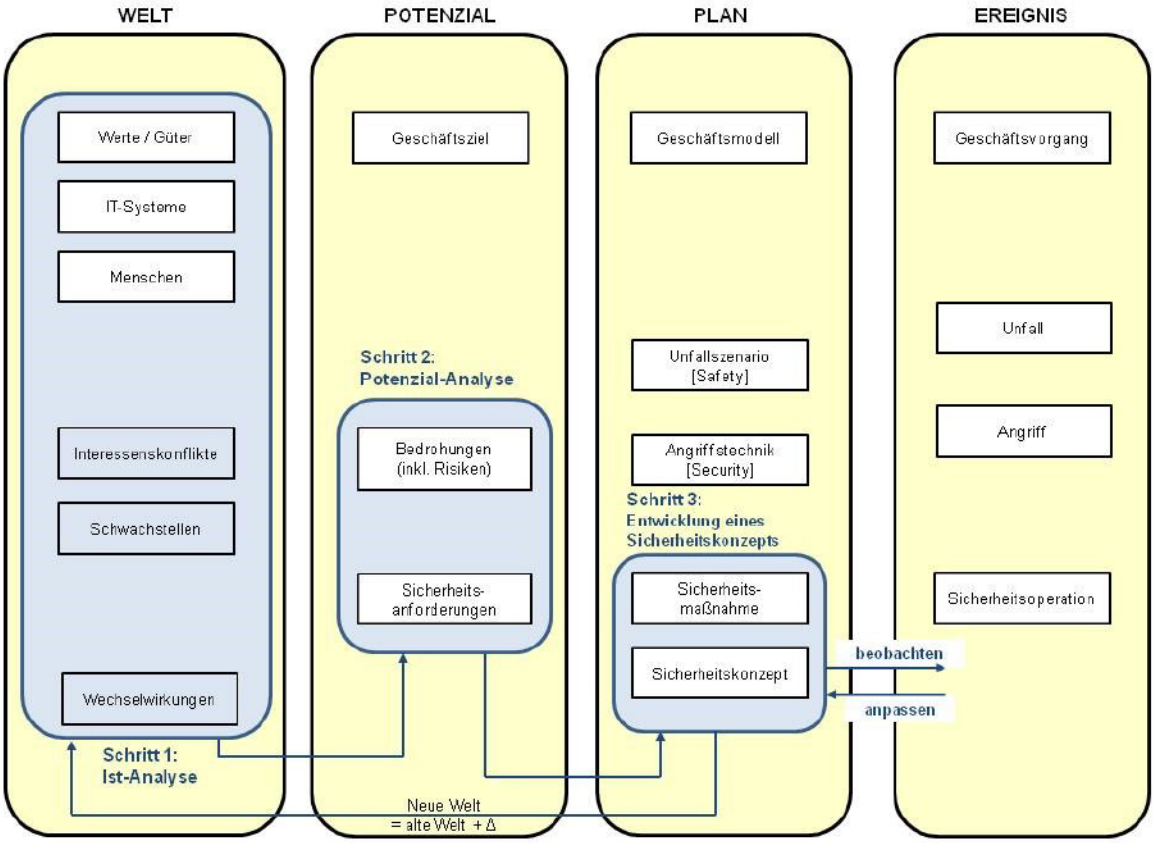


Abb. 3.4: Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse (angelehnt an (Grimm et al. 2016, S. 4))

Im Rahmen des ersten Schritts, der IST-Analyse, ist „eine Bestandsaufnahme der Welt mit der Identifikation der zu schützende Güter, der Schwachstellen des Systems, der beteiligten Akteure, der zugrundeliegenden Interessenkonflikte und der Wechselwirkung der Elemente der Welt untereinander“ zu machen (Grimm et al. 2016, S. 11). In dem hier betrachteten Zusammenhang sind die Güter die persönlichen Daten, als IT-Systeme gelten die Endgeräte der Nutzer, die Router und die Server und als Akteure fungieren der Nutzer, die Administratoren der Netzwerke, über die der Datenverkehr gehen wird, die Dienstanbieter und letztendlich auch die Personen, die unbefugt in den Prozess des Datenaustauschs eingreifen (sogenannten Angreifer). Interessenkonflikte können in dem, was der Nutzer erwartet, und dem, was die Anderen, die an dem Kommunikationsprozess beteiligten, sich erhoffen, entstehen: zum Beispiel möchte der Nutzer in einem Sozialen Netzwerk mit anderen Menschen in Kontakt stehen, jedoch erhofft sich der Betreiber, dass der Nutzer möglichst viele personenbezogene Daten von sich preisgibt, die er dann verwertet, um beispielsweise Werbung seiner Kunden zu schalten.

Schwachstellen im System können durch eine falsche Konfiguration der Hard- und Software, durch Fehler in der Software, aber auch durch Missachtung von Verhaltensregeln entstehen. Diese Schwachstellen entstehen letztendlich aber durch den Menschen.

Der zweite Schritt stellt die Analyse des Potenzials dar. Hier geht es um „die Auflistung aller Bedrohungen mit deren Risiko, [um] eine Zuordnung der Bedrohungen zu den schützenswerten Gütern und ausgenutzten Schwachstellen, sowie [um] die mit den Bedrohungen assoziierten Sicherheitsanforderungen an das IT-System“ (Grimm et al. 2016, S. 12). Angriffe als mögliche Folge von Bedrohungen (z. B. auf das Endgerät des Nutzers und auf den Kommunikationsprozess oder auch in Form eines Man-in-the-Middle-Angriffs) sind z. B. eine Fremdsteuerung des eigenen Geräts, Ausspähen oder Verlust von Daten etwa durch Diebstahl von Kreditkartendaten, das unbefugte Mitlesen von Kommunikation oder eine zweckfremde Nutzung von veröffentlichten Daten in Sozialen Netzwerken. Das Risiko ist immer in Bezug auf die schützenswerten Güter, die bedroht sind, zu bemessen. Im Falle der bedrohten personenbezogenen Daten ist ihr Bedrohungsrisiko von der Datenart abhängig und nicht immer direkt monetär zu beziffern. So ist die Schadenshöhe bei Kreditkartendaten leichter finanziell zu schätzen, als bei der ungewollten Bekanntgabe eines Beziehungsstatus, deren Schaden individuell unterschiedlich einzuschätzen ist. Schwachstellen, die hier ausgenutzt werden können, sind zu leichte Zugänge zu den Servern (z. B. durch schwache Passwörter), unzureichend geschützte Zugänge zu den Daten (offene Netze und ungeschützte Datenspeicher) und das Nutzerverhalten (z. B. die Vermeidung kryptographischer Verfahren oder eine unnötige Preisgabe von Daten). Die Anforderung eines Privatheitschutzes lässt sich so in folgende funktionale Sicherheitsanforderungen zerlegen:

- Vertraulichkeit (d. h. Zugriff nur durch berechtigte Kommunikationspartner),
- Zweckbindung (aus zweckentsprechender Nutzung der Daten),
- Vertrauenswürdigkeit der anderen Parteien und
- eine funktionsintegre Verfügbarkeit der Daten.

Der nächste Schritt ist die Entwicklung eines Sicherheitskonzepts, „in dem sämtlichen identifizierten Bedrohungen durch hinreichend wirksame Sicherheitsmaßnahmen entgegengewirkt wird und … alle spezifizierten Sicherheitsanforderungen durch adäquate Sicherheitsmaßnahmen umgesetzt werden“ (Grimm et al. 2016, S. 12). Typische klassische Sicherheitsmaßnahmen sind die Nutzung von starken Passwörtern, die Verschlüsselung beim Mailen und Chatten und die Beachtung einer verschlüsselten Internetkommunikation, wobei man dies mit dem Vertrauen auf den Anbieter tut. Zur Vermeidung von Schwachstellen sind regelmäßige Updates der Software erforderlich. Speziell für den Datenschutz sind die Datenschutzprinzipien zu beachten (DSGVO Art. 5). Dazu gehört die Datenminimierung, die besagt, dass nur ausgewählte Inhalte mit Bedacht kommuniziert werden. Weiterhin gibt es die Möglichkeit, Selbstdatenschutz zu üben, beispielsweise Sicherheitseinstellungen im Browser vornehmen, Anti-Tracker installieren, überflüssige Daten löschen lassen, alternative Suchmaschinen nutzen

oder das regelmäßige Löschen von Cookies und Browser-Verläufen. Die „Entwicklung des Sicherheitskonzeptes“[108] für den Schutz der Privatheit erfordert eine ausgewiesene Datenschutzkompetenz, nämlich Kenntnis und Erfahrung in Bezug auf den Umgang mit personenbezogenen Daten.

Der letzte Schritt ist die „Installation eines Sicherheitskonzepts“[108]. Dieses dient dem Entwickler als Vorlage seines Entwicklungsprojekts. Dem Internetnutzer dient es insoweit, als er entscheiden kann, welche Sicherheitsmechanismen des Selbstdatenschutzes vorhanden sind, um ein ihm adäquates Sicherheitskonzept zu erfüllen, und in wieweit er ansonsten einem Restrisiko ausgesetzt ist und ob er den Partnern, von denen er dann noch abhängt, vertrauen kann. Hier ist die Handlungsfähigkeit in der Datenschutzkompetenz gefragt.

In abgewandelter Form gibt das Modell einen Weg vor, wie eine Risikobewertungskompetenz beschrieben werden kann. Nachdem ein Risiko erkannt wurde, gilt es dieses zu bewerten, um passende Schutzmechanismen einzusetzen und die Vertrauenswürdigkeit einzuschätzen. Eine Einschätzung kann über die sogenannten *Common Criteria*[109] erfolgen.

3.4. Ableitung eines Datenschutzkompetenzmodells und Definition von Datenschutzkompetenz

Im vorliegenden Abschnitt wird nun aus den voran vorgestellten Modellen ein Datenschutzkompetenzmodell hergeleitet, zu dem folgende Veröffentlichungen existieren: (Hug und Grimm 2016a, 2016b, 2017).

Als Basis für das Datenschutzkompetenzmodell dient das Medienkompetenzmodell von Six/Gimmler (vgl. Abschnitt 3.1), aus dem die Dimensionen Orientierungswissen, Hintergrundwissen, Urteilskompetenz und Auswahl- und Nutzungskompetenz übernommen werden. Diese Dimensionen sind zur Beschreibung einer Datenschutzkompetenz notwendig, da Wissen eine Grundlage bildet, Urteile vor dem Handeln gefällt werden müssen und Auswahl und Nutzung aus einem Angebot an Schutzmaßnahmen zum Schutz der persönlichen Daten notwendig sind. Das Gestaltungswissen und das prozedurale Wissen sind wichtige Elemente einer Medienkompetenz, fördern aber keine Datenschutzkompetenz. Wenn Six/Gimmler im Rahmen des Gestaltungswissens von der technischen Manipulierbarkeit sprechen, dann kann dies auch als ein Hintergrundwissen im Sinne der Datenschutzkompetenz verstanden werden, denn hierbei geht es um das Wissen, dass technische Manipulationen möglich sind, jedoch wird man sie nicht ausführen oder anwenden. Ebenso sind die Rezeptions- und Verarbeitungskompetenz und die Kommunikatorkompetenz Bestandteile der allgemeinen Medienkompetenz und daher keine Spezifika der Datenschutzkompetenz. Aus diesem Grund werden vier der acht Dimensionen des Medienkompetenzmodells für das Datenschutzkompetenzmodell übernommen.

[108] Die Begrifflichkeit folgt aus dem Modell; bei dem Aufruf einer Webseite wird man kein Sicherheitskonzept entwickeln oder installieren.

[109] Die *Common Criteria for Information Technology Security Evaluation* – kurz Common Criteria (CC) – sind ein international gültiger Kriterienkatalog zur Evaluierung und Zertifizierung von IT-Produkten.

Somit kann man in Anlehnung an die Definition von Six/Gimmler unter Orientierungswissen das Wissen über verschiedene Produkte (Produktkategorien), deren funktionelle Einsetzbarkeit, spezifischen Anforderungen, Grenzen und gegebenenfalls spezifische Wirkungspotentiale und über die Beschaffung weiterer situationsbezogener Informationen verstehen. Hintergrundwissen ist demnach das Wissen über die Prinzipien des Datenschutzes und deren Bedeutung und Anwendung sowie über mögliche Schadensursachen bezüglich der Abschätzung eines Risikos und deren Gegenmittel.

Im Laufe der Anfertigung der Arbeit hat sich herausgestellt, dass im Fall der Beschreibung einer Datenschutzkompetenz (im Gegensatz zur Medienkompetenz) eine Unterscheidung zwischen Orientierungswissen und Hintergrundwissen nicht sinnvoll ist.[110] Stellt man sich z. B. die Frage, welche Softwareprodukte aus einer Liste (z. B. *Mozilla Firefox*, *Google Chrome*, *Adobe Acrobat* und *Microsoft Edge*) Browser sind, so verlangt dies ein Orientierungswissen. Aber ohne entsprechendes Hintergrundwissen lässt sich diese Frage nicht beantworten, da eine Risikoabschätzung über den ausgewählten Browser nötig sein kann (z. B. ist dem Nutzer die Performanz von *Google Chrome* wichtiger als die datenschutzrechtlichen Einstellungen von *Mozilla Firefox*). Es macht somit Sinn, im Folgenden nur noch von *Wissen* (W) statt von Orientierungswissen und Hintergrundwissen zu sprechen bzw. die Aspekte von Hintergrundwissen in Orientierungswissen zu integrieren. Wissen ist die Basis für alle weiteren Kompetenzen.[111]

Die *Auswahl- und Nutzungskompetenz* (ANK) beschreibt die Fähigkeit und Fertigkeit zur selbstbestimmten, zielorientierten und reflektierten Auswahl und Nutzung von Angeboten.

Urteilskompetenz (UK) schließlich ist die Fähigkeit und Fertigkeit, eine Entscheidung auf Grundlage des Wissens, der Risikobewertungskompetenz (s. nächster Absatz) und der Auswahl- und Nutzungskompetenz zu treffen.

Als weitere Dimension kommt die *Risikobewertungskompetenz* (RK) ins Spiel, die sich aus dem Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse ergibt. Die Risikobewertungskompetenz beschreibt die Fähigkeit und Fertigkeit, Gefahren (Risiken) zu erkennen und zu bewerten, sowie die Vertrauenswürdigkeit anderer Kommunikationsteilnehmer einzuschätzen.

Eine ähnliche, aber doch andere Situation wie im Fall des Unterschieds zwischen Orientierungswissen und Hintergrundwissen stellt sich im Fall Risikobewertungskompetenz und Urteilskompetenz dar. Auch hier scheint es, dass zwischen beiden Kompetenzen ein sehr enger Zusammenhang besteht. Aber der Unterschied ist, dass im Fall der Risikobewertungskompetenz das Risiko „nur“ erkannt und bewertet wird, während bei der Urteilskompetenz nach Auswahl eines passenden Lösungswegs zur Verringerung (oder gar Vermeidung) des Risikos

[110] Der Prozess der Q-Sortierung im Rahmen der Studie (vgl. Abschnitt 4.2.2) zeigte, dass die Q-Sortierer zwar Wissensitems eindeutig bestimmten, aber die Differenzierung zwischen Orientierungswissen und Hintergrundwissen nicht verständlich war, sodass letztendlich auf diese Unterscheidung im Sinne der besseren Verständlichkeit des Modells verzichtet worden ist.

[111] Trepte et al. unterscheiden in ihrer OPLIS-Studie (Masur et al. 2017; Trepte et al. 2015b) verschiedene Wissensbereiche (aber keine Kompetenzen): institutionelle Praktiken, technische Aspekte des Datenschutzes, Datenschutzrecht und Datenschutzstrategien. Das erscheint aber nach Meinung des Autors zur Beschreibung der Datenschutzkompetenz nicht notwendig. In der Studie zur Entwicklung der Online-Privatheitskompetenz-Skala (OPLIS) ist ausschließlich Wissen, aber keine Kompetenz überprüft worden.

ein Urteil gefällt wird, auf dessen Grundlage letztendlich gehandelt wird. Risikobewertungskompetenz leitet sich zudem aus dem Modell von Grimm ab, während die Urteilskompetenz aus dem Medienkompetenzmodell stammt. Risikobewertungskompetenz und Urteilskompetenz liegen nah beieinander, können aber voneinander abgegrenzt werden.

Die fünfte Dimension wird durch die *Handlungskompetenz* (HK) beschrieben, die eine Anwendung von Handlungen ist, nämlich die Fähigkeit und Fertigkeit im Sinne des Schutzes persönlicher Daten nach persönlichem Urteil zu handeln.

Betrachtet man die einzelnen Dimensionen des Datenschutzkompetenzmodells, so lässt sich folgende Schrittfolge herausarbeiten:

$$W \rightarrow RK \rightarrow ANK \rightarrow UK \rightarrow HK$$

Zu Beginn steht das Wissen als Grundlage, um jemandem eine Datenschutzkompetenz zuzuschreiben. Wenn das vorhandene Risiko erkannt wurde, dann kann es auf Basis des Wissens bewertet werden (RK). Nun wird auf Grundlage dieser beiden Dimensionen unter den Angeboten z. B. ein Tool ausgewählt (ANK). Im nächsten Schritt wird eine Entscheidung getroffen und dabei ein Urteil gefällt (UK), dem dann letztendlich die Handlung folgt (HK).[112]

Der Zusammenhang zwischen den Dimensionen macht deutlich, dass diese nicht orthogonal sind. So fußen z. B. alle Dimensionen auf der Dimension *Wissen*. Dieser Zusammenhang wird sich im Rahmen der Studie zeigen (vgl. Abschnitt 4.3.3.2).

Das Modell kann durch folgende Grafik beschrieben werden:

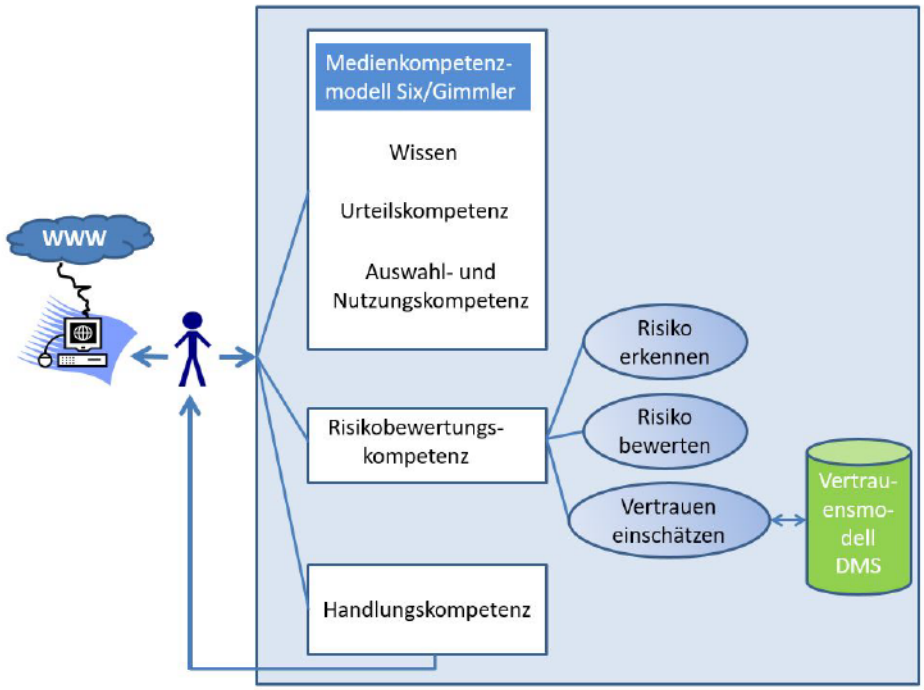


Abb. 3.5: Das abgeleitete Datenschutzkompetenzmodell

[112] Diese Schrittfolge kann als Idealfall aufgefasst werden. Je nach Anwendungskontext kann aufgrund von Wissen sofort gehandelt (z. B. die Ausführung einer Überweisung beim Online-Banking) oder aufgrund einer Risikobewertung direkt geurteilt werden (z. B. verpflichtende Form der Zahlungsmethode beim Online-Einkauf).

Auf Basis dieses Modells kann nun die **Datenschutzkompetenz** als der Zusammenschluss von Wissen, Risikobewertungskompetenz, Auswahl- und Nutzungskompetenz, Urteilskompetenz und Handlungskompetenz (im Sinne der Anwendung von Handlungen) mit Bezug auf das schützenswerte Gut der persönlichen Daten definiert werden. Eine Person gilt als datenschutzkompetent, wenn sie in allen diesen Dimensionen ein (noch zu definierendes) ausreichendes Maß an Kompetenz besitzt.

Die Definition des Maßes und die Formulierung von Datenschutzkompetenzen erfolgt im folgenden Abschnitt.

3.5. Ableitung von Datenschutzkompetenzen aus dem Datenschutzkompetenzmodell

Es gibt keine festgelegten Regeln, wie Kompetenzmodelle zu entwickeln sind. Wie jedoch z. B. aus dem PISA-Kompetenzstufenmodell in Mathematik ersichtlich, „muss ein Kompetenzmodell … mehrdimensional[113] angelegt sein“ (Schulte und Brinda 2005, S. 139). Dabei „beschreiben sie [, die Kompetenzmodelle, erstens] das Gefüge der Anforderungen, deren Bewältigung von Schülerinnen und Schülern erwartet wird (Komponentenmodell); zweitens liefern sie wissenschaftlich begründete Vorstellungen darüber, welche Abstufungen eine Kompetenz annehmen kann bzw. welche Grade oder Niveaustufen sich bei den einzelnen Schülerinnen und Schülern feststellen lassen (Stufenmodell). Klieme u. a. (2003, S. 22) fordern, dass jede Kompetenzstufe durch kognitive Prozesse und Handlungen von bestimmter Qualität spezifiziert [ist], die Schüler auf dieser Stufe bewältigen können, nicht aber Schüler auf niedrigeren Stufen“ (Kohl 2009, S. 37). Das Ergebnis sind dann Kompetenzentwicklungsmodelle.[114]

Mit dem vorangegangenen Abschnitt wurde ein Datenschutzkompetenzmodell entwickelt und auf dessen Basis eine Definition für Datenschutzkompetenz abgeleitet, die insofern noch unvollständig ist, dass kein Maß festgelegt ist. Um diese Frage zu beantworten, greift der Autor auf die Dimensionalität der Kompetenzmodelle, die didaktischer Art sind und nicht mit dem Begriff *Dimension* des Datenschutzkompetenzmodells verwechselt werden dürfen, zurück. (Baumann 2008, S. 54) formuliert:

(1) Eine Inhaltsdimension, die inhaltliche Kompetenzen im Fokus hat;
(2) Eine Handlungsdimension, die allgemeine Kompetenzen umfasst;
(3) Eine Komplexitätsdimension, die durch eine Abstufung den Anspruch beschreibt, wenn nicht ausschließlich von Mindeststandards ausgegangen wird.

Die Inhaltsdimension und die Handlungsdimension werden durch die Dimensionen des Datenschutzkompetenzmodells beschrieben. Die Komplexitätsdimension ermöglicht die Beschreibung durch ein Maß. „Mit den durch Anforderungsbereiche präzisierten Komplexitätsstufen ist – neben Prozess- und Inhaltsbereichen[115] – eine dritte Dimension gewonnen, mit deren

[113] Der Begriff Dimension ist hier nicht mit dem Dimensionsbegriff des Datenschutzkompetenzmodells zu verwechseln.
[114] Siehe dazu auch (Klieme 2004, S. 13).
[115] Gemeint sind hier die Bereiche aus den Bildungsstandards Informatik (vgl. Abschnitt 2.2.1).

Hilfe sich die Frage, ‚bis zu welchem Grad' eine gewisse Kompetenz erreicht sei, beantworten lässt" (Baumann 2008, S. 55).

(Baumann 2008) schlägt in Anlehnung an die Anforderungsbereiche der Bildungsstandards Mathematik[116] drei Stufen für die Komplexitätsdimension vor:

(1) Geringe Komplexität
(2) Mittlere Komplexität
(3) Hohe Komplexität

Wenn davon ausgegangen wird, dass diese Komplexdimension den Anforderungsbereichen der EPA[117] gleichgestellt wird, so wie sich das aus (Baumann 2008) ableiten lässt, dann bedeutet dies, dass eine geringe Komplexität dem Anforderungsbereich *Reproduktion*, eine mittlere Komplexität dem Anforderungsbereich *Reorganisation und Transfer* und eine hohe Komplexität dem Anforderungsbereich *Reflexion und Problemlösen* entspricht. Der Autor sieht darin jedoch das entscheidende Problem, dass Entscheidungen, wie sie dem Bereich der Urteilskompetenz entstammen können, einer mittleren bis hohen Komplexität zuzuordnen sind. Andererseits sollen die Datenschutzkompetenzen aber Basiskompetenzen (vgl. Abschnitt 2.1.5), also Minimalanforderungen von Bildungsstandards entsprechen und untere Stufen des Modells darstellen. Daher wird eine Beschreibung der Datenschutzkompetenzen aus den Bildungsstandards Informatik anzustreben sein.

Bei der Konstruktion von Aufgaben, welches das Thema in (Baumann 2008) ist, wird die Komplexität durch die benutzten Operatoren in den Aufgabenstellungen festgelegt, wodurch diese Aufgaben klassifizierbar werden. Einschränkend aber schreiben die Autoren der Bildungsstandards für die Sekundarstufe II, dass „eine [allgemeine] Zuordnung von Operatoren zu Anforderungsbereichen [bei den Bildungsstandards] … nicht [erfolgt], weil eine eindeutige Zuordnung nicht möglich ist. Die Zuordnung kann erst erfolgen, wenn ein Operator zur Formulierung einer konkreten Aufgabe verwendet wird" (Gesellschaft für Informatik e. V. 2016, S. 14). Daher werden die informatischen Aktivitäten zur Beschreibung der Anforderungsbereiche auch erst in den Prozessbereichen ausdifferenziert (Gesellschaft für Informatik e. V. 2016, S. 3). Diese Meinung teilt der Autor und kann hier nicht über Operatoren der Kompetenzniveaus im Vorfeld definiert werden, da die folgende Studie (vgl. Kapitel 4) eine Online-Befragung mit geschlossenen Fragestellungen werden wird.[118]

Eine Basis für die Ableitung von Mindeststandards der Datenschutzkompetenzen sind die Bildungsstandards Informatik für die Sekundarstufe I (vgl. Abschnitt 2.2.1), denn diese Standards sind ebenfalls als Mindeststandards formuliert, sodass in beiden Fällen die Forderungen nach

[116] Analog auch an die Komplexitätsdimension der 2016 erst erschienen Bildungsstandards Informatik Sekundarstufe II (Gesellschaft für Informatik e. V. 2016).
[117] EPA sind die von der KMK herausgegebenen einheitlichen Prüfungsanforderungen in der Abiturprüfung (vgl. https://www.kmk.org/dokumentation-statistik/beschluesse-und-veroeffentlichungen/bildung-schule/allgemeine-bildung.html#c1284, Stand: 17.03.19).
[118] Gründe für die Gestaltungsform der Studie vgl. Abschnitt 4.1.1.

dem Minimum und dem ausreichenden Maß an Kompetenz ausgedrückt wird.[119] Die Bildungsstandards beschreiben ein „Minimum an Kompetenzen“, die jeder Schüler am Ende der Sekundarstufe I „aufweisen sollte“. „Das Unterschreiten dieser Mindeststandards lässt erhebliche Schwierigkeiten beim Übergang ins Berufsleben und bei ihrer künftigen Position im gesellschaftlichen Leben erwarten“ (Gesellschaft für Informatik e. V. 2008, S. 2).[120] Ebenso verhält es sich mit der Datenschutzkompetenz.

Dem Inhaltsbereich der Bildungsstandards können folgende Kompetenzen entnommen werden, die annähernd zu dem Kontext *Datenschutz* stehen:

Inhaltsbereich	**Kompetenz: Schülerinnen und Schüler …**	**Code**[121]
Sprachen und Automaten	nutzen formale Sprachen zur Interaktion mit Informatiksystemen und zum Problemlösen	SA_1_I
Informatiksysteme	wenden Informatiksysteme zielgerichtet an	IS_1_I
Informatik, Mensch und Gesellschaft	benennen Wechselwirkungen zwischen Informatiksystemen und ihrer gesellschaftlichen Einbettung	IMG_1_I
	nehmen Entscheidungsfreiheiten im Umgang mit Informatiksystemen wahr und handeln in Übereinstimmung mit gesellschaftlichen Normen	IMG_2_I
	reagieren angemessen auf Risiken bei der Nutzung von Informatiksystemen	IMG_3_I

Tab. 3.6: Ausgewählte Kompetenzen der Inhaltsbereiche Bildungsstandards Sek. I (Gesellschaft für Informatik e. V. 2008, S. 16)

[119] Geht man von der allgemeinen Definition für *ausreichend* aus, so versteht man darunter, dass es „eine Leistung [ist], die zwar Mängel aufweist, aber im Ganzen den Anforderungen noch entspricht“ (z. B. ÜSchO §53(2)).
Vgl. dazu http://landesrecht.rlp.de/jportal/portal/t/sbz/page/bsrlpprod.psml?showdoccase=1&doc.id=jlr-SchulORP2009rahmen&doc.part=X (Stand: 17.03.2019)

[120] Weil die Bildungsstandards für die Sekundarstufe I als Mindeststandards formuliert sind, wird in diesen auch die Komplexitätsdimension – im Gegensatz zu den Bildungsstandards für die Sekundarstufe II – nicht thematisiert.

[121] Die Codierung erlaubt später ein leichteres in Bezug setzen zu den Datenschutzkompetenzen.

Zudem können aus den Inhaltsbereichen der Bildungsstandards Sekundarstufe II folgende Kompetenzen aufgelistet werden, die in einem Bezug zum Thema *Datenschutz* stehen:

Inhaltsbereich	**Kompetenz: Schülerinnen und Schüler …**	**Code**
Informatiksysteme	analysieren die Kommunikation und die Datenhaltung in vernetzten Systemen und beurteilen diese auch unter den Gesichtspunkten des Datenschutzes und der Datensicherheit	IS_1_II
Informatik, Mensch und Gesellschaft	beschreiben Chancen, Risiken und Missbrauchsmöglichkeiten von Informatiksystemen	IMG_1_II
	diskutieren und bewerten wesentliche Aspekte des Datenschutz- und Urheberrechts anhand von Anwendungsfällen	IMG_2_II
	verwenden und beschreiben Verfahren zur Sicherung von Vertraulichkeit, Authentizität und Integrität von Daten	IMG_3_II
	ziehen Rückschlüsse für das eigene Verhalten beim Einsatz von Informatiksystemen	IMG_4_II
	analysieren und beurteilen Verfahren zur Sicherung von Vertraulichkeit, Authentizität oder Integrität von Daten in konkreten aktuellen Anwendungskontexten	IMG_5_II
	konzipieren Maßnahmen zur Realisierung von Datensicherheit für konkrete Anwendungsfälle, insbesondere Zugriffskontrolle	IMG_6_II

Tab. 3.7: Ausgewählte Kompetenzen der Inhaltsbereiche Bildungsstandards Sek. II (Gesellschaft für Informatik e. V. 2016, 11f)
kursiv geschrieben = erhöhtes Anforderungsniveau

Auf der Basis dieser aus den Bildungsstandards gewählten Kompetenzbeschreibungen leitet der Autor konkrete Kompetenzen ab, die in der zweiten Spalte der folgenden Tabelle aufgelistet sind. Die dritte Spalte enthält die codierten Bildungsstandards und die vierte Spalte die zugeordneten Dimensionen des Datenschutzkompetenzmodells, wobei hier immer nur die höchststehende Dimension angegeben ist, da diese die anderen darunterliegenden Dimensionen einschließt (vgl. Schrittfolge in Abschnitt 3.4). Ausnahmen bilden die Kompetenzen, bei denen mehrere Operatoren genannt sind.

Code DSK	Schüler …	Code Bildungs-standards	Dimension Da-tenschutzkom-petenzmodell[122]
DSK1	kennen Grundbegriffe im Umgang mit Internetnut-zung	IMG_1_I / IMG_1_II / IS_1_I	W
DSK2	ordnen den Begriff "Datenschutz-Erklärung" im Kon-text der Internetnutzung ein und kennen die daraus abgeleiteten Rechte und Pflichten	IMG_2_I / IMG_1_II / IMG_2_II	W
DSK3	geben ihre Rechte aus der informationellen Selbst-bestimmung an	IMG_2_I / IMG_2_II	W
DSK4	wissen um das Verhalten (insb. nicht-europäischer) Unternehmen, personenbezogene Daten anderwei-tig als für den vorgesehenen Zweck zu verwenden	IMG_1_I / IMG_3_I / IMG_1_II / IMG_2_II	W
DSK5	kennen Maßnahmen, um das Internet-Surfverhalten zum eigenen Schutz anzupassen, und wenden tech-nische und weitere Maßnahmen zur sicheren Inter-netnutzung an	IMG_1_I / IMG_2_I / IMG_3_I / SA_1_I / IMG_4_II / IS_1_II	W + HK
DSK6	bewerten die Sensibilität personenbezogener Daten	IMG_3_I / IMG_1_II / IMG_2_II	RK
DSK7	schätzen den Wirkradius und die Gefahr (selbst-)ver-öffentlichter (persönlicher) Daten ab	IMG_2_I / IMG_3_I / IMG_1_II / IMG_2_II	UK
DSK8	bewerten den Datenschutz im Bereich der Social Me-dia und ziehen Rückschlüsse für das eigene Verhal-ten	IMG_2_I / IMG_3_I / IMG_1_II / IMG_2_II / IMG_4_II / IS_1_II	RK + UK
DSK9	bewerten und beurteilen die Gefahren von ungüns-tigen Internettätigkeiten (wie z. B. Cybermobbing, Spam-Mail und Trickbetrug)	IMG_1_I / IMG_3_I / IMG_1_II	RK + UK
DSK10	beurteilen den Missbrauch von Online-Konten (wie z. B. E-Mail, Banking, Einkauf und Dienstleistungen)	IMG_1_I / IMG_1_II / IMG_2_II / IMG_5_II / IS_1_II	RK

Tab. 3.8a: Gegenüberstellung der Datenschutzkompetenzen den Kompetenzen aus den Bildungsstandards und Zuordnung zu den Dimensionen des Datenschutzkompetenzmodells

[122] Die Abkürzungen in Spalte 4 stehen für die entsprechenden Dimensionen des Datenschutzkompetenzmodells.

Code DSK	Schüler …	Code Bildungs-standards	Dimension Da-tenschutzkom-petenzmodell
DSK11	bewerten das Ausmaß von Kenntnissen persönlicher Informationen durch Dritte und reagieren angemes-sen	IMG_2_I / IMG_3_I / IMG_1_II / IMG_2_II / IMG_4_II	UK + HK
DSK12	bewerten die Gefahren bei der Online-Kommunika-tion (z. B. durch Mailen, Chatten und Surfen) und re-agieren angemessen	IMG_1_I / IMG_2_I / IMG_3_I / IMG_4_II / IS_1_II	RK + HK
DSK13	bewerten und beurteilen die Risiken einer unbe-merkten Infektion durch Schadsoftware	----	RK + UK
DSK14	bewerten die Gefahren durch unüberlegte Handlun-gen (z. B. Anklicken von Links in Mails, Ausführen von Downloads und Anklicken von Werbeanzeigen)	IMG_1_I / IMG_3_I / IMG_1_II / IS_1_II	UK
DSK15	wenden Maßnahmen zum Schutz von Zugängen (zu Systemen, Portalen, …) an	IMG_2_I / IMG_3_I / SA_1_I / IMG_3_II / IMG_4_II / IMG_6_II	HK
DSK16	berücksichtigen Risiken der Internetnutzung und handeln dementsprechend	IMG_1_I / IMG_2_I / IMG_3_I / IMG_1_II / IMG_3_II / IMG_4_II / IS_1_II	HK
DSK17	nutzen kostenlose Alternativen (gegenüber kosten-pflichtigen Produkten) aus dem Internet	IMG_2_I	ANK

Tab. 3.8b: Gegenüberstellung der Datenschutzkompetenzen den Kompetenzen aus den Bildungsstandards und Zuordnung zu den Dimensionen des Datenschutzkompetenzmodells

Die obige Liste von Datenschutzkompetenzen beschreibt ein Mindestmaß an Kompetenzen, die insgesamt betrachtet ein Nutzer besitzen muss, um als datenschutzkompetent bezeichnet zu werden. Sie erhebt keinen Anspruch auf Vollständigkeit und kann jederzeit um weitere Kompetenzbeschreibungen erweitert werden. Die Gegenüberstellung zeigt deutlich, dass die Förderung der Datenschutzkompetenzen auch ein Beitrag zur Förderung der in den Bildungsstandards beschriebenen Kompetenzen ist. Zudem wird hier durch Kompetenzbeschreibungen der Forderung Kliemes nach der über die Jahre systematisch aufzubauenden Fähigkeiten

entsprochen (Klieme 2004, S. 13), da die Kompetenzförderung aller Kompetenzen nicht gleichzeitig erfolgen kann, sondern sich dem Alter und Auffassungsvermögen entsprechend über die Schulzeit verteilen muss.

Der nächste Schritt ist, „dass Kompetenzmodelle empirisch geprüft werden, um Erwartungen präzise und realistisch ansetzen zu können. Keineswegs zwingend wird man dabei in hierarchisch gestuften Kompetenzmodellen enden“ (Klieme 2004, S. 13).

3.6. Erstes Zwischenergebnis

Die erste Forschungsfrage lautet:

> Wie kann man Datenschutzkompetenz konzeptualisieren?

Das in diesem Kapitel hergeleitete Datenschutzkompetenzmodell bietet die Möglichkeit, Datenschutzkompetenz der Untersuchung zugänglich zu machen. Dies geschieht dadurch, dass dem Modell fünf Dimensionen zugrunde gelegt werden:

- (Nutzung von) Wissen,
- Risikobewertungskompetenz,
- Auswahl- und Nutzungskompetenz,
- Urteilskompetenz und
- Handlungskompetenz.

Durch Beherrschung dieser Kompetenzen, die ineinandergreifen und nicht als unabhängig voneinander betrachtet werden können, kann der Nutzer als datenschutzkompetent betrachtet werden, wenn er ein ausreichendes Maß, d. h. Mindeststandards, an Wissen und den oben genannten Kompetenzen besitzt.

Im Folgenden geht es darum, die Datenschutzkompetenz bei Schülern unter Verwendung des Datenschutzkompetenzmodells zu untersuchen. Dazu wird in dem nun folgenden Kapitel eine Untersuchung zum Thema *Datenschutz und Jugendliche* beschrieben, die an allgemeinbildenden Schulen in Rheinland-Pfalz in den Jahrgangsstufen 5 bis 7 durchgeführt worden ist.

„Und was sind eigentlich jene Netzwerke, die sich sozial nennen?
Kinder und Jugendliche vertrauen ihnen Intimstes an. …
Sie kommen gemeinnützig daher, sind aber höchst eigensüchtig."
Hans-Ulrich Jörges (Jörges 2017)

4. Untersuchung der Datenschutzkompetenz bei Jugendlichen

Im folgenden Kapitel wird die Durchführung und Auswertung einer Untersuchung der Datenschutzkompetenz bei Jugendlichen im Alter von zehn bis 13 Jahren an allgemeinbildenden Schulen in Rheinland-Pfalz beschrieben. Dazu wird auf das Datenschutzkompetenzmodell (vgl. Kapitel 3) zurückgegriffen.

Zuerst werden das Konzept, die Methode und das Untersuchungsinstrument vorgestellt, wobei parallel dazu der Zeitplan mit betrachtet wird. Der zweite Teil ist die Auswertung der Erhebung, wobei die Zwischenergebnisse der Q-Sortierung, der Prä-Pilotierung[123] und der Pilotierung immer wieder Einfluss auf das Untersuchungsinstrument hatten.

4.1. Konzeption und Methode der Untersuchung

Zu Beginn steht die Frage, ob zur Erhebung eine qualitative oder quantitative Forschungsmethode genutzt werden soll. Im Rahmen einer ersten Befragung (vgl. Abschnitt 4.1.2, Teilabschnitte (2) und (3)) wurden auch Interviews mit Schülern durchgeführt, um eine qualitative Untersuchung in Betracht zu ziehen. Da der Einsatz von Interviews keine große Teilnehmerzahl erlaubt und sich im Rahmen der Interviewauswertung Probleme abzuzeichnen schienen (vgl. Abschnitt 4.1.2, Teilabschnitt (3) und Abschnitt 4.3.1), bietet sich ein quantitatives Vorgehen an, bei dem im Forschungskontext replizierbare Daten erzeugt werden können. Der Forscher nimmt bei quantitativen Verfahren (im Gegensatz zu qualitativen Verfahren) als Forschungsperspektive eine Außenperspektive ein. Am Ende sind durch quantitative Messungen Erklärungsversuche kausaler Zusammenhänge möglich. (Wolf 1995, S. 316) zitiert dazu Treumann: „Immer dann, wenn es um die Aussagen über Kollektive … geht, sind quantitative Verfahren ein unabdingbares Werkzeug der Datenerhebung und der Datenanalyse". Denn „die zentralen Funktionen quantitativer Forschung … [liegen] in der Identifizierung von Faktoren, die als kausal wirkend angesehen werden können, indem Scheinzusammenhänge zwischen Variablen mittels experimenteller oder statistischer Verfahren kontrolliert werden können" (Wolf 1995, S. 317). Details zu dem Zusammenhang zwischen qualitativer und quantitativer Forschung findet man bei (Scheibler o. J.).

[123] Einer Erhebung geht in der Regel eine Pilotierung im Sinne eines Testlaufs voraus. Im vorliegenden Fall gab es schon eine probenhafte Erhebung vor der Pilotierung. Diese wird im Folgenden *Prä-Pilotierung* genannt.

Die Untersuchung kann durch eine Online-Befragung mit einem standardisierten Fragebogen erfolgen. Dies bietet die Vorteile, dass die Schüler orts-, zeit- und plattformunabhängig teilnehmen können und eine große Reichweite erzeugt werden kann. Ferner ist dieses Verfahren kostengünstig. Nachteile einer Online-Befragung sind das Risiko unkonzentrierter, unseriöser und unsauberer Antworten aufgrund der Anonymität und eine gegebenenfalls nicht ausreichende Kenntnis über die Grundgesamtheit, was aber im vorliegenden Fall aufgrund des ausgewählten Teilnehmerkreises ausgeschlossen werden kann. Abschließend ist zu bedenken, dass bei der Auswahl des Befragungsmediums eine hohe Repräsentanz gewährleistet wird. Im vorliegenden Fall ist dies gesichert, da alle infrage kommenden Schulen in Rheinland-Pfalz zur Teilnahme an der Befragung eingeladen wurden. Die gesammelten und auf einem Server abgespeicherten Daten liegen direkt für die Auswertung digital vor, sodass zudem Übertragungsfehler ausgeschlossen werden können (Homburg und Krohmer 2008).

Neben wenigen personenbezogenen Daten (Alter, Geschlecht, Schulform) werden Wissensfragen, aber auch Fragen z. B. zur Einschätzung von Risiken gestellt. Diese Daten können einerseits deskriptiv genutzt werden, andererseits sollen Korrelationen[124] zwischen den einzelnen Dimensionen (z. B. „Wie hängt die Risikobewertungskompetenz mit der Handlungskompetenz zusammen?“) aufgezeigt werden. Weitere Informationen zum jeweiligen Fragebogen und dessen Struktur folgt in den entsprechenden Abschnitten innerhalb Abschnitt 4.2.

Für die Online-Befragung wurde das Werkzeug *LimeSurvey*[125] genutzt, welches vom Methodenzentrum der Universität Koblenz-Landau angeboten wird. Die Vorteile der Software sind unter anderem die einfache Bedienbarkeit und der leichte Datenexport zu Excel und SPSS. Das Hosting des Systems wird vom Rechenzentrum in Landau gewährleistet.

4.1.1. Forschungsdesign und Erhebungsinstrument

Die Untersuchung fand in Form einer Online-Befragung während der Schulzeit statt, da auf diesem Weg die Schüler am Einfachsten zu erreichen sind. Es wurden alle allgemeinbildenden Schulen der Sekundarstufe I[126] in Rheinland-Pfalz mit der Bitte um Teilnahme angeschrieben, sodass in der Altersgruppe von 10 bis 13 Jahren rund 108 000 Schüler[127] hätten teilnehmen können. In die Erhebung wurden keine weiteren Bundesländer aufgenommen, da gegebenenfalls unterschiedliche Bildungskonzepte, die es zu betrachten gegolten hätte, Einfluss auf die Ergebnisse hätten nehmen können. So sind in Rheinland-Pfalz die Schulen verpflichtet, die

[124] Die Korrelation gibt an, ob und wie stark zwei Merkmale zusammenhängen (Kuß et al. 2018, S. 238).
[125] Siehe https://www.limesurvey.org/de/ (zuletzt geprüft am 20.03.2018)
[126] Dies sind die Schulformen *Realschule Plus*, *Gymnasium* und *Integrierte Gesamtschule*. Strenggenommen gehören dazu auch noch die Schulformen *Förderschule* und *Waldorfschule*, die jedoch unter anderem wegen ihrer differenzierten Förderkonzepte außen vor gelassen worden sind.
[127] Diese Zahl ist hochgerechnet aufgrund der öffentlich zugänglichen Schülerdaten des Statistischen Landesamtes Rheinland-Pfalz (vgl. https://www.statistik.rlp.de/de/gesellschaft-staat/bildung/; Stand: 07.11.2018).

Richtlinien der Verbraucherbildung fächerübergreifend umzusetzen, in denen das Thema *Datenschutz* eine eigene Einheit darstellt (vgl. Abschnitt 2.2.2.3).[128]

Ganz bewusst wurde für die Untersuchung eine Altersgruppe gewählt, bei der die Smartphone-Nutzung – und damit gleichzeitig die Nutzung Sozialer Netzwerke[129], anderer Plattformen und weiterer Angebote des Internets (insbesondere des World Wide Webs) – deutlich zunimmt (vgl. Abschnitt 2.3.2). Somit lautet eine Leitfrage der Erhebung: Wie gut sind die Kinder und Jugendlichen auf die digitale Welt vorbereitet?

Bei der Entwicklung eines standardisierten Fragebogens muss man sich bewusst sein, dass die Wirksamkeit des Instruments bei einer standardisierten Befragung abhängig von der Interpretation der Befragungsteilnehmer ist (Homburg und Krohmer 2008, S. 42). Daher sollten die Fragen eindeutig, klar verständlich und im vorliegenden Fall in der Sprache auch altersgerecht sein. Ein weiterer Aspekt ist, dass eine Umfrage ein sogenanntes reaktives Erhebungsverfahren ist, weil die Befragten – und hier insbesondere die Schüler – sich in einer Test- und Überprüfungsfunktion fühlen und dies mögliche Reaktionen beeinflussen kann (Wübbenhorst 2018)[130]. Obwohl im Einleitungstext der Online-Umfrage und den zuvor ausgegebenen Begleitunterlagen den Schülern garantiert wird, dass die anonymen Befragungsergebnisse vertraulich behandelt und nicht an Lehrkräfte und Eltern weitergegeben werden, kann wegen der Unbekanntheit des Autors gegenüber den Teilnehmern auf ein Vertrauen im Umgang mit den Daten von den Schülern nur gehofft werden. Wer dies nicht glaubt, wird gegebenenfalls auch nicht alle Fragen korrekt und ehrlich beantworten. Ferner ist bei der Entwicklung des Instruments zu bedenken, dass die Länge des Fragebogens dem Alter und der zur Verfügung stehenden Zeit (max. eine Unterrichtsstunde) entsprechend ausgerichtet ist, um Demotivation und geringe Antwortquote zu vermeiden. Gemäß Literatur (Homburg und Krohmer 2008, S. 44) gelten 25 Fragen als Richtwert. Bei der finalen Struktur waren es insgesamt 22 Fragen, bei der Erhebung im Sommer 2016 und der Prä-Pilotierung im Sommer 2017 waren es deutlich mehr, jedoch standen hier auch andere Ziele (wie z. B. Verständlichkeit der Fragen) im Fokus.

Zur Entwicklung eines Fragebogens gibt es zwei Wege. Entweder man formuliert eigene Fragen und Fragestellungen, die vor der endgültigen Nutzung mehrere Iterationsschritte mit ei-

[128] Um den Einfluss der Verbraucherbildung zu messen, hätte man zwei Gruppen von Schüler aufstellen müssen: Eine Gruppe, bei der Verbraucherbildung unterrichtet wurde bzw. wird, und eine Gruppe, für die dies nicht zutrifft. Da die Verbraucherbildung über den gesamten Zeitraum der allgemeinbildenden schulischen Ausbildung (also beginnend mit der Grundschule) unterrichtet und in den Schulen die Umsetzung unterschiedlich gehandhabt wird, ist es nicht möglich, dies differenziert zu messen, da es zu viele, unüberschaubare Einflussgrößen gibt. Auch wenn die Forschungsfrage sehr interessant ist, wird sie im Rahmen dieser Studie nicht untersucht.

[129] Zur Bedeutung und Verwendung des Begriffs *Soziale Netzwerke* im Rahmen der Arbeit siehe Anhang A4.17.

[130] „reaktive Messverfahren: Begriff der Marktforschung für alle Instrumente, die eine Einbeziehung und Motivation der Testperson voraussetzen. Die Reaktion der zu testenden Person auf bestimmte Stimuli kann durch das Wissen, dass sie getestet wird, verändert werden (systematischer Fehler). Die Befragung ist stets [ein] reaktives Messverfahren. Die Beobachtung kann sowohl reaktiv (Laborforschung) als auch nicht reaktiv (Feldforschung) sein." (Wübbenhorst 2018)

ner sehr hohen Teilnehmerzahl an zu Fragenden durchlaufen und durch ein Fachgremium (Experten) gebilligt werden, oder man greift auf Items früherer Studien zurück, da diese als abgesichert angenommen werden können. Wegen des großen Aufwands und der Frage nach der großen Anzahl der Teilnehmer wurde die erste Option verworfen. Über den gesamten Prozess der Untersuchung wurde auf ausgewählte Items folgender Studien zurückgegriffen:

(1) BITKOM (2014): Jung und vernetzt. Kinder und Jugendliche in der digitalen Welt. (BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2014)
(2) DIVSI (2015): U9-Studie. Kinder in der digitalen Welt. (Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) 2015)
(3) DIVSI (2018): U25-Studie. Kinder, Jugendliche und junge Erwachsene in der digitalen Welt. (Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) 2018)
(4) Medienpädagogischer Forschungsverbund Südwest (2015): JIM-Studie 2015. Jugend, Information, (Multi-)Media. (Feierabend et al. 2015)
(5) Masur, P.; Teutsch, D.; Trepte, S.: Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). (Masur et al. 2017)
(6) Schenk, M.; Niemann, J.; Reinmann, G.; Roßnagel, A. (2012): Digitale Privatsphäre. Heranwachsende und Datenschutz auf sozialen Netzwerkplattformen. (Schenk et al. 2012a)
(7) Hoofnagle, C. J.; King, J.; Li, S.; Turow, J.: How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? (Hoofnagle et al. 2010)
(8) Kehr, F.; Rothmund, T.; Gollwitzer, M.; Füllgraf, W.: Prädiktoren sicherheitsrelevanten Verhaltens bei jugendlichen Computernutzern. Computersicherheit und Medienkompetenz. (Kehr et al. und Kehr et al. 2015)[131]

Im Anhang A4.1 ist ersichtlich, welche Items aus welcher Studie entnommen worden sind. Alle Items sind geschlossene Fragen, deren Antworten entweder über eine 5-Likert-Skala[132] (z. B. Einschätzungsfragen) oder Multiple-Choice (z. B. Wissensfragen) gesammelt werden; weitere Fragen stellten eine Mehrfachauswahl von vorgegebenen Wahlmöglichkeiten dar (z. B. Nutzung welcher Sozialen Netzwerke). Dies hat den Vorteil, dass die Antworten leicht analysiert und ausgewertet und Ergebnisse einfacher als bei offenen Fragen miteinander verglichen werden können (Kuß et al. 2018, S. 94; Homburg und Krohmer 2008, S. 27). Ferner sind geschlossene Fragen einfacher zu beantworten, was auf eine höhere Antwortquote hoffen lässt. Im Gegenzug ist nachteilig, dass die Fragen möglicherweise Anhaltspunkte liefern können, welche Antworten präferiert werden. Zudem ist durch ein einfaches „Durchklicken“ im Online-Fragebogen ein oberflächliches Antwortverhalten möglich (Kuß et al. 2018, S. 94).

[131] Der Fragebogen wurde beim erstgenannten Autor erfragt und ist nicht veröffentlicht.
[132] Die Likert-Skala (benannt nach dem US-amerikanischen Sozialforscher Rensis Likert (1903 – 1981)) ist eine eindimensionale Rating-Skala zur Einstellungsmessung, die von einer stark negativen zu einer stark positiven Einstellung gerichtet ist (Greving 2009, S. 73).

Im folgenden Abschnitt wird zuerst der Zeitplan der Studie dargestellt, dem sich dann Bemerkungen zur Datenanalysemethode anschließen, bevor die Beschreibung der Durchführung beginnt.

4.1.2. Zeitplan der Studiendurchführung

Der gesamte Zeitraum von der Entwicklung des ersten Fragebogens bis hin zur Auswertung der finalen Erhebung erstreckt sich vom Mai 2016 bis zum März 2019. Die folgende Tabelle gibt einen ersten groben Überblick, wobei weitere zugehörige Erläuterungen im Anschluss folgen; zur leichteren Orientierung ist den Schritten eine Nummerierung vorangestellt.

Nr.	Zeitraum	Tätigkeit
(1)	Mai bis Juni 2016	Entwicklung eines ersten Fragebogens
(2)	Juli 2016	Erste Befragung einer Schülergruppe
(3)	Herbst 2016	Deskriptive Auswertung der ersten Befragung
(4)	Herbst 2016 – Frühjahr 2017	umfangreiche Recherche nach deutschsprachigen Studien zu Datenschutz u. ä. Themen mit dem Ziel der Item-Gewinnung
(5)	April 2017	Implementierung von Items in *LimeSurvey*
(6)	Mai 2017	Endgültige Auswahl und Adaption der infrage kommenden Items
(7)	Juni 2017	Prä-Pilotierung unter Verwendung von *LimeSurvey* inklusive Dokumentation durch die Schüler
(8)	August 2017	Auswertung von (7) Studie *Digitale Privatsphäre*, die weitere passende Items liefern konnte, aufgefunden
(9)	September/Oktober 2017	Gegenüberstellung ausgewählter Items den Dimensionen des Datenschutzkompetenzmodells Q-Sortierung vorbereitet, durchgeführt und ausgewertet
(10)	Oktober 2017	Implementierung des endgültigen Fragebogens für die Pilotierung Adaption altersgerechter Sprache Antrag bei der Schulbehörde zur Durchführung der Studie
(11)	November 2017	Pilotierung, Auswertung und Überarbeitung des Fragebogens
(12)	Dezember 2017 – Januar 2018	Durchführung der Umfrage
(13)	Februar 2018 – März 2019	Auswertung der Umfrage

Tab. 4.1: Übersicht des Zeitplans der Studiendurchführung

Erläuterungen zu den einzelnen Einträgen in der Tabelle:

(2) Im Sommer 2016 hat der Autor eine Gruppe 13 Jugendlicher im Alter von zwölf bis 19 Jahre nach München begleitet.[133] Im Vorfeld entstand die Idee, diese Teilnehmer als Probanden für eine Erhebung zu nutzen, um einen ersten Eindruck zur Datenschutzkompetenz zu gewinnen. Die Befragung bestand aus zwei Teilen: (a) Alle Schüler beantworteten in Einzelarbeit einen Papier-Fragebogen (s. Anhang A4.12) und (b) danach fanden im Laufe der gesamten Woche vom Autor geleitete Interviews statt, wobei die Gruppen altersspezifisch zusammengestellt worden sind und die Fragen dementsprechend unterschiedlichen waren (s. Anhang A4.14). Die Items hierfür entstammten den in Abschnitt 4.1.1 aufgezählten Studien (1) bis (5) und (7).

(3) Der erste Teil (Fragebogen) wurde deskriptiv ausgewertet, dessen Ergebnis im Anhang A4.13 hinterlegt ist. Als problematischer erwies sich die Transkription und Auswertung der Interviews. Aufgrund der Heterogenität und Qualität der Antworten zeigte sich, dass eine qualitative Untersuchung keine passende Methode zur Messung der Datenschutzkompetenz ist. Zudem erlauben Interviews keine große Teilnehmerzahl an einer Untersuchung, sodass der Schluss auf eine größere Gesamtheit schwierig ist. Die Ergebnisse insgesamt dienten aber durchaus als Impulse der Weiterentwicklung der Studie, die in den folgenden Schritten Berücksichtigung fanden. Weitere Erläuterungen sind in Abschnitt 4.3.1 zu finden.

(4) In diesem Zeitraum setzte sich der Autor vermehrt mit der Frage nach Forschungsmethoden auseinander und wurde in der Entscheidung, nur quantitative Methoden zur Messung der Datenschutzkompetenz in Betracht zu ziehen, bestärkt. Um passende Items für die Erhebung abzuleiten, fand eine ausführliche Recherche vor allem deutschsprachiger Literatur statt.[134] Eine Konzentration auf diesen Raum hatte ferner den Sinn, dass in anderen Ländern, z. B. den USA, ein anderes Datenschutzverständnis existiert und damit auch andere Gesetze gelten, die gegebenenfalls eine Übertragbarkeit von Items nicht ganz einfach erschienen ließ.

Im Rahmen der Recherche konnte der Autor feststellen, dass es zu diesem Zeitpunkt keine Studie gab, die ausschließlich eine Datenschutzkompetenz untersuchte. Somit kann die vorliegende Befragung als ein „Novum“ angesehen werden.

(5) Wegen der Entscheidung für eine quantitative Forschungsmethode wurde aufgrund der Empfehlung des Methodenzentrums der Universität Koblenz-Landau die Software *LimeSurvey*[135] ausgewählt. Die Universität besitzt eine Software-Lizenz für das Produkt, welches vom Rechenzentrum Landau gehostet wird. Alle Datensätze wurden auf Servern in

[133] Die Jugendlichen waren Preisträger eines Reisestipendiums an das Deutsche Museum in München, welches der Landesverband Rheinland-Pfalz des MNU e. V. (vgl. http://www.mnu.de/landesverbaende/landesverband-rheinland-pfalz) jährlich für herausragende Arbeiten im Rahmen des Wettbewerbs *Jugend forscht/Schüler experimentieren* vergibt.

[134] Passende internationale Studien konnten vom Autor nicht ausfindig gemacht werden.

[135] Siehe https://www.limesurvey.org/de/ (zuletzt geprüft am 20.03.2018)

Landau gespeichert, sodass hier auch mit einer dem Datenschutzgesetz konformen Regelung zu rechnen war. Die Bedienung soll sowohl für die Teilnehmer an der Studie als auch die Nutzer des Produkts relativ einfach sein. Gerade der erste Grund war ein entscheidendes Kriterium für die Wahl dieser Software. Die Testläufe bestätigten dies.

(6) Im darauffolgenden Zeitraum fand eine Sichtung und Auswahl aller infrage kommenden Items aus den nutzbaren Studien statt, die gegebenenfalls noch entsprechend zu adaptieren waren. Diese wurden alle in *LimeSurvey* erfasst, sodass daraus der erste Fragebogen für die Prä-Pilotierung, der im Anhang A4.15 in gedruckter Form vorliegt, entstand.

(7) Diese Prä-Pilotierung, bei der wieder 13 Schüler im Rahmen eines Kurses am Deutschen Museum München zur Verfügung standen, verfolgte mehrere Ziele. Zum einen ging es darum, unter den vorgelegten Fragen (rund 80 Stück) die Geeignetsten herauszufinden, denn der Fragebogen als Ganzes war viel zu lang und zu umfangreich. Zudem hatten die Schüler die Möglichkeit, anhand eines mitgereichten Analysebogens (vgl. Anhang A4.16) Rückmeldungen zum gesamten Prozess, aber auch zu einzelnen Items zu geben (z. B. unklare Fragestellungen).[136] Zum anderen stand die Testung und Usability von *LimeSurvey* im Fokus. Es sollte festgestellt werden, ob die Software den geforderten Ansprüchen genügt. Weitere Erläuterungen finden sich in Abschnitt 4.2.1.

(8) Die Auswertung war insgesamt sehr umfangreich, da die Anzahl der Fragen extrem groß gewesen ist. Wichtige Kritikpunkte der Schüler, die teilweise mehrfach genannt worden sind, sind in Abschnitt 4.2.1 festgehalten. Diese Anregungen und Anmerkungen flossen in den Fragebogen für die spätere Pilotierung mit ein.

Die Studie *Digitale Privatsphäre* (Schenk et al. 2012a) bot noch einen weiteren Fundus an Items, die zur Q-Sortierung (siehe Punkt (9)) und Pilotierung herangezogen worden sind.

(9) Für die finale Auswahl der Items wurde neben der Rückmeldung durch die Schüler (siehe Punkt (8)) auch bedacht, dass die Items eine breite und möglichst gleichmäßige Verteilung der Dimensionen aus dem Datenschutzkompetenzmodell abdecken sollten. Da die Zuordnung der Items zu den Dimensionen des Modells durch den Autor jedoch subjektiv wäre, wurde daher das Verfahren einer Q-Sortierung eingeleitet (Funder et al. 2000). Ziel des Prozesses war, dass eine größere Anzahl an Personen die vorgelegten Items auf ihre Messungsspezifikation beurteilten (vgl. Abschnitt 4.2.2). Die daraus gezogenen Ergebnisse führten zum Pilotierungsfragebogen.

(10) Der Fragebogen für die Pilotierung wurde in *LimeSurvey* implementiert und dabei die Fragen entsprechend dem Alter der Probanden adaptiert. Als Rückversicherung wurde dieser Fragebogen einer erfahrenen Grundschullehrkraft vorgelegt, damit das Sprachniveau dem Alter von zehn bis 13 Jahren passend ist.[137]

[136] Jede Frage besaß einen Code, durch den jeder Kommentar einer Frage eindeutig zugeordnet werden konnte.
[137] Eine Grundschullehrkraft kennt das Sprachniveau und die Sprachkompetenz von Schülern, die die Grundschule verlassen und eine weiterführende Schule besuchen. Daher schien es passend, hier die entsprechende Fachexpertise abzugreifen.

Gleichzeitig wurde bei der Aufsichts- und Dienstleistungsdirektion Trier (ADD) die Umfrage zur Anzeige gebracht. Ohne Einschränkungen oder Auflagen seitens der Behörde konnte wie geplant die Pilotierung und spätere Erhebung durchgeführt werden.

(11) Die Pilotierung – ausführlich beschrieben in Abschnitt 4.2.3 – fand am Goethe-Gymnasium, Germersheim, statt. Je eine Klasse der Klassenstufen 5, 6 und 7 haben an der Befragung, die über einen Zeitraum von zwei Wochen lief, teilgenommen. Die Rückmeldung der Schule aus der Erhebung wurde genutzt, um den Fragebogen für den finalen Durchlauf zu überarbeiten. Die Ergebnisse der Schüler wurden nicht weiter betrachtet, da der überarbeitete Fragebogen sich in einigen Punkten deutlich von dem der Pilotierung unterschied. Die Änderung betraf insbesondere die Vereinheitlichung der Likert-Skala, also messtechnische, weniger inhaltliche Aspekte des Fragebogens. (vgl. Anhang A4.7)

(12) Nach der Rückmeldung durch die ADD wurden die Schulleitungen aller allgemeinbildenden Schulen der Sekundarstufe I in Rheinland-Pfalz per E-Mail mit der Bitte um Teilnahme angeschrieben. Die gesamten Unterlagen befinden sich im Anhang A4.6. Die Teilnahmeerklärung von 16 Schulen sind an den Autor zurückgesandt worden. Aufgrund persönlicher Gespräche mit Kolleginnen und Kollegen ausgewählter Schulen, die keine Teilnahmeerklärung abgegeben haben, muss der Autor schließen, dass es eine noch größere Anzahl an teilnehmenden Schulen gab. Während des Erhebungszeitraums führte der Autor ferner Telefonate mit Lehrkräften, die von inhaltlichen Problemen bei der Erhebung sprachen. Ausführliche Erläuterungen sind in Abschnitt 4.2.4 festgehalten.

(13) Am Ende des Erhebungszeitraums haben 1077 Schüler teilgenommen, jedoch lagen nur 1013 vollständige Datensätze vor. Nach Durchsicht konnten 17 weitere Datensätze identifiziert werden, bei denen die Fragen offensichtlich nicht mit dem nötigen Ernst beantwortet worden sind, sodass diese Datensätze ebenfalls eliminiert worden sind. Die verbliebenen Datensätze wurden dann einerseits deskriptiv und andererseits korrelativ ausgewertet, um Zusammenhänge zwischen den einzelnen Dimensionen des Datenschutzkompetenzmodells aufzudecken. Die Ergebnisse sind in Abschnitt 4.3.3 dokumentiert.

4.1.3. Methoden der Datenanalyse

In einem ersten Schritt werden die Daten einer deskriptiven Beschreibung unterworfen (vgl. Abschnitt 4.3.3.1). Mit einem Teil der Daten soll in einem zweiten Schritt erforscht werden, ob es korrelative Zusammenhänge zwischen den Dimensionen des Datenschutzkompetenzmodells gibt. Dazu wird versucht, paarweise zwischen allen Dimensionen Regressionsgeraden zu ermitteln. Damit kann gezeigt werden, ob sich die Dimensionen des Datenschutzkompetenzmodells in irgendeiner Form bedingen oder beeinflussen (vgl. Abschnitt 4.3.3.2). Abschließend findet noch eine differenzierte deskriptive Auswertung ausgewählter Items statt, um gegebenenfalls vorhandene Muster in Geschlecht und Altersgruppen aufzudecken (vgl. Abschnitt 4.3.3.3).

4.2. Studiendurchführung

Im folgenden Abschnitt werden chronologisch gegliedert die Erstellung der Fragebögen und die Rückmeldungen zu diesen Bögen, die bis auf den finalen Fall zur Überarbeitung dieser führten, beschrieben. Zudem werden der Prozess und die Auswertung der Q-Sortierung erläutert. Die Anzeige der Studie bei der Schulbehörde und die Bewerbung der Teilnahme an der Studie sind in Abschnitt 4.2.4 geschildert. Die Vorstellung der Ergebnisse der Datenanalyse erfolgt dann in Abschnitt 4.3.

4.2.1. Prä-Pilotierung (Sommer 2017)

Die Ziele der Prä-Pilotierung waren der Gewinn eines ersten Eindrucks von und die Einarbeitung in *LimeSurvey*, die theoretische Betrachtung der Auswertungsmöglichkeiten und der Erhalt von Schülerrückmeldungen. Ferner galt es aus der großen Anzahl von 78 Fragen Passende herauszufiltern.

Nach der Frage, mit welchem Gerätetyp der Fragebogen bearbeitet worden ist, gaben fünf Teilnehmer das Smartphone und acht Personen den PC/Laptop an. Mit einem Tablet nahm keiner an der Prä-Pilotierung teil.

Der Fragebogen gliedert sich in vier Teile.

Teil A ist die Gruppe der persönlichen Fragen und beinhaltet neben den Angaben wie Alter und Geschlecht auch Fragen zur Internet- und Computernutzung, zur Behandlung von Verbraucherbildung im Schulunterricht und zur Teilnahme am Informatikunterricht oder an einer AG Informatik.

Mit *Internet* ist der Teil B des Fragebogens überschrieben. Hier stehen Fragen zur Internetnutzung (Zeitumfang, der Art und Weise, den Motiven), der Nutzung von Messengern, Sozialen Netzwerken[138], Browsern, Browsertools und Apps im Zentrum. Ferner wurden die Schüler nach ihren häufig besuchten Internetseiten, Maßnahmen und Strategien zur sicheren Internetnutzung, zur Veröffentlichung persönlicher Daten im Netz, dem Teilen von Informationen im Netz und zu Rechten und Pflichten in Bezug auf Datenschutz befragt. Ferner beinhaltet dieser Fragenkomplex Wissensfragen. Einschätzungen zur persönlichen Internetkompetenz, zu Risiken im Internet und zu Datensicherheit in Communities und in Messengern runden den Abschnitt ab.

Im Teil C sind alle Fragen zusammengefasst, die aus der OPLIS-Studie (Masur et al. 2017) entnommen worden sind. Hierbei handelt es sich um Wissensfragen zu Fachbegriffen, zur Einschätzung von Aussagen in Bezug auf Datenschutz und zu Selbsteinschätzungen.

[138] Zu der Frage des Begriffsverständnisses *Soziale Netzwerke* (Frage B8) siehe Anhang A4.17.

Der letzte Block D ist mit *Computersicherheit und Medienkompetenz* überschrieben und orientiert sich mit den Fragen an der Studie *Computersicherheit, Medienkompetenz und Persönlichkeit* (Kehr et al.). Beginnend mit Fragen zu installierten Programmen auf Computer und Smartphone und aktivierten Sicherheitseinstellungen an den Geräten geht es über zum eigenen Nutzungsverhalten, zu Risiko-Einschätzungen im Umgang mit Computer und Internet und der Rolle der Eltern bei der Computer- und Internetnutzung. Auch in diesem Block sind Wissensfragen (zu Fachbegriffen, zur Passwortverwendung, zu Gefahren diverser Dateitypen, über die Kennzeichen einer verschlüsselten Internetverbindung und Gefahren, die von Viren ausgehen) integriert. Abschließend werden Fragen zu eigenen Erlebnissen (oder von Bekannten der Befragten) bezüglich Vorfällen bei der Internetnutzung, zum eigenen Umgang mit Datenschutz (und dem der Eltern) und zum Verständnis von Vertrauen gestellt.

Die Gliederung des Fragebogens orientierte sich weder an einem Schwierigkeitsgrad noch an inhaltlichen Schwerpunkten innerhalb der Frageblöcke, sondern ausschließlich die genutzten Studien waren eine Orientierung, was dem Autor bei der Gliederung eine Hilfe war.

Die Ergebnisse der Befragung sind in Abschnitt 4.3.2 nachzulesen.

Durch die ausgefüllten Rückmeldebögen der Schüler (vgl. Anhang A4.16) konnten folgende Punkte festgestellt werden, die dann in die späteren Fragebögen eingeflossen sind:

- Wie (Homburg und Krohmer 2008, S. 44) beschreiben, hat die Fragebogenlänge Einfluss auf die Antwortquote, da zu lange Fragebögen zu einer geringeren Quote führen. Zwei Faktoren sind für die Länge entscheidend: (1) das Themeninvolvement der Studienteilnehmer (je höher das Involvement, desto länger kann der Fragenkatalog sein) und (2) der gewählte Weg, wobei für einen Online-Fragebogen nicht mehr als 25 Fragen vorgeschlagen werden. Dieser Aspekt war dem Autor von vorneherein bewusst und er hoffte im Fall dieser Prä-Pilotierung auf das „Durchhaltevermögen" der Schüler, um einen ersten Eindruck von Schülern im Umgang mit den Items zu gewinnen.
- Die Eindeutigkeit der Fragestellung, d. h. der Befragte erfasst, welche Information gefordert wird, ist nach (Homburg und Krohmer 2008, S. 27) wichtig, da die Schüler keine Rückfragen stellen können. Die Prinzipien der Einfachheit, der Neutralität und der Eindeutigkeit sind zu beachten.[139] Einige Fragen sind jedoch unklar (z. B. B3, B12, C6, B11) oder unzureichend (z. B. D14) gestellt. In anderen Fällen wiederum (z. B. B2, B3) gab es keine ausreichende Anzahl an Auswahlmöglichkeiten. Unter der Annahme, dass solche Fragen bei der finalen Umfrage verwendet werden, müssen die Fragestellungen angepasst werden. In einer Antwortmöglichkeit wie *ja/unsicher/nein* ist der Gebrauch des Worts *unsicher* nicht klar (z. B. B26); ferner fehle bei einigen Fragen (z. B. C8, D7) die Antwortmöglichkeit *weiß nicht*.
- Gerade jüngere Schüler haben keine Ahnung von online-Banking (B13), Dateiendungen (D12) oder Browsertools (B8); auch die Wissensfragen C6 bis C10 seien zu schwer.

[139] Einfachheit meint beispielsweise die Verwendung einfacher Sätze und keiner unbekannten Fachausdrücke; dass die Frage keinen Rückschluss auf das Antwortverhalten zulässt, beschreibt die Neutralität (vgl. Homburg und Krohmer 2008, S. 45).

- Manche Fragen führen je nach Betriebssystem, mit dem man arbeitet, zu anderen Antworten. Solche Fragen galt es im Folgenden zu eliminieren.
- Auf doppelte Fragen wurde hingewiesen (z. B. C6 und C10).
- Fragen zu Sozialen Netzwerken sollten ausgeblendet werden, wenn der Befragte angibt, dass er solche nicht nutzt.

Erste Kürzungen des Fragebogens für die Weiterarbeit entstanden durch Wegfall von Fragen wie beispielsweise zu installierten Programmen (D2), zur Gerätenutzung und Nutzungsdauer (A4 – A11), zur Verbraucherbildung im Unterricht (A14 – A17), zur Internetnutzung (B4ff), zu Internetkompetenzen (B12) und Fragen, die im Zusammenhang mit den Eltern stehen (z. B. D5, D18). Der gekürzte Fragebogen ist die Grundlage für das Verfahren der Q-Sortierung.

4.2.2. Prozess der Q-Sortierung

Die für die Erhebung genutzten Items sind nationalen Studien entnommen, die durch ausführliche Recherche identifiziert worden sind. Da die Ziele der endgültigen Untersuchung die Identifikation der Defizite bei Jugendlichen in den einzelnen Dimensionen des Datenschutzkompetenzmodells und der Nachweis der Abhängigkeit der Dimensionen im Modell sind, ist es unabdingbar festzustellen, welches Item welche Dimension misst. Ferner gilt es, hierbei die geeignetsten Items herauszufiltern.

Eine abgewandelte Form des Verfahrens der Q-Sortierung (Funder et al. 2000) bietet hier einen Ansatz, um eine objektive Zuordnung der Items zu den entsprechenden Dimensionen vorzunehmen. Die Idee ist, dass eine repräsentative Anzahl an Personen gebeten wird, ihre Einschätzung zu einem Sachverhalt – hier die Zuordnung der Items zu den Dimensionen – abzugeben. Wenn sich eine deutliche Mehrheit in der Zuordnung bildet, dann darf angenommen werden, dass das entsprechende Item die zugehörige Dimension misst. Ein Vorteil dieses Verfahrens ist die rasche Verfügbarkeit von Resultaten.

Um ein möglichst objektive Einschätzung zu erhalten, wurden knapp 80 Personen um die Teilnahme an der Q-Sortierung gebeten. Der Kreis setzte sich aus Wissenschaftlern, Lehrkräften und Studierenden[140] aus den Gebieten der Informatik bzw. MINT-Fächern, Erziehungswissenschaften und Jura zusammen, wobei auf eine Gleichverteilung der Geschlechter geachtet worden ist. Der den Personen vorgelegte Fragebogen und Auswertungsbogen ist im Anhang A4.2 und A4.3 hinterlegt.

Der Fragebogen ist in neun Teile geteilt. Teil A trägt den Titel *Persönliche Einschätzungen* und beinhaltet Fragen zur Selbsteinschätzung von Kompetenzen und zur Einschätzung von Verhalten und Wissen. Im Teil B *Internetnutzung* sind Fragen zu Maßnahmen und Strategien einer sicheren Internetnutzung und zur Anwendung von Messengern zusammengefasst. Unter dem

[140] Studierende an der Teilnahme zu bitten, lag die Idee zugrunde, dass sie der Generation *Digital Natives* angehören.

Titel *Technisches* (Teil C) finden sich Fragen zu Browsertools, zur Aufgabe einer Firewall und Wissensfragen rund um die Internetnutzung. Inhaltlich gleich ist Teil D mit Fragen zu Computerviren, WLAN-Verschlüsselung, Gefahr von Dateitypen und Computereinstellungen zur sicheren Internetnutzung. Rechtliche Aspekte umfassen Teil E, in dem die Probanden den Wahrheitsgehalt von Aussagen einschätzen und den Begriff der *informationellen Selbstbestimmung* kennen müssen. Teil F ist dem Datenschutz gewidmet und beinhaltet Fragen zur Nutzung Sozialer Netzwerke und zur Sensibilität persönlicher Daten in solchen. Dem folgt Teil G mit Privatsphäreeinstellungen in Sozialen Netzwerken, Selbsteinschätzung über die Veröffentlichung persönlicher Daten im Rahmen der Internetnutzung und Wissensfragen zum Datenschutz. Der vorletzte Teil H trägt den Titel *Risiko vs. Vertrauen* und verlangt Einschätzungen zu Vertrauen in Dinge rund um Computer und Internetnutzung, zu Risiken im Umgang mit Computer und Internet und der Entlarvung einer Phishing-E-Mail. Im letzten Block werden Alter, Geschlecht und Informationswünsche abgefragt. Die Gliederung des Bogens war rein inhaltlicher Art gewählt.

Eine Rückmeldung von 32 Personen führte zu dem im Anhang A4.4 aufgelisteten Ergebnis. Items, bei denen keine eindeutige Zuordnung gab oder deren Formulierung mehrdeutig war, sind aussortiert worden. Trotzdem gab es auch Items, die zwar eine Zuordnung zuließen, aber kein ganz klares Votum zeigten. So ist z. B. die Frage, ob und welche Privatsphäreeinstellungen im genutzten Sozialen Netzwerk geändert wurden (oder nicht), von 33 % der Q-Sortierer als Urteilskompetenz und nur von 13 % als Risikobewertungskompetenz identifiziert worden, wenn gleich in diese Frage beide Dimensionen reinspielen.[141] Dieses Item wurde letztendlich wegen des größeren Anteils der Urteilskompetenz zugeordnet.

Den Teilnehmern wurde zudem die Möglichkeit gegeben, eine Zweitzuordnung der Items zu einer Dimension zu geben, wenn ihnen die Zuordnung nicht eindeutig erschien. Für die Auswertung spielte diese Zweitzuordnung dann aber letztlich keine Rolle, weil bei einer ausreichenden Anzahl an Items sich ein relativ klares Bild der Zuordnung abgezeichnet hat.

Die Auswertung der Rückmeldung brachte jedoch leider keine gleiche Anzahl an Items für jede einzelne Dimension. Aus dem Bereich *Wissen* waren deutlich mehr Items als aus dem Gebiet *Urteilskompetenz* charakterisiert worden. Dies war aber auch nicht weiter verwunderlich, nachdem schon die Vorauswahl aus den genutzten Studien keine Gleichverteilung auf der Basis der Dimensionen vermuten ließ. Wissensfragen waren weit überproportional vertreten.

[141] Weitere Verteilung: *Wissen* 17 %, *Auswahl- und Nutzungskompetenz* 22%, *Handlungskompetenz* 21%.

Am Ende ergab sich folgende Itemanzahl pro Dimension:

Dimension	Item[142]	Anzahl
W	C1-C5 und E1-E2	15
RK	A2, (D6)[143], F1, F2, H1f, H1g und H1h	8
ANK	G1-Block1, G1-Block2, H1a und H1e	4
UK	B1, B3b, B3c und H1d	3
HK	B3a, G2, H1b, H1c, H1i, H1j, H1k, H1l	8

Tab. 4.2: Anzahl der Items pro Dimension

Der Fragekatalog für die Umfrage wurde ferner um vier Items, die nach der Kenntnis und Nutzung von Browsern und Browsertools fragen, ergänzt, ohne dass diese den Q-Sortierern vorlagen oder bewertet worden sind. Diese Fragen standen erstmals in dem Papierfragebogen aus dem Sommer 2016 (vgl. Anhang A4.12), wurden zuerst in *LimeSurvey* gar nicht übertragen und dann letztendlich aufgenommen. Dies geschah aus dem Grund, dass einerseits das Interesse des Autors bestand, diese Informationen abzugreifen, und andererseits die vier Items als „einfache“ Fragen in der Mitte des Fragebogens einen Motivationsfaktor für die Schüler darstellen sollten, um weiter zu antworten, falls durch die vorherigen Fragen der Eindruck entstünde, „schlecht“ abgeschnitten zu haben.

Bevor aus den final ausgewählten Items der Fragebogen für die Pilotierung erstellt worden ist, wurden die Fragen einer erfahrenen Grundschullehrkraft vorgelegt, um möglicherweise auftretende Sprachschwierigkeiten bei den Kindern entgegen zu wirken. Daher wurde einige Fragen adaptiert und dann in *LimeSurvey* implementiert. Der Fragebogen für die Pilotierung findet sich in Anhang A4.5.

4.2.3. Pilotierung (Herbst 2017)

Die Pilotierung – auch Pre-Test genannt – verfolgt laut (Homburg und Krohmer 2008, S. 46) in erster Linie das Ziel, die Verständlichkeit der Fragen und des Fragebogens innerhalb der Zielgruppe zu klären (weisen die Schüler ein ausreichendes Wissen zur Beantwortung auf, werden bei den Antwortmöglichkeiten alle wesentlichen Gesichtspunkte erfasst und ist die zur Verfügung stehende Zeit für die Beantwortung ausreichend). Sie erfolgte im November 2017 am Goethe-Gymnasium in Germersheim.[144] Mit der Schulleitung war vereinbart worden, dass je eine Lerngruppe der Klassenstufe 5, 6 und 7 an der Pilotierung teilnehmen, um das gesamte Altersspektrum der späteren Teilnehmer abzudecken.

Der Fragebogen, dessen Fragen sich aus den Ergebnissen der Q-Sortierung ergibt (vgl. Abschnitt 4.2.2), ist prinzipiell angelehnt an den Bogen der Prä-Pilotierung (vgl. Abschnitt 4.2.1),

[142] Die Abkürzung bezieht sich auf das Item im finalen Fragebogen im Anhang A4.7.
[143] Sofern der Schüler einen Messenger nutzt und diese Frage beantwortet.
[144] Zum Genehmigungsverfahren der Schulaufsicht siehe Abschnitt 4.2.4

jedoch sind die Frage umgestellt und kleinere Blöcke eingerichtet worden, die jeweils eine Internetseite darstellen. Durch die Untergliederung sollte vor allem eine Übersichtlichkeit erreicht und damit verbunden ein längeres Scrollen über eine Seite verhindert werden. Die folgende Tabelle dokumentiert den Seitenaufbau, dem die Begründung dafür folgt. Der Fragebogen ist im Anhang A4.5 hinterlegt:

Seite	Inhalt
1	Begrüßungstext und Erläuterungen zur Durchführung
2	Nutzung Sozialer Netzwerke; Sensibilität persönlicher Daten bei der Veröffentlichung in Sozialen Netzwerken
3	Privatsphäreeinstellungen in Sozialen Netzwerken; Informationen zur eigenen Person im Internet
4	Wissensfragen (Faktenwissen)
5	Kenntnis über und Nutzung von Browsern und Browsertools; Nutzung von Messengern
6	Wissensfragen (Faktenwissen; Einschätzung des Wahrheitsgehalts von Aussagen)
7	Einschätzung von Risiken im Internet
8	Technische Maßnahmen zur sicheren Internetgestaltung
9	Einschätzung des eigenen Verhaltens bei der Internet- und Computernutzung
10	Persönliche Angaben (Alter, Geschlecht, Schulform, Informationswünsche)

Tab. 4.3: Inhaltsübersicht der einzelnen Seiten des Pilotierungsfragebogens

Der Fragebogen ist so aufgebaut, dass die Schüler auf der zweiten und dritten Seite Fragen erhalten, die sie beantworten können, damit zu Beginn keine Frustration erzeugt wird, da davon ausgegangen werden kann, dass alle Umfrageteilnehmer Soziale Netzwerke[145] kennen und mehrheitlich sicherlich auch nutzen. Dem schließt sich die erste von zwei Wissensfragenseiten an. Hier werden Begriffe aus dem alltäglichen Umgang mit dem Computer und Internet als Multiple-Choice-Fragen gestellt. Um einen zweiten Wissensblock, der den Wahrheitsgehalt von Aussagen abfragt, vom ersten zu trennen, werden dazwischen auf der fünften Seite wiederum Fragen im Umgang mit dem Internet gestellt, die sich aus der täglichen Nutzung ergeben, sodass diese ebenfalls als einfach einzustufen sind und einer Frustration entgegenwirken sollen. Mit der siebten Seite beginnen nun Fragestellungen rund um die Risikoeinschätzung (Was sind Risiken? Wie hoch werden Risiken eingeschätzt?), um dann auf der folgenden Seite nach technischen Maßnahmen zur sicheren Internetgestaltung zu fragen. Bevor auf der letzten Seite, wie bei Studien üblich, die persönlichen Daten eines jeden einzelnen Teilnehmers erfasst werden, geht es auf der Seite zuvor um das eigene Verhalten im Umgang mit Computer und Internet. Insgesamt ist eine (leichte) Steigerung des Schwierigkeitsgrads durch diese Gliederung erreicht worden.

[145] Zu der Auswahl der Internetplattformen für Soziale Netzwerke siehe Anhang A4.17.

Die Lehrkräfte, die die Durchführung der Umfrage betreuten, sollten eine Rückmeldung zu folgenden Aspekten geben:

- Waren die Anleitungen für die Lehrer, die Erläuterungen für die Erziehungsberechtigten und für die Schüler und die Information für die Schulleitung ausreichend und verständlich?[146]
- Kam es während des Prozesses der Durchführung zu technischen Problemen? War die Bedienung von *LimeSurvey* einfach und intuitiv?
- Wie lange haben die Schüler im Schnitt benötigt, um alle Fragen zu beantworten?
- Gab es Begriffe, einzelne Fragen oder Ähnliches, die von den Schülern nicht verstanden worden sind? Sind die Schüler dazu während der Durchführung auf die Lehrkräfte zugegangen?

Die Schulleitung meldete zurück, dass die den Erziehungsberechtigten und ihnen zur Verfügung gestellten Informationen und Erläuterungen ausreichend waren, sodass an dieser Stelle kein Änderungsbedarf bestand. Zudem kam es während der Durchführung innerhalb der Unterrichtsstunden zu keinen technischen Problemen. Die Schüler konnten die URL zur Umfrage aufrufen und den Browser und die Software bedienen.

Während die Schüler der Klassenstufe 5 gute 30 Minuten zur Beantwortung benötigten, hatten die Schüler der 7. Klasse schon nach 20 Minuten alle Fragen bearbeitet. Diese angegebenen Zeiten entsprachen der Erwartung des Autors.

Leider hat der Autor es versäumt, mit den einzelnen betreuenden Lehrkräften Rücksprache zu halten. Dies wird sich noch als ein Fehler erweisen, denn die Rückmeldung des stellvertretenden Schulleiters lautete, dass es zu keinen nennenswerten Problemen in Bezug auf den letzten oben genannten Aspekt gekommen sei. Diese Aussage war aber zu pauschal. Die Durchführung der finalen Erhebung (vgl. Abschnitt 4.2.4) wird nämlich zeigen, dass es an einigen Stellen zu erheblichen Problemen kommen wird. Sie werden einerseits die Bedienung des Computers und die Nutzung des Browsers, andererseits aber auch das Verständnis verschiedener Begriffe betreffen.

Der nächste Schritt bestand nun darin, die Ergebnisse der Pilotierung einer ersten Auswertung zu unterziehen. Ziel ist es nicht, bei diesem kleinen Teilnehmerkreis detaillierte Daten und Aussagen abzuleiten, sondern die gesamte Machbarkeit der Auswertung zu prüfen. Während die deskriptive Form problemlos darzustellen war, zeigten sich einige Schwierigkeiten bei der korrelativen Anwendung. Da z. B. bei den Items auf die originalgetreue Übernahme geachtet worden ist, gab es Items mit unterschiedlichen Skalenniveaus (3-, 4- und 5-Likert-Skalen). Um diesem Problem zu begegnen, wurden für die finale Version alle Skalen auf das Niveau fünf angepasst.

[146] Diese gesamten Unterlagen sind im Anhang A4.6 hinterlegt.

Der finale Fragebogen enthält folgende Änderungen im Vergleich zum Fragebogen der Pilotierung:

- Aufgrund des Hinweises der Schule wurde der Begrüßungstext zum einen um die Bemerkung, den Text der ersten Seite sorgfältig zu lesen, und zum anderen um die beispielhafte Erläuterung einer 5-Likert-Skala erweitert.
- Die 3- und 4-Likert-Skalen wurden zur Vereinheitlichung alle auf 5-Likert-Skalen gesetzt (z. B. F2, H1) und die Antwortmöglichkeit *weiß nicht* entfernt (z. B. A2, H1). Dadurch sind die Schüler gezwungen eine Antwort zu geben. Im Fall von F2 wurde die „Richtung" von hohem zu geringem Risiko umgedreht, damit alle Likert-Skalen von *sehr hoher Eigenschaft* nach *sehr schwacher Eigenschaft* gerichtet sind. Unterschiedliche Richtungen könnten bei unkonzentriertem Lesen leicht überlesen werden.
- In B3 z. B. sind die Freitextfelder entfernt worden, da es hier keine Einträge gab.
- In C5 z. B. wurde die Bezeichnung *URL* durch den Begriff *Internetseitenadresse* ergänzt, um keine Unklarheiten bei Bezeichnungen zu erzeugen.
- Der Fragenblock G war sehr lang und wurde der Übersichtlichkeit wegen gesplittet.
- Bei den Antwortmöglichkeiten wurden nicht nur die Satzenden, sondern vollständige Sätze formuliert (z. B. C4, F2), um das Lesen zu vereinfachen.

Der finale Fragebogen zur Durchführung der Studie, der sich nun ergab, wird im folgenden Abschnitt vorgestellt.

4.2.4. Durchführung der Studie (Winter 2017/2018)

Der finale Fragebogen zur Durchführung der Studie hat die in Tabelle 4.4 ersichtliche Gliederung, die größtenteils der Gliederung des Pilotierungsfragebogens entspricht, und befindet sich im Anhang A4.7.

Seite	Inhalt
1	Begrüßungstext und Erläuterungen zur Durchführung
2	Nutzung und bevorzugte Nutzung Sozialer Netzwerke; Sensibilität persönlicher Daten bei der Veröffentlichung in Sozialen Netzwerken
3	Privatsphäreeinstellungen in Sozialen Netzwerken; Informationen zur eigenen Person im Internet
4	Wissensfragen (Faktenwissen)
5	Kenntnis über und Nutzung von Browsern und Browsertools; Nutzung von Messengern
6	Wissensfragen (Einschätzung des Wahrheitsgehalts von Aussagen)
7	Einschätzung von Risiken im Internet
8	Allgemeine und technische Maßnahmen zur sicheren Internetgestaltung
9	Einschätzung des eigenen Verhaltens bei der Internet- und Computernutzung
10	Persönliche Angaben (Alter, Geschlecht, Schulform, Informationswünsche)

Tab. 4.4: Inhaltsübersicht der einzelnen Seiten des finalen Fragebogens

Die Durchführung einer Studie (inkl. Pilotierung) an rheinland-pfälzischen Schulen ist nur dann zulässig, wenn dies vorher bei der Schulaufsicht in Rheinland-Pfalz, der Aufsichts- und Dienstleistungsdirektion Trier (ADD), beantragt bzw. im Fall der Hochschulen angezeigt worden ist.[147] Neben einem formgebundenen Antrag ist der Fragebogen der Erhebung beizufügen, damit auch eine datenschutzrechtliche Prüfung erfolgen kann. Die Anzeige im vorliegenden Fall wurde ohne Auflagen zur Kenntnis genommen.

Somit konnte die Studie von Dezember 2017 bis Januar 2018 durchgeführt werden.[148] Um eine hohe Akzeptanz an den Schulen und eine gute Teilnehmerquote zu erreichen, wurde der Versuch unternommen, EPOS für die Bewerbung der Studie zu nutzen.[149] Die ADD lehnte eine Information an die Schulen über EPOS ab, da sie sich für nicht zuständig ansah. Das Pädagogische Landesinstitut (PL) schlug eine Bewerbung aus, da viele Schulen die Rückmeldung gäben, dass EPOS vom PL für zu viele Dinge genutzt würde, sodass PL-Mitteilungen an Schulen häufig ignoriert würden. Das Ministerium für Bildung (MB) lehnte eine Bewerbung ab, da ansonsten ein Präzedenzfall für weitere Hochschulstudien geschaffen werde.

Daher wurden alle in Betracht kommenden Schulen (Gymnasien, Realschulen Plus und Integrierten Gesamtschulen) am 24.11.2017 vom Autor persönlich per E-Mail mit der Bitte um Teilnahme angeschrieben und alle Unterlagen (vgl. Anhang A4.6) direkt mitgesandt, damit es zu möglichst wenig Rückfragen seitens der Schulen kommen möge.

Um Unterstützung im Werbeprozess wurde das Zentrum für Lehrerbildung am Campus Koblenz gebeten, welches ein Kooperationsprojekt *Netzwerk Campus-Schule* leitet. Die in diesem Netzwerk kooperierenden Schulen wurden um Teilnahme gebeten. Ferner fand eine Bewerbung über den Newsletter für die Informatiklehrkräfte durch die regionalen Fachberater statt. Zeitgleich erschien der Hinweis auf dem Informatik-Bildungsserver. Über den Sprecher der Direktorenkonferenz Region Trier wurden die dortigen Gymnasien zur Teilnahme eingeladen.

Da der erste Rücklauf an Teilnahmezusagen noch sehr schwach gewesen war, wurde eine zweite Runde an E-Mails an die Schulen versandt. Gleichzeitig fanden Gespräche mit der Dienststelle des Datenschutzbeauftragten des Landes Rheinland-Pfalz statt und es wurde um Unterstützung der Bewerbung gebeten.

Am Ende sind dem Autor 16 Einverständniserklärungen von den Schulen zugesandt worden. Jedoch aufgrund von Gesprächen mit dem Autor bekannten Lehrkräften kann der Rückschluss

[147] Grundlage ist hier § 67 (6) des SchulG i. d. F. v. 16.02.2016 (vgl. https://bm.rlp.de/fileadmin/mbwwk/Publikationen/Bildung/Schulgesetz_2016.pdf; Stand: 27.01.19).

[148] Ursprünglich sollte der Zeitraum schon Anfang Januar enden. Jedoch aufgrund der Tatsache, dass an vielen Schulen im Dezember noch schriftliche Überprüfungen und Veranstaltungen wie Weihnachtskonzerte stattfinden und zudem die Weihnachtsferien in den Zeitraum fielen, wurde eine Verlängerung beschlossen. Wie die Teilnehmeranzahl später zeigte, war dies eine vernünftige Entscheidung.

[149] EPOS ist ein Rheinland-Pfalz-weites E-Mail-System für Schulen, welches von Behörden zur Postverteilung genutzt wird.

gezogen werden, dass nicht alle teilnehmenden Schulen einen solche Erklärung auch abgegeben haben. Somit kann eine genaue Anzahl an teilnehmenden Schulen nicht festgestellt werden.

Noch während des Erhebungszeitraums wurde der Autor von sechs Lehrkräften kontaktiert, weil ihre Schüler Probleme bei der Bearbeitung des Fragebogens hatten. Zusammenfassend wurden folgende Kritikpunkte genannt:

- Man müsse bedenken, dass Schüler in diesem Alter noch nie an einer Umfrage teilgenommen hätten. Diese Umfrage sei zu anspruchsvoll.
- Schüler konnten die URL im Browser nicht eingeben, weil ihnen (a) nicht bekannt war, wie dies zu tun sei, und (b) die Nutzung einer Tastatur fremd sei (Eingabe eines Doppelpunkts oder eines Slashs war nicht möglich). Dies läge daran, dass die Schüler nicht mehr am Computer arbeiten, sondern stattdessen Smartphones (bevorzugt mit Sprach- statt Texteingabe) nutzen würden.
- Die allermeisten Fragen wurden in der Regel wegen der Fachbegriffe nicht verstanden (z. B. was ein Profil sei). Der Fragebogen sei an der Zielgruppe vorbei konzipiert worden.
- Der Text auf der Begrüßungsseite sei viel zu lang und für Schüler Klasse 5 nicht zu verstehen (passend wäre er für Schüler der Klassenstufe 9). Die Metaanweisungen können Schüler in diesem Alter nicht verstehen.
- Besser wäre gewesen, wenn es noch die zusätzliche Antwortmöglichkeit „Frage verstehe ich nicht“ gegeben hätte.
- Bei fast allen Schülern könne man ganz allgemein ein vermehrtes Aufmerksamkeitsdefizitsyndrom diagnostizieren. Die Umfrage sei zu umfangreich für diese Altersstufe.
- In WhatsApp werden (i) vor allem Sprachnachrichten versandt, (ii) Satzzeichen ausgelassen und (iii) alles klein und nur noch in Drei-Wort-Sätze geschrieben. Eine fehlende Kommunikationskultur wurde beklagt.
- Es soll sogar Schülerinnen gegeben haben, die weinend vor den Fragen gesessen hätten, da sie den Text nicht verstanden hätten.

Dazu kamen auch noch Probleme organisatorischer Art an Schulen, auf die der Autor keinen Einfluss hatte:

- Ein Lehrer wurde am Morgen überraschend zu einer 90-minütigen Vertretungsstunde in einer 5. Klasse bestellt, die ihm aus dem regulären Unterricht nicht bekannt ist. Da nicht alle Schüler die Teilnahmeerklärung abgegeben hatten, musste er zwei unterschiedliche Gruppen betreuen, was letztendlich zu massiver Unruhe und dem Abbruch der Studienteilnahme führte.
- Schüler waren im Vorfeld noch nie in dem Computerraum der Schule und kannten den Anmeldeprozess zu ihren Konten und die Verhaltensregeln in dem Raum nicht.
- Wegen technischer und anderer Probleme begannen Schüler erst nach 30 Minuten mit der Umfrage.

Bemerkenswert ist, dass im Rahmen der Pilotierung die erstgenannten Kritikpunkte gar nicht genannt worden sind. Gründe dafür sind vielfältig und es können nur Vermutungen angestellt werden, die nicht zu belegen sind. Durch eine Rückfrage des Autors bei dem stellvertretenden Schulleiter der Pilotschule konnten keine logisch ableitbaren oder beweisbaren Gründe identifiziert werden.

Insgesamt haben an der Studie 1077 Schüler teilgenommen, wobei nur 1013 Fragebögen vollständig beantwortet worden sind. Von diesen waren jedoch nur 996 Datensätze brauchbar, denn die Restlichen ließen aufgrund der gegebenen Antworten daraus schließen, dass die Umfrage nicht mit dem notwendigen Ernst angegangen worden ist.

Im folgenden Abschnitt werden die Ergebnisse der Studie diskutiert.

4.3. Datenanalyse

Von den Anfängen, die Datenschutzkompetenz bei den Jugendlichen zu untersuchen, bis hin zur endgültigen Erhebung umfasst es den Zeitraum vom Frühjahr 2016 bis zum Januar 2018. Die Ergebnisse der ersten Befragung vom Sommer 2016 sind im Abschnitt 4.3.1. diskutiert, erste Aussagen der Prä-Pilotierung sind knapp in Abschnitt 4.3.2 zu finden und die Ergebnisse der finalen Erhebung sind im Abschnitt 4.3.3 dargelegt.

Die Daten der Pilotierung vom November 2017 sind aus unterschiedlichen Gründen nicht ausgewertet worden. Ein Ziel war gewesen, den Umgang mit *LimeSurvey* für die Schüler zu überprüfen (Wie sind die Schüler mit dem Tool zurecht gekommen? Ist der gewählte Zeitansatz realistisch?). Zudem galt es zu testen, ob die Fragestellungen passend und altersgemäß gewählt worden sind. Ferner wurde die Export-Funktion von *LimeSurvey* und die Auswertungsmöglichkeiten im Ansatz überprüft. Und da letztendlich nur rund 80 Jugendliche (statt rund 1000 Schülern in der finalen Erhebung) teilgenommen hatten und ein Vergleich oder ein In-ein-Verhältnis-Setzen der Daten der Pilotierung mit dem der finalen Erhebung keinen Sinn ergibt, werden die Daten der Pilotierung nicht diskutiert. Hinzu kommt, dass einige Items für die finale Erhebung überarbeitet worden sind (z. B. Vereinheitlichung der Likert-Skala). Weitere Erläuterungen sind in Abschnitt 4.2.3 zu finden.

4.3.1. Ergebnisse der Erhebung vom Sommer 2016

Die Erhebung bestand aus zwei Teilen: (1) Einem Fragebogen und (2) einem geleiteten Interview, welches der Autor geführt und mit Einverständnis der Schüler aufgenommen hat. Da diese Erhebung einen ersten Versuch zur Datenschutzkompetenzmessung darstellt und die spätere Studie ganz anders aufgebaut ist, werden die Ergebnisse aus (1) nur knapp präsentiert. Zudem lag auch das Datenschutzkompetenzmodell noch nicht in der endgültigen Form so vor, weshalb die Fragen ohne Bezug zu den Dimensionen gestellt worden sind. Jedoch waren die

hierbei gemachten ersten Ergebnisse mitentscheidend für den weiteren Entwicklungsprozess der Umfrage, weshalb an dieser Stelle über ausgewählte Ergebnisse berichtet werden soll.

Der Fragebogen (s. Anhang A4.12) wurde von allen Teilnehmern in Einzelarbeit innerhalb einer guten halben Stunde unter Aufsicht des Autors, der für Rückfragen zur Verfügung stand, durchgeführt. Bis auf die Fragen I., II., VII., X., XIII.2, XIX. und XXIII. sind alle Fragen Studien entnommen[150]. Die Auswertung erfolgte deskriptiv und ist im Anhang A4.13 zu finden.

An der Befragung haben neun Jungen und vier Mädchen im Alter von zwölf bis 19 Jahren teilgenommen, wobei sieben Personen zwischen 14 und 16 Jahren die Mehrheit bildeten. In sieben Fällen wurde das Thema *Datenschutz* im Unterricht schon behandelt, wobei neben ITG/EDV/Informatik auch Medienpädagogik, Deutsch und ein Kompetenztraining genannt worden sind. Nur fünf Teilnehmer haben das Fach *Informatik* in Form von Unterricht oder einer AG kennengelernt.

Alle Befragten nutzen das Internet, um Videos zu schauen (*YouTube* ist mit weitem Abstand die meist besuchte Seite), und zwölf von 13 Schüler mailen, wobei eher zu erwarten gewesen wäre, dass die Nutzung von Messenger-Diensten mehr im Vordergrund stünde.[151] *WhatsApp* wird von elf Schülern als Messenger benutzt, dem mit acht Personen SMS folgt und nur fünf der Befragten *Instagram* nutzen. Soziale Netzwerke werden eher seltener genutzt; sechs Schüler gaben an, *Facebook* zu verwenden.[152] Motive der Internetnutzung sind vor allem Unterhaltung, Beziehungspflege und Informationsrecherche. Gerade die beiden erst genannten Aspekte verlangen eine Förderung der Datenschutzkompetenz, auch wenn die Schüler angeben, dass sie der Meinung sind, dass ihre eigenen Fähigkeiten und ihre Internetkompetenzen hoch sind. Bei einer Datenveröffentlichung im Internet würden immerhin noch sieben Schüler ihren Geburtstag, sechs (also knapp 50 %) ihre Ausbildung und fünf ihre E-Mail-Adresse angeben. Nickname, Fotos und Namen werden als unproblematisch angesehen. Positiv ist zu bemerken, dass alle Teilnehmer Änderungen in den Privatsphäre-Einstellungen ihres Sozialen Netzwerks vorgenommen haben und nicht auf die Einstellungen des Anbieters vertrauen. Weiterhin ist interessant, dass die Schüler sich bei *Facebook* in Bezug auf Datensicherheit eher unsicher, während bei *WhatsApp* und *Instagram* hier sicher bis unentschieden fühlen, wobei vermutlich nicht bekannt ist, dass *Facebook* den Messengerdienst *WhatsApp* aufgekauft hat und Versuche unternimmt, die Daten beider Dienste miteinander zu verknüpfen. Daher vertrauen sie *Facebook* nur wenig, während sie *WhatsApp* und *Instagram* nur skeptisch gegenüberstehen. Die Vermutung ist, dass die Schüler glauben, bei *WhatsApp* unter „sich“ zu sein, und kein anderer außer dem Empfängerkreis ihre Daten liest, da das Unternehmen eine End-To-End-Ver-

[150] Weitere Details sind im Anhang A4.12 zu finden.

[151] Laut KIM-Studie 2016 nutzen 57 % der Kinder *WhatsApp* und 28 % der Kinder E-Mail (fast) jeden Tag oder mehrmals die Woche (Feierabend et al. 2017, S. 35). In den JIM-Studien 2017 und 2018 waren keine konkreten Daten über die Messenger-Nutzung im Vergleich zum Mailen aufgelistet, jedoch lässt die Alltagserfahrung die Vermutung zu, dass die Verwendung von Messengern das Mailen immer mehr verdrängt.

[152] In der Liste der Sozialen Netzwerke wurden auch Internetplattformen aufgenommen, die in diesem Sinne keine solchen sind. Details dazu siehe Anhang A4.17.

schlüsselung verspricht. Insgesamt sind sie sich mehrheitlich einig, dass die persönlichen Daten im Netz weniger sicher sind. Die Einschätzung, was Risiken im Netz darstellen, ist in Tabelle 4.5 dargestellt:

Anzahl	Risiko
4	Verlust persönlicher Daten
6	Andere wissen, was ich tue; Datennutzung für Werbezwecke; Spam
8	Fake-Profil; Beleidigung/Belästigung
10	Veröffentlichung peinlicher Fotos; Betrug
11	Mobbing, Stalking; Versand von Mails in meinem Namen
12	Ausspionieren
13	Unerwünschte Datenweitergabe; Infizierung

Tab. 4.5: Einschätzung von Risiken im Netz

Es ist bei diesen Zahlen insofern überraschend, dass z. B. der Verlust persönlicher Daten von nur so wenigen Befragten als Risiko eingeschätzt wird. Dafür hat der Autor drei Vermutungen, die aber aus den Daten nicht bewiesen werden können: (1) In der Fragestellung ist nicht ausreichend erläutert, was alles ganz konkret mit persönlichen Daten gemeint ist, und daher (2) die Schüler glauben, dass die „paar" Daten, die sie veröffentlicht haben, keine Bedeutung haben, und sind sich damit (3) der Tragweite und Folgen eines Datenverlustes nicht bewusst. Es werden zwar unterschiedliche Maßnahmen zur sicheren Internetgestaltung getroffen, aber nicht von allen Befragten. So werden beim Chatten oder beim Mailen von der deutlichen Mehrheit personenbezogene Daten preisgegeben. Dies steht jedoch im Widerspruch, dass man den Anbietern von Sozialen Netzwerken und Messenger-Diensten nur wenig Vertrauen entgegenbringt. Malware ist den Schülern kaum bekannt, was vielleicht aber auch an dem Begriff liegen mag. Strategien wie die Nutzung von Pseudonymen oder das Löschen von Cookies und Caches oder das Updaten der Anti-Viren-Software werden von der Mehrheit verwendet; Anwendung von Anonymisierungstools, Anti-Tracking-Software und Verschlüsselungssoftware wird kaum genutzt. Fragen aus dem Bereich des Wissens wurden insgesamt zu 62,8 % korrekt beantwortet. Informationen werden vor allem zur rechtlichen Situation, zum Schutz der Daten und den technischen Möglichkeiten gewünscht.

Der zweite Block bestand aus einem geleiteten Interview, dessen Fragen im Anhang A4.14 festgehalten sind. Zu Beginn des Transkribierens zeigte sich rasch, dass eine Codierung der Antworten (für die weitere Auswertung) bei der Vielzahl und Heterogenität der Antworten nur sehr schwer möglich ist. Zudem war ein einheitliches Bild von Aussagen kaum erkennbar und damit darstellbar. Da letztendlich auch eine große Teilnehmerzahl in der Erhebung gewünscht ist, um aussagekräftige Daten zu gewinnen, ist eine qualitative Messmethode (z. B. Inhaltsanalyse) ungeeignet. Daher fiel zu diesem Zeitpunkt die Entscheidung, auf ein qualitatives zugunsten eines quantitativen Verfahrens zur Erhebung der Daten zu verzichten, weshalb auch die Interviewdaten an dieser Stelle dann nicht weiter ausgewertet worden sind.

4.3.2. Ergebnisse der Prä-Pilotierung

Die Daten der Prä-Pilotierung vom Juni 2017 sind aus unterschiedlichen Gründen nicht vollständig und endgültig ausgewertet und dokumentiert worden (z. B. die große Altersspanne der MINT-begabten Befragten, die nicht der späteren Zielgruppe entspricht). In diesem Teilschritt der Studiendurchführung galt es zuerst einmal die „Qualität" der Fragen und ein „Gespür" für die Fragen zu entwickeln. Des Weiteren sollte auf die Funktionalität und die Usability von *LimeSurvey* (für die Schüler, aber auch für die Auswerter) ein Augenmerk gelenkt werden. Und da letztendlich der finale Erhebungsbogen nur einen Bruchteil der Fragen dieses Bogens enthielt, schien es nicht zweckmäßig, alle Daten zu interpretieren und vor allem mit den Daten der finalen Erhebung zu durchmischen.

Durch die Prä-Pilotierung konnten folgende Beobachtungen unter anderem herausgearbeitet werden:

- Den Schülern war der Begriff *Verbraucherbildung* (A14)[153] unbekannt; die Bereiche *Finanzen und Konsum* und *Gesundheit und Ernährung* wurden in zwei bzw. drei Fällen im Unterricht behandelt, während *Datenschutz* immerhin von sieben bejaht, einmal verneint wurden, während fünf Befragte damit nichts anfangen konnten.
- Sieben Schüler waren es, die unter den vier Antwortmöglichkeiten, die richtige Antwort auf die Frage der informationellen Selbstbestimmung (C8) ankreuzten; aber die Rechte und Pflichten bezüglich Datenschutz konnten sie für sich daraus nicht ableiten (B28).
- Sehr lückenhaft waren Fragen zur Selbsteinschätzung (C11) beantwortet worden. Auf die Aussage, dass man g*ut einschätzen könne, was Online-Unternehmen mit den eigenen Daten und Informationen mache*, stimmten nur zwei *voll und ganz* zu und einer stimmte *gar nicht* zu. Oder: Man *kenne Hard- und Softwareanwendungen, mit denen man die eigenen Daten schützen könne* stimmten zwei *voll und ganz* zu und vier *gar nicht* zu.
- Zwölf Teilnehmer wussten, dass Passwörter aus Buchstaben, Ziffern und Sonderzeichen bestehen sollten (D11).
- Auf die Frage nach der Einschätzung zu den eigenen Fähigkeiten und der Internetkompetenz zur Informationsrecherche (B9) schätzten sich acht Schüler *kompetent* ein, während die restlichen Fünf nichts ankreuzten; seine Privatsphäre schützen zu können, sahen sich nur fünf als *kompetent* an, während die anderen Schüler nichts ankreuzten.
- Die Einschätzung bezüglich Datensicherheit in einzelnen Communities (B19) wurde in den meisten Fällen offen gelassen (und wenn sie beantwortet wurden, dann in der Regel mit *nicht sicher*).

[153] Zu der Nummerierung der Fragen siehe Anhang A4.15.

Die Items, die sich für die Schüler als problematisch herausstellten und bei denen sie keine Einschätzung geben konnten, wurden gestrichen, da davon auszugehen ist, dass auch die Zielgruppe der deutlich jüngeren Schüler diese Probleme haben wird. Mit dem überarbeiteten Fragebogen (vgl. Anhang A4.2) wurde die Q-Sortierung (vgl. Abschnitt 4.2.2) durchgeführt.

4.3.3. Ergebnisse der Studie

Die an dieser Stelle vorzustellenden Ergebnisse wurden aus der im Rahmen der Online-Befragung stattgefundenen Studie gewonnen, an der 996 Schüler im Zeitraum von Dezember 2017 bis Januar 2018 teilgenommen haben. Der Anteil der Schülerinnen und Schüler war annähernd gleich. Die Altersverteilung gibt folgende Tabelle wieder:

Alter	< 10 Jahre	10 Jahre	11 Jahre	12 Jahre	13 Jahre	>13 Jahre
Anteil	0,40 %	20,26 %	32,86 %	30,24 %	13,10 %	3,13 %

Tab. 4.6: Altersverteilung der Schüler im Rahmen der Umfrage

Der Altersdurchschnitt betrug 11,2 Jahre. Unter den Jugendlichen besuchten 75,98 % das Gymnasium, 15,48 % die Realschule Plus und 8,54 % die Integrierte Gesamtschule (IGS).

Die Datenauswertung der finalen Erhebung erfolgt in drei Schritten. Der erste Schritt ist eine deskriptive Auswertung (vgl. Anhang A4.9), der sich dann eine bivariate Analyse (korrelative Auswertung; vgl. Anhang A4.11) anschließt, um mögliche Abhängigkeiten zwischen den Dimensionen des Modells aufzuzeigen. In einem dritten Schritt wird anhand ausgewählter Items untersucht, ob alters- oder geschlechterspezifische Aspekte eine Rolle spielen (differenzierte deskriptive Auswertung; vgl. Anhang A4.10). Die detaillierte Aufschlüsselung der Zahlen und deren graphische Darstellung befinden sich im jeweiligen Anhang. Die Ergebnisse der deskriptiven Auswertung werden im folgenden Abschnitt, zu dem die Veröffentlichung (Hug 2018) existiert, mit ausgewählten Graphiken vorgestellt und interpretiert.

4.3.3.1. Deskriptive Auswertung

Wie aus dem Anhang A4.7 ersichtlich, sind den Items die jeweiligen Dimensionen (im Anhang rot geschrieben) zugewiesen, die sich aus den Ergebnissen des Q-Sortierungsprozesses ergeben (Anhang A4.4). Zudem ist jedem Item die entsprechend zu überprüfende Datenschutzkompetenz (vgl. Tabelle 3.8) zugeordnet.

Es folgt zuerst eine Beschreibung der Ergebnisse sortiert nach den Dimensionen des Modells und anschließend die Beschreibung der Items, die im Prozess der Q-Sortierung nicht eingebunden waren. Für jede Dimension folgt abschließend eine Gesamtbeurteilung der Kompetenz, die sich an folgender Skala orientiert:

Prozentualer Anteil „korrekter“ Antworten	Notenstufe/Leistung
100 % - 91 %	sehr gut
90 % - 81 %	gut
80 % - 66 %	befriedigend
65 % - 50 %	ausreichend
Weniger als 50 %	mangelhaft

Tab. 4.7: Notenschlüssel für die Gesamtbeurteilung

Die Berechnung des jeweiligen prozentualen Anteils ist im Anhang A4.8 beschrieben.

Dimension *Wissen*:

Die Gruppe der Wissensfragen ist in zwei Blöcke eingeteilt. Im ersten Block werden Fachbegriffe abgefragt, die über Multiple-Choice zu beantworten sind.[154] Hierbei ist je eine Aussage richtig und den Probanden wird pro korrekter Antwort ein Punkt vergeben, wobei *weiß nicht* als falsche Antwort gewertet wird. Am Ende wird die Summe der korrekten Antworten betrachtet. Es sind ein Fünftel (19,5 %) der vorgegebenen Antworten richtig, während mehr als die Hälfte (55,5 %) *weiß ich nicht* lautet (Abb. 4.1). Gut zwei Fünftel (45,3 %) der Teilnehmer gibt keine richtige Antwort oder weiß es nicht. Immerhin bei rund einem Viertel (28,1 %) ist es noch eine korrekte Antwort unter allen (Abb. 4.2).

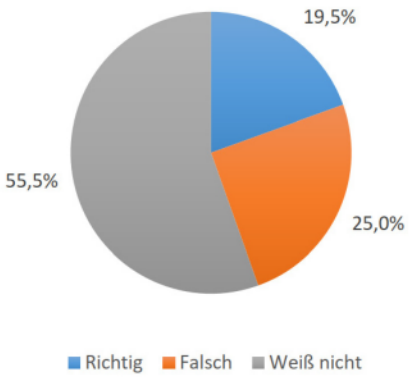


Abb. 4.1: Anteil aller abgegebenen Antworten im ersten Wissensteil (Anhang Abb. A4.9-6)

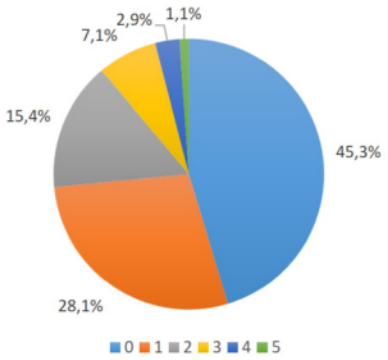


Abb. 4.2: Anzahl an richtigen Antworten im ersten Wissensteil (Anhang Abb. A4.9-7)

[154] Die Ratewahrscheinlichkeit für die jeweils korrekte Antwort der Multiple-Choice-Aufgaben beträgt 1/4 (unter der Annahme, dass *weiß nicht* nicht geraten wird).

Im zweiten Block werden Aussagen zu den Themen *Datenschutzerklärung*, *Urheberrecht*, *Tracking* und *Nutzung von Nutzerdaten durch Dritte* getroffen und die Probanden entscheiden, ob diese wahr oder falsch sind; als dritte Antwortoption steht *weiß nicht* zur Verfügung. Hierbei wird pro korrekte Antworte ein Punkt vergeben, wobei *weiß nicht* als falsche Antwort gewertet wird. Am Ende wird die Anzahl der korrekten Antworten aufsummiert. Während knapp die Hälfte (46,7 %) der vorgegebenen Antworten *weiß ich nicht* lautet, können 35,5 % aber als korrekt verbucht werden (Abb. 4.3). Im Schnitt sind zwei bis vier (von zehn) Fragen bei knapp 50 % der Schüler korrekt beantwortet, wobei nur ca. ein Drittel der Befragten noch mehr richtige Antworten geben kann. Keine oder nur eine Frage beantworteten 17,9 % der Schüler richtig (Abb. 4.4).

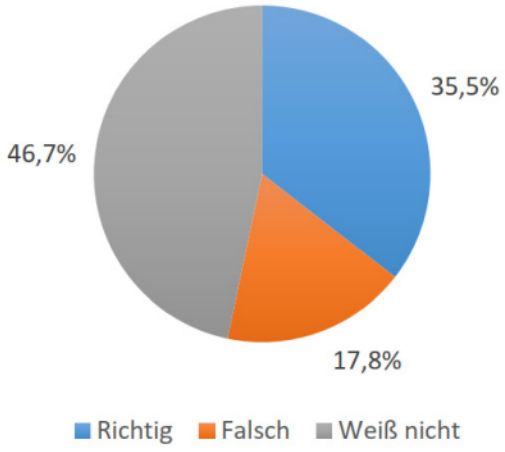


Abb. 4.3: Anteil aller abgegebenen Antworten im zweiten Wissensteil (Anhang Abb. A4.9-15)

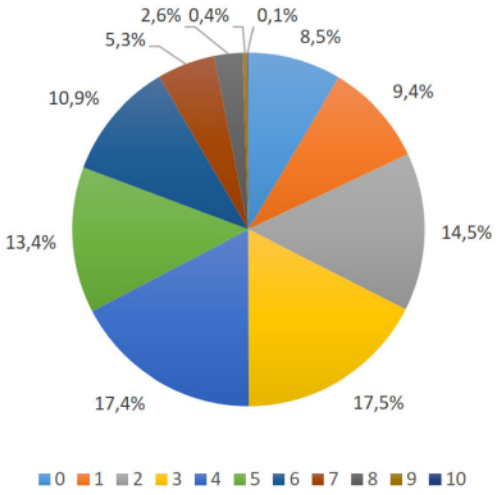


Abb. 4.4: Anzahl an richtigen Antworten im zweiten Wissensteil (Anhang Abb. A4.9-16)

Vergleicht man die beiden Blöcke miteinander, so kann festgestellt werden, dass der Bereich mit den spezifischen Aussagen besser (35,5 % korrekte Antworten) als der Bereich mit dem Faktenwissen (19,5 % korrekte Antworten) beantwortet worden ist. Der Durchschnittswert liegt bei 27,5 % korrekter Antworten und ergibt somit die Leistung *mangelhaft*.

Dimension *Risikobewertungskompetenz*:

Die persönliche Einschätzung zur Sensibilität veröffentlichter personenbezogener Daten in Sozialen Netzwerken ist ein Maß für die Risikobewertungskompetenz. Die Zahlen zeigen, dass weit mehr als die Hälfte der Befragten (je nach Item zwischen 54 % und 90 %) schon gut zwi-

schen sehr persönlichen Daten und mehr beliebigen Daten unterscheiden kann. Die Items *Religion*[155], *Lieblingsfilm etc.* und *Geburtsdatum* bilden eine Ausnahme. Die Berechnung des Durchschnittwerts für diese Frage ergibt 66,5 %, was einer noch befriedigenden Leistung entspricht (Abb. 4.5).

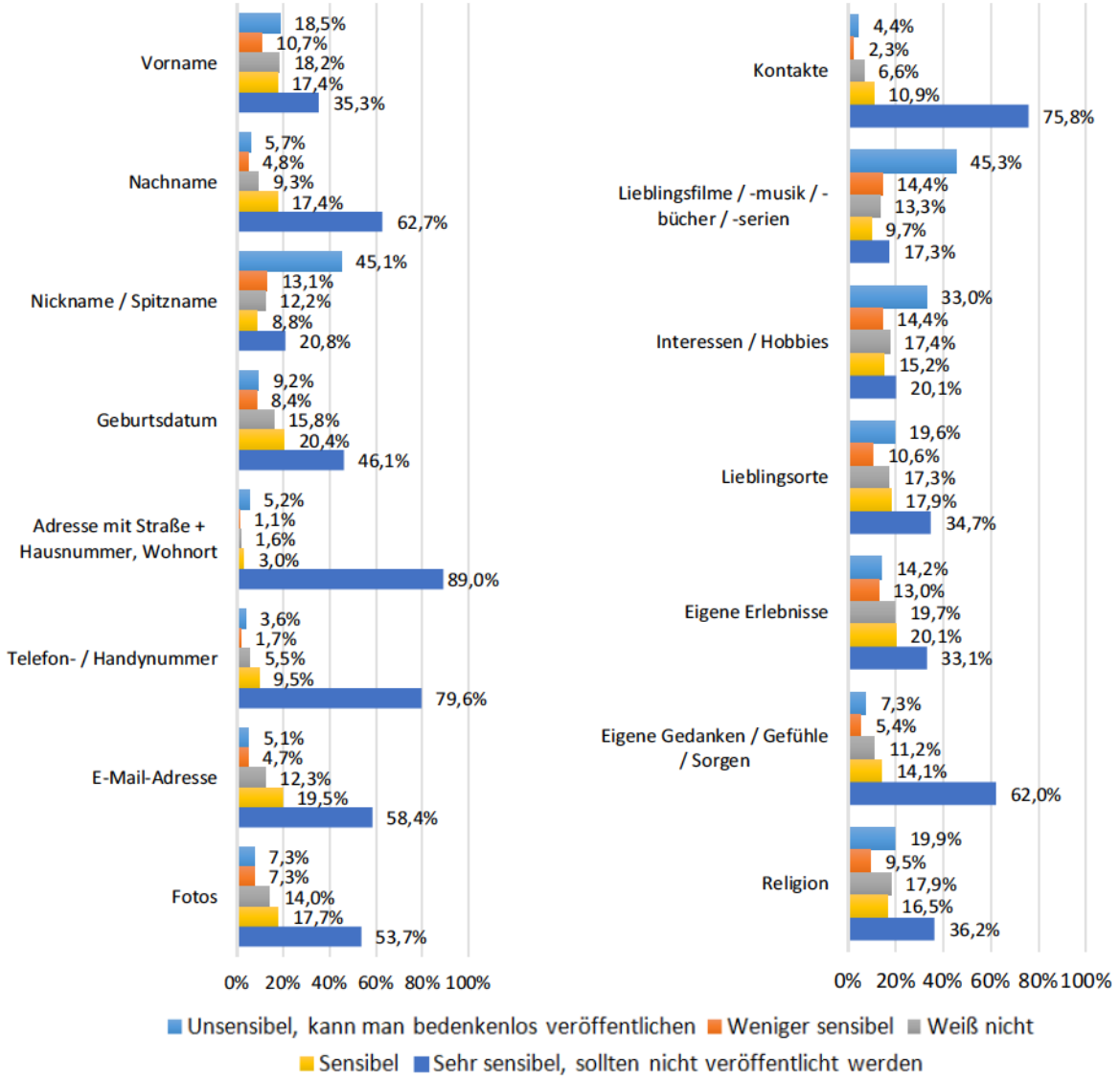


Abb. 4.5: Einschätzung der Sensibilität personenbezogener Daten zur Veröffentlichung in Sozialen Netzwerken (Anhang Abb. A4.9-2)

Bei den Fragen zur Messenger-Nutzung sind eine verschlüsselte Kommunikation und die Identifikationsmöglichkeit des jeweiligen Gegenübers einer sehr klaren Mehrheit wichtig bzw. sehr

[155] Dass die Schüler dieses Item für weniger sensibel halten, mag daran liegen, dass für viele Jugendliche ihre Religion – sofern sie überhaupt einer angehören – eine untergeordnete und geringe Rolle im Alltag spielt (vgl. Shell-Studie 2010, https://jugend.ekir.de/Bilderintern/20100922_zusammenfassung_shellstudie2010.pdf, S. 5).

wichtig (85,4 % bzw. 85,5 %), sodass daraus eine gute Risikobewertungskompetenz abgeleitet werden kann (Abb. A4.9-14).

Innerhalb der Untersuchung wurden die Schüler mit einer Frage zu ihrer Einschätzung nach Risiken im Internet gefragt (Abb. 4.6). In 53,5 bis 64,6 % werden die vorgelegten Fälle[156] als (ernsthafte) Risiken im Internet eingestuft, was positiv zu bewerten ist. Ausschließlich der Spam-Mail-Empfang wird von nur einem Drittel (33,4 %) der Schüler als sehr hohes Risiko eingestuft. Vermutlich werden solche E-Mails eher als eine Belästigung statt als ein Risiko gesehen, da sie einfach weggeklickt werden können. Betrachtet man die Fälle unter der Prämisse *hohes Risiko* und *sehr hohes Risiko*, dann liegt der Mittelwert für diese Frage bei 65,4 %, was einer voll ausreichenden Risikobewertungskompetenz entspricht.

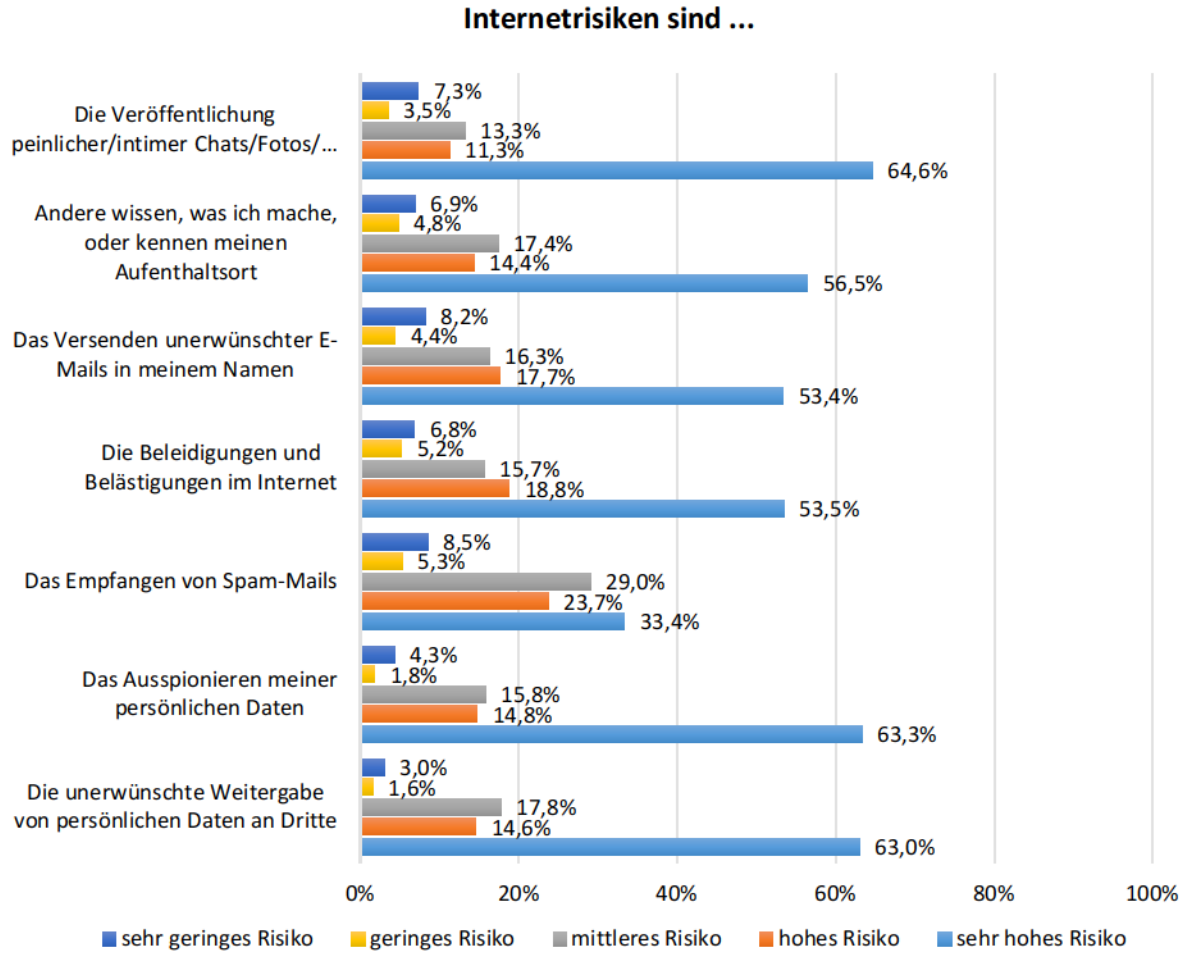


Abb. 4.6: Einschätzung von Internetrisiken (Anhang Abb. A4.9-17)

[156] Die Fälle waren: *Veröffentlichung peinlicher Fotos, den eigenen Aufenthaltsort frei geben, Versand unerwünschter E-Mails im Namen des Schülers, Beleidigung und Belästigung im Web, Empfang von Spam-Mails, Ausspionieren persönlicher Daten* und *unerwünschte Weitergabe persönlicher Daten an Dritte*.

Im darauffolgenden Frageblock sollte eine Risikoabschätzung für eine Virusinfektion durch reines Internetsurfen, durch Dateidownload über Tauschbörsen und durch Öffnen von E-Mail-Anhängen und für eine unbemerkte Infektion entweder durch den Nutzer oder durch einen theoretischen Ausfall der Anti-Viren-Software getroffen werden (Abb. A4.9-18). Im Schnitt sind es zwischen 49,4 % und bis zu 71,2 % der Jugendlichen, die in den gefragten Fällen ein hohes Risiko sehen, sonst schätzt knapp ein Drittel es als mittleres Risiko ein, wobei hierzu auch diejenigen aufgrund des Ankreuzverhaltens gezählt werden, die im Sinne von Unsicherheit geantwortet haben.[157] Im Fall der unbemerkten Infektion mit einem Virus fällt mit 47,7 % ein sehr hohes Risiko durch ein klares Votum ins Auge. Auf Basis des Auswertungsschemas (vgl. Anhang A4.8) ergibt dieser Fragenkomplex einen Mittelwert von 68,9 %, also einer befriedigenden Leistung.

Der Fragekomplex F ergibt somit bei einem Mittelwert von 67,2 % eine insgesamt noch befriedigende Leistung.

Bei den Antworten auf die Fragen, ob darauf geachtet werde, von welchen Seiten die heruntergeladenen Dateien stammen, und ob E-Mail-Anhänge oder zugesandte Links unbedacht und unüberlegt geöffnet werden, gaben im Schnitt 35 % an, bei diesen Tätigkeiten überlegt zu handeln, so spricht dies nur für eine mangelhafte Risikobewertungskompetenz (Abb. A4.9-21).

Fasst man letztendlich alle Durchschnittswerte der Fragekomplexe zusammen, so errechnet sich ein Mittelwert von 63,5 %. Die Risikobewertungskompetenz ist somit voll ausreichend.

Dimension *Auswahl- und Nutzungskompetenz*:

Mit einem Fragekomplex wurde abgefragt, welche technischen Maßnahmen zur sicheren Internetgestaltung von den Befragten ergriffen werden (Abb. 4.7). Mit Ausnahme von Anti-Viren-Software weiß die Mehrheit der Befragten nicht, ob eine entsprechende andere Schutzsoftware auf dem Gerät installiert oder eine Einstellung aktiviert ist. Die Anti-Viren-Software wird von 46 % eingesetzt. Werbefilter[158], Anonymisierungstools und Anti-Tracking-Software kommen kaum zum Einsatz. Bei 24,9 % der Befragten ist die Firewall aktiviert, wobei nur 14,5 % in der Wissensfrage die korrekte Antwort für die Funktion der Firewall angaben. Dies lässt die Vermutung zu, dass die Schüler wissen (weil sie es einmal irgendwo gehört oder gelesen haben), dass es beim Internetsurfen wichtig ist, die Firewall aktiviert zu haben, aber weder die Funktion noch die Bedeutung der Firewall kennen. Knapp 30 % nutzen die Verschlüsselung, wobei aus der Zahl nicht abgeleitet werden kann, ob die Jugendlichen dies aktiv beim Mailen tun oder die Verschlüsselung bei einem Messenger automatisch aktiviert ist.[159] Aus

[157] Siehe dazu den Einleitungstext zur Umfrage im Anhang A4.7.
[158] Werbefilter werden häufig auch Adblocker – aus dem Englischen ad block – genannt.
[159] Beginnt man einen Chat in *WhatsApp*, dann steht dort, dass die „Nachrichten … in diesem Chat … mit Ende-zu-Ende-Verschlüsselung geschützt" sind. Es bleibt die Frage, ob die genannten 30 % diesen Sachverhalt oder einen anderen meinen.

den vorliegenden Daten errechnet sich ein Mittelwert von 24,6 %, sodass daraus eine mangelhafte Auswahl- und Nutzungskompetenz abgeleitet werden kann.

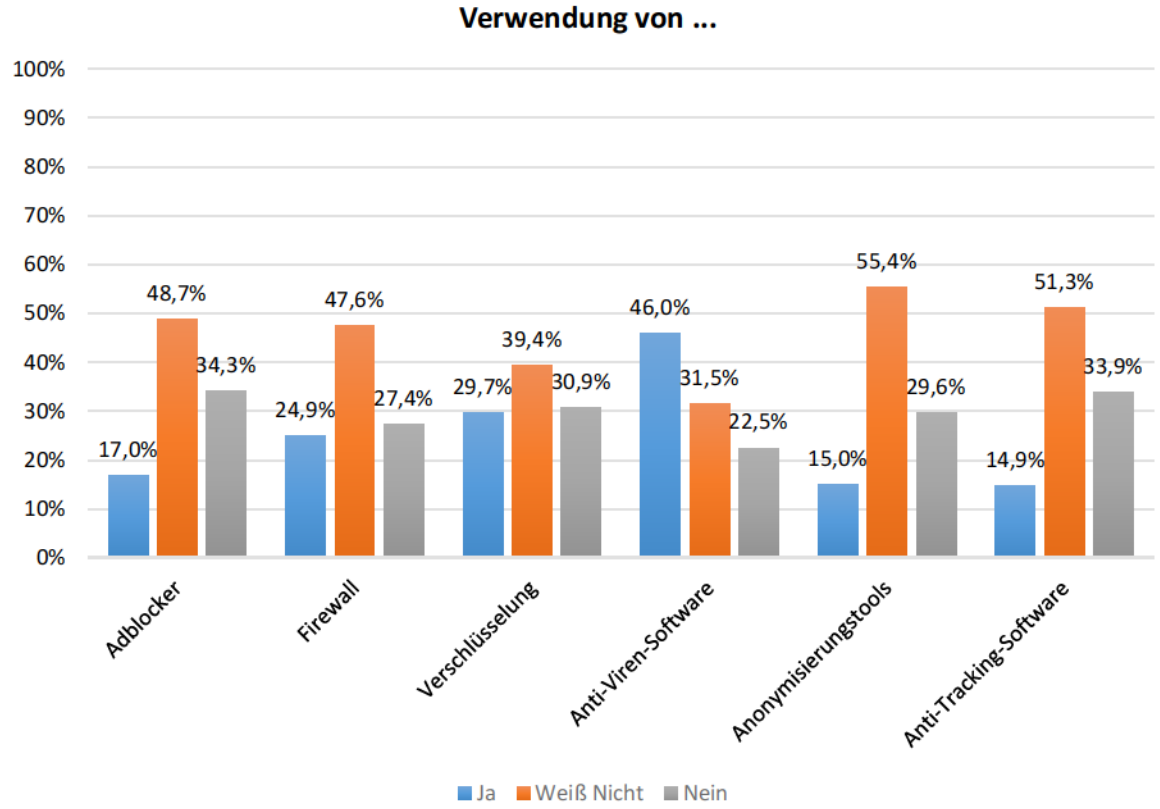


Abb. 4.7: Technische Maßnahmen zur sicheren Internetnutzung (Anhang Abb. A4.9-19)

Auf die Frage, ob die Befragten erst nach kostenlosen Alternativen im Web für die Musik schauen, bevor sie diese kaufen, kann mit 53,3 % als eine ausreichende Auswahl- und Nutzungskompetenz gesehen werden, wobei davon ausgegangen wird, dass es sich um legale Quellen für den Musikdownload handelt. Ob dies die Schüler auch so verstanden haben, kann nicht mit Sicherheit gesagt werden (Abb. A4.9-21).

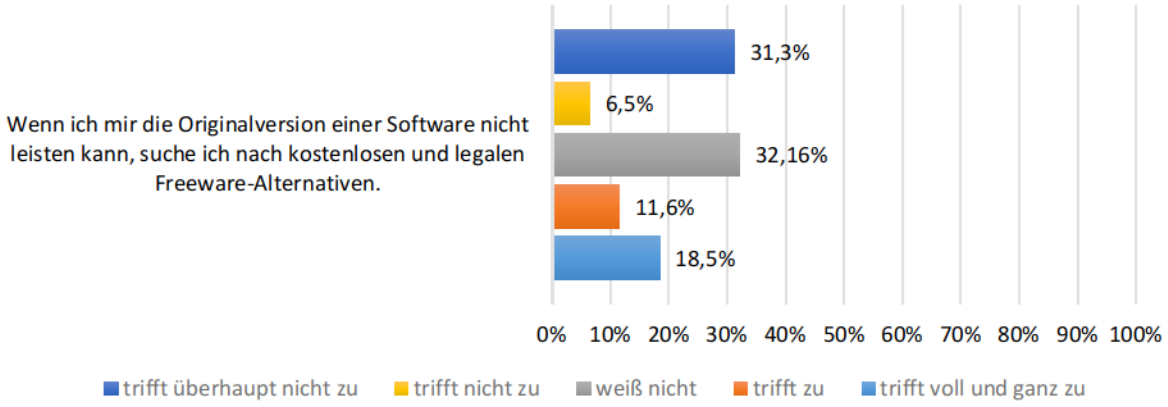


Abb. 4.8: Auswahl von Software-Alternativen (Anhang Abb. A4.9-22)

Anders liegt die Bewertung bei der Frage nach der Suche von kostenlosen und legalen Software-Alternativen, wenn die Originalversion einer Software zu teuer ist. Hier nutzen 30,1 % diese Option, was für eine mangelhafte Auswahl- und Nutzungskompetenz spricht (Abb. 4.8).

Zusammenfassend errechnet sich ein Durchschnittswert von 36,0 %, was einer mangelhaften Auswahl- und Nutzungskompetenz entspricht.

Dimension *Urteilskompetenz*:

Bei der Frage nach der Änderung von Privatsphäreeinstellungen in Sozialen Netzwerken nehmen 54% der Jugendlichen keine Änderungen in den Grundeinstellungen vor und vertrauen den Einstellungen der Anbieter. Ein Fünftel (20,1 %) der Schüler nimmt eine Änderung und rund ein Viertel (25,8 %) nimmt zwei oder mehr Änderungen vor (Abb. 4.9).

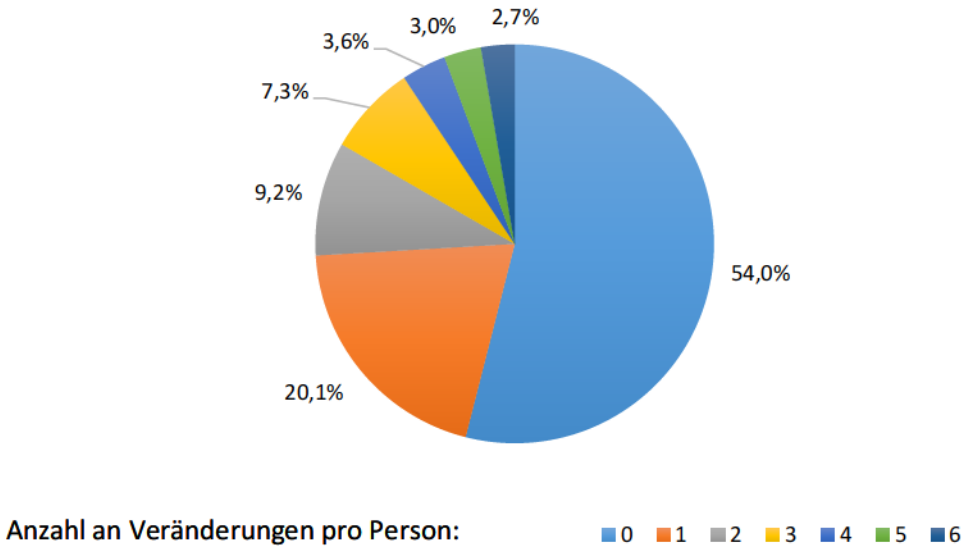


Abb. 4.9: Anzahl der Änderungen von Privatsphäreneinstellungen in Sozialen Netzwerken (Anhang Abb. A4.9-3)

Wegen des Vertrauens in den Anbieter wird laut Ankreuzverhalten nichts geändert. Die Gründe für das Nichtändern könnten aber auch andere wie Faulheit oder Unwissenheit sein. Die Änderungen betreffen vor allem die Möglichkeit der Einschränkung der Kontaktaufnahme und Auffindbarkeit zur eigenen Person und die Sichtbarkeit des eigenen Profils im Sozialen Netzwerk (jeweils ca. 20 %). Von rund 15 % wird die Sichtbarkeit eigener Posts und des eigenen Profils außerhalb des Sozialen Netzwerks eingeschränkt. Und 11,4 % begrenzen die Post-Möglichkeiten Anderer auf der eigenen Seite (Abb. A4.9-4). Dies lässt insgesamt auf eine mangelhafte Urteilskompetenz schließen.

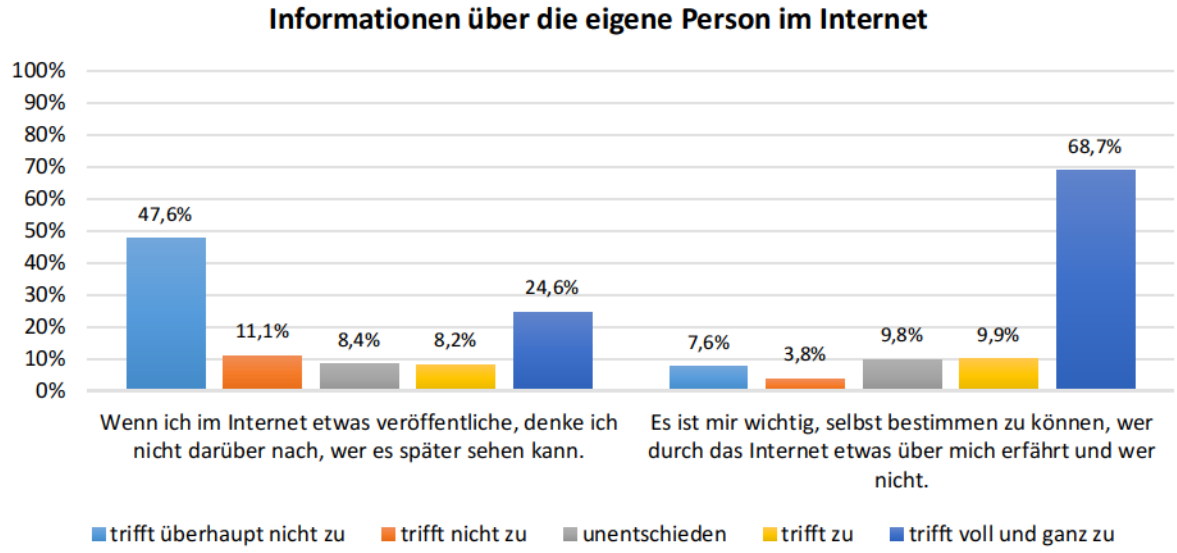


Abb. 4.10: Darstellung der eigenen Person im Internet (Anhang Abb. A4.9-5)

Von den Befragten denken 58,7 % darüber nach, wer gepostete Inhalte später sehen kann. Und 78,6 % der Befragten ist es wichtig, selber entscheiden zu können, wer durch das Internet etwas über einen erfährt oder auch nicht (Abb. 4.10). Mit einem Schnitt von 68,7 % spricht dies für eine befriedigende Urteilskompetenz.

Die Deaktivierung aktiver Inhalte im Browser als Maßnahme zur sicheren Internetgestaltung nutzen nur 14,9 % (Abb. A4.9-20). Da das Item von 61,9 % mit *weiß nicht* quittiert und damit nicht verstanden worden ist, ist die Urteilskompetenz hier nicht beurteilbar.

Auf die Frage, ob es schon mal vorkomme, dass reizvolle Werbebanner angeklickt werden, gaben 56,2 % an, hierbei vorsichtig zu sein und dies nicht zu tun. Dies spricht für eine ausreichende Urteilskompetenz (Abb. 4.11).

Insgesamt ergibt sich für diese Dimension ein Durchschnittswert von 59,9 %. Demzufolge ist die Urteilskompetenz ausreichend.

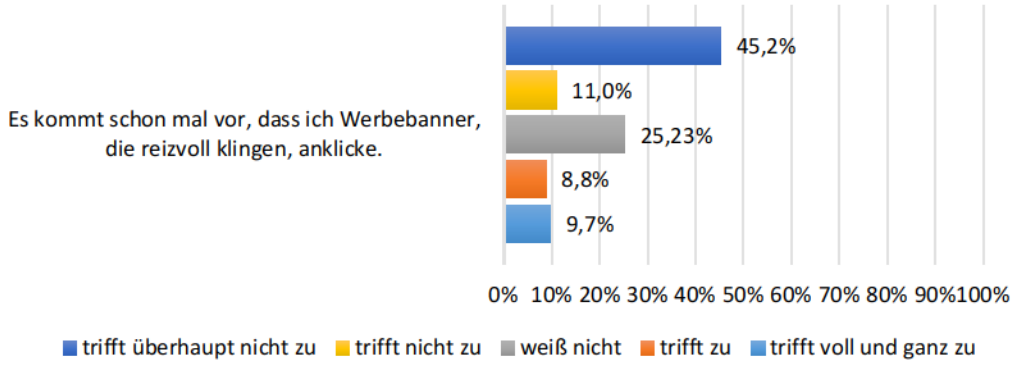


Abb. 4.11: Unkonzentriertes Anklicken reizvoller Werbebanner (Anhang Abb. A4.9-21)

Dimension *Handlungskompetenz*:

Rund 87,7 % der Befragten achten auf die Informationen, die sie selbst über sich ins Internet stellen (Abb. 4.12). Die Handlungskompetenz ist damit sehr gut.

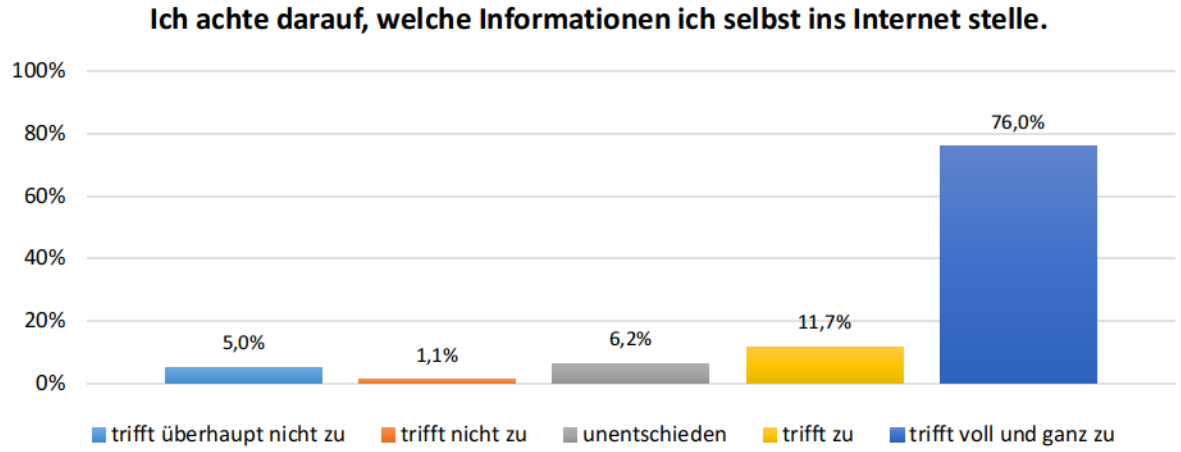


Abb. 4.12: Darstellung der eigenen Person im Internet (Anhang Abb. A4.9-5)

Innerhalb einer Frage wurden Maßnahmen zur sicheren Internetgestaltung abgefragt (Abb. 4.13). Die Nutzung sicherer Geräte mit Passwörtern (73,1 %), gefolgt von der Nutzung verschiedener Passwörter (57,6 %) und dem Besuch sicherer Seiten (54,4 %) werden von einer deutlichen Mehrheit der Jugendlichen angegeben. Mit der Tatsache, Sicherheitseinstellungen in Sozialen Netzwerken zu aktualisieren, können 51,1 % nichts anfangen; immerhin 34 % aktualisieren diese. Die Handlungskompetenz ist ausreichend ausgebildet.

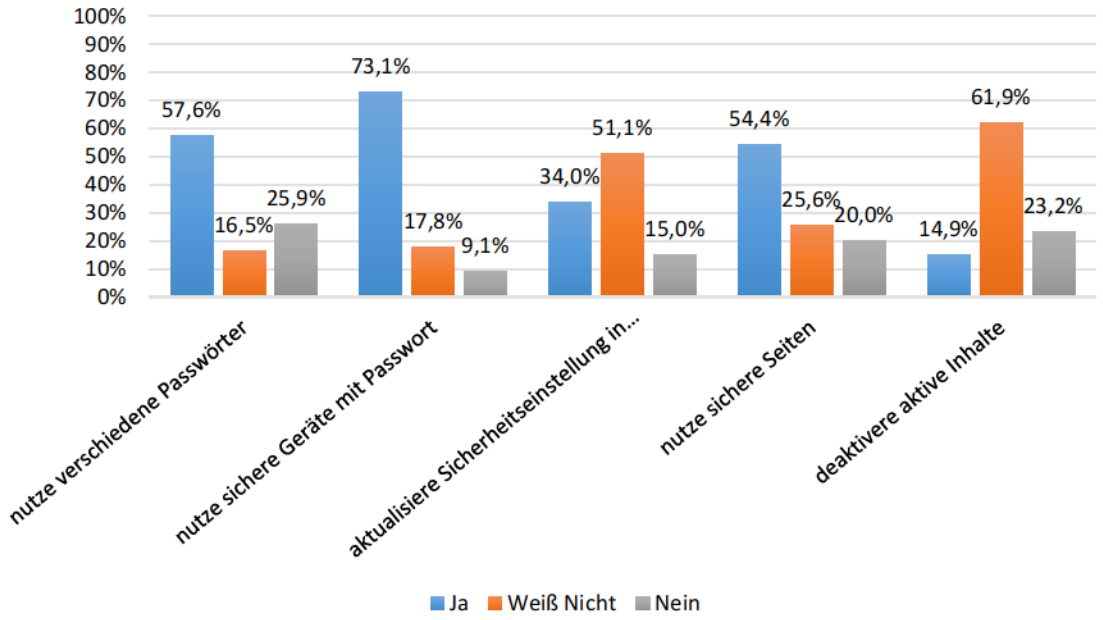


Abb. 4.13: Maßnahmen zur sicheren Internetnutzung (Anhang Abb. A4.9-20)

Vermuteter Spam wird von 59,1 % sofort gelöscht. Aber die Online-Zeit aufgrund von Sicherheitsrisiken einzuschränken, trifft nur für 35,8 % zu. Unter den Befragten bemühen sich 44,1 % ihre Software auf dem neuesten Stand zu halten. Jedoch ist die regelmäßige Änderung von Passwörtern nur für 25,1 % selbstverständlich. Ein geregelter Virenscan der Rechnerfestplatte wird von 40 % durchgeführt, aber nur 30,6 % sichern regelmäßig ihre Daten auf externe Datenträger (Abb. A4.9-22). Der Durchschnittswert dieser Frage ergibt einen Wert von 39,1 %.

Zusammengefasst ergibt sich über alle Fragen bei einem Durchschnittswert von 47,2 % eine mangelhafte Handlungskompetenz.

Beschreibung der nichtzugeordneten Items:

Das eindeutig (mit 89,6 %) bevorzugte Soziale Netzwerk[160] ist *YouTube*, gefolgt von *Snapchat* (45,3 %) und *Google+* (45,7 %), wobei es durchaus sein kann, dass das Pluszeichen an dem Wort *Google* überlesen worden ist und die Suchmaschine fälschlicherweise als Soziales Netzwerk angesehen worden ist. Mit 35,3 % spielt *Instagram* noch eine kleine Rolle, während alle anderen Netzwerke weit abgeschlagen sind. Bemerkenswert ist, dass von den Favorisierten nur Google+ als ein Soziales Netzwerk gilt. Gerade YouTube als eine Videoplattform und Snapchat als ein Instant-Messaging-System entsprechen nicht den Vorstellungen eines solchen (Abb. A4.9-1).

[160] Zur Auswahl von Internetplattformen als Soziale Netzwerke siehe Anhang A4.17.

Die Frage nach der Kenntnis von Browsern ergab, dass *Google Chrome* (82,4 %) und *Mozilla Firefox* (64,7 %) die Bekanntesten sind (Abb. A4.9-8).[161] Mit 42,4 % spielen *Microsoft Internet Explorer* bzw. *Edge* und mit 39,2 % *Apple Safari* noch eine Rolle. Die Nutzung keines Browsers (ein hoher Anteil von 6,5 %) verwundert und lässt vermuten, dass entweder der Begriff *Browser* nicht bekannt ist, die Schüler ihn aber trotzdem nutzen, oder dass sie einen Browser zwar nutzen, ohne aber zu wissen, dass sie einen Browser verwenden, oder dass sie tatsächlich keinen nutzen, weil sie noch nie im Internet gesurft haben. Da den Schülern jedoch recht viele Browser bekannt sind (72,2 % der Jugendlichen kennen bis zu drei unterschiedliche Produkte), können sie gut ausweichen (Abb. A4.9-9). Mit 64,1 % wird von den Schülern bevorzugt *Google Chrome* und mit 35,7 % *Mozilla Firefox* genutzt; *Apple Safari* wird von 27,6 % verwendet, sodass davon ausgegangen werden kann, dass dies dem Anteil der Nutzer von *Apple*-Produkten entspricht (Abb. A4.9-10).[162]

Die Frage nach der Kenntnis von Browsertools ergab, dass 82,7 % der Schüler keine Tools kennen, um ihren Browser sicherer zu gestalten. Ein Werbeblocker (*AdBlock Plus* 10,6 %) und *Firebug* (6,2 %) sind noch die am meisten gekannten Werkzeuge (Abb. A4.9-11). Von den Befragten, die Browsertools kennen, setzen 37,4 % keine ein. Vielleicht vertrauen die Jugendlichen den Grundeinstellungen des Browsers (z. B. durch den Anbieter), aber weder durch die Umfrage noch durch eine andere Studie können solche Rückschlüsse gezogen werden. Unter den eingesetzten Produkten nehmen *AdBlock Plus* einen Anteil von 29,9 %, *Firebug* einen Anteil von 11,7 %, *NoScript* einen Anteil von 9,3 % und *Ghostery* einen Anteil von 4,7 % ein; die anderen Tools haben keinen nennenswerten Anteil (Abb. A4.9-13).

Zusammenfassung:

Im gesamten Wissensbereich kann eine mangelhafte Leistung identifiziert werden. Während in einigen Dingen die Befragten schon eine ordentliche Risikobewertungskompetenz aufzeigen, besteht in anderen Fällen noch ein Nachholbedarf, sodass insgesamt nur von einer ausreichenden Risikobewertungskompetenz ausgegangen werden kann. Die Auswahl- und Nutzungskompetenz kann als mangelhaft bezeichnet werden. Die Zahlen zeigen eine ausreichende Urteilskompetenz, jedoch zeichnet sich wiederum nur eine mangelhafte Handlungskompetenz ab.

Auffällig ist bei diesen Zahlen, dass die Risikobewertungskompetenz und die Urteilskompetenz mit ausreichend (im Vergleich zu den anderen Dimensionen mit mangelhaft) abschneiden. Dies deckt sich mit den existierenden Studien. Wie schon in 2.3.2 geschrieben, werden die

[161] Eine Recherche nach Daten über die Verwendung unterschiedlicher Browser blieb insoweit erfolglos, als dass ausschließlich Daten zu den Marktanteilen der führenden Browserfamilien an der Internetnutzung in Deutschland gefunden wurden (vgl. https://de.statista.com/statistik/daten/studie/13007/umfrage/marktanteile-der-browser-bei-der-internetnutzung-in-deutschland-seit-2009/; Stand: 16.01.19). Demnach kommt *Google Chrome* auf 42 %, *Mozilla Firefox* auf 29 %, *Microsoft Internet Explorer* auf 10 %, *Apple Safari* und *Microsoft Edge* jeweils auf 7 % und *Opera* auf 4 %.

[162] Bei dieser Frage war eine Mehrfachauswahl möglich.

Chancen und Risiken der Internetnutzung wahrgenommen, was aber nicht zu einer Verstärkung der Sicherheitsanforderungen führt. Den Jugendlichen fehlen der fachliche Hintergrund und das Verständnis.

4.3.3.2. Bivariate Analyse

Ein weiterer zu betrachtender Aspekt ist, ob und gegebenenfalls wie die Dimensionen des Datenschutzkompetenzmodells zueinander in Beziehung stehen. Dazu werden die Korrelationen zwischen den einzelnen Dimensionen betrachtet, denn sie beschreiben die statistische Abhängigkeit zwischen einzelnen Größen (hier: den Dimensionen) (vgl. (Kuß et al. 2018, S. 238), (Wirtz und Nachtigall 2012, S. 102)).

Bei der Auswertung ist jedoch zu bedenken, dass „eine einzelne Korrelation, die lediglich den Zusammenhang zwischen zwei Variablen zum Ausdruck bringt, … ungeeignet [ist], um dieses Beziehungsgeflecht[163] vollständig abzubilden“ (Sedlmeier und Renkewitz 2013, S. 213).

Die Beschreibung zur Berechnung der Dimensionsmittelwerte befindet sich in Anhang A4.8. Diese Werte wurden jeweils gegeneinander aufgetragen. Ferner wurden die Mittelwerte von Risikobewertungskompetenz, Auswahl- und Nutzungskompetenz, Urteilskompetenz und Handlungskompetenz abschließend (und ausschließlich für diese Betrachtung) als (neue Variable) Datenschutzkompetenz (DK) zusammengefasst und als solche zur Dimension *Wissen* in Beziehung gesetzt. Die graphische Auswertung der bivariaten Analyse befindet sich in Anhang A4.11.

Bei der Betrachtung der Regressionsgeraden in den Diagrammen fällt auf, dass in allen Fällen eine steigende oder fallende Gerade identifiziert werden kann, wobei die Stärke der Steigung recht unterschiedlich ist. Während beispielsweise im Fall *Risikobewertungskompetenz* und *Wissen* kaum ein Zusammenhang abgelesen werden kann, ist im Fall von *Handlungskompetenz* und *Wissen* ein solcher erkennbar. Um die Beziehungen zwischen den Dimensionen des Modells besser beschreiben zu können, werden die Korrelationskoeffizienten r mit Hilfe der Software *IBM SPSS Statistics 24* berechnet:

[163] Die Mehrheit an Variablen einer Untersuchung stehen in einem wechselseitigen Verhältnis zu vielen anderen Variablen und bilden damit ein Beziehungsgeflecht.

		W	RK	ANK	UK	HK	DK
W	Korrelation nach Pearson	1	,009	,168**	,154**	,254**	,266**
	Signifikanz (2-seitig)		,765	,000	,000	,000	,000
	N	996	996	996	996	996	996
RK	Korrelation nach Pearson	,009	1	-,111**	,238**	,088**	,454**
	Signifikanz (2-seitig)	,765		,000	,000	,006	,000
	N	996	996	996	996	996	996
ANK	Korrelation nach Pearson	,168**	-,111**	1	-,072*	,333**	,546**
	Signifikanz (2-seitig)	,000	,000		,023	,000	,000
	N	996	996	996	996	996	996
UK	Korrelation nach Pearson	,154**	,238**	-,072*	1	,102**	,610**
	Signifikanz (2-seitig)	,000	,000	,023		,001	,000
	N	996	996	996	996	996	996
HK	Korrelation nach Pearson	,254**	,088**	,333**	,102**	1	,644**
	Signifikanz (2-seitig)	,000	,006	,000	,001		,000
	N	996	996	996	996	996	996
DK	Korrelation nach Pearson	,266**	,454**	,546**	,610**	,644**	1
	Signifikanz (2-seitig)	,000	,000	,000	,000	,000	
	N	996	996	996	996	996	996

**. Die Korrelation ist auf dem Niveau[164] von 0,01 (2-seitig) signifikant.
*. Die Korrelation ist auf dem Niveau von 0,05 (2-seitig) signifikant.

Tab. 4.8: Korrelationen zwischen den jeweiligen Dimensionen[165]

Um die Stärke eines Zusammenhangs zu beurteilten, wurde von Cohen auf der Grundlage des Effektstärkemaßes r, das dem Korrelationskoeffizienten entspricht, folgende Vereinbarung getroffen:

$|r| \approx .1$ schwacher Effekt
$|r| \approx .3$ mittlerer Effekt
$|r| \approx .5$ starker Effekt

(vgl. (Döring und Bortz 2016, S. 820), (Wirtz und Nachtigall 2012, S. 107)).

Die Auswertung zeigt, dass in allen Fällen eine schwache bis mittlere Korrelation zwischen den einzelnen Dimensionen existiert. Nur im Fall des Paars *Risikobewertungskompetenz* und *Wissen* liegt keine Korrelation vor. Das Signifikanzniveau beträgt $p < .01$ mit Ausnahme des Paars *Auswahl- und Nutzungskompetenz* und *Urteilskompetenz* ($p < .05$). Daraus lassen sich folgende Aussagen schließen:

- Je höher das *Wissen*, desto höher ist die *Auswahl- und Nutzungskompetenz* und umgekehrt (schwacher bis mittlerer Effekt).

[164] Signifikanzniveau ist die Irrtumswahrscheinlichkeit.
[165] Zu den Abkürzungen der Dimensionen siehe Abschnitt 3.4. Positive Korrelationen sind grün, negative Korrelationen gelb und keine Korrelation rot markiert; die grau unterlegten Zahlen haben keine Bedeutung.

- Je höher das *Wissen*, desto höher ist die *Urteilskompetenz* und umgekehrt (schwacher bis mittlerer Effekt).
- Je höher das *Wissen*, desto höher ist die *Handlungskompetenz* und umgekehrt (mittlerer Effekt).
- Je höher die *Risikobewertungskompetenz*, desto niedriger ist die *Auswahl- und Nutzungskompetenz* und umgekehrt (schwacher Effekt).
- Je höher die *Risikobewertungskompetenz*, desto höher ist die *Urteilskompetenz* und umgekehrt (schwacher bis mittlerer Effekt).
- Je höher die *Risikobewertungskompetenz*, desto höher ist die *Handlungskompetenz* und umgekehrt (schwacher Effekt).
- Je höher die *Auswahl- und Nutzungskompetenz*, desto niedriger ist die *Urteilskompetenz* und umgekehrt (schwacher Effekt).
- Je höher die *Auswahl- und Nutzungskompetenz*, desto höher ist die *Handlungskompetenz* und umgekehrt (mittlerer Effekt).
- Je höher die *Urteilskompetenz*, desto höher ist die *Handlungskompetenz* und umgekehrt (schwacher Effekt).
- Zwischen den Dimensionen *Wissen* und *Risikobewertungskompetenz* konnte keine signifikante Korrelation festgestellt werden.

Zwischen der neuen Variablen *Datenschutzkompetenz* und *Wissen* wurde ein mittlerer Zusammenhang festgestellt ($r = .27$, $p < .01$). Somit geht einem höheren *Wissen* auch eine höhere *Datenschutzkompetenz* einher und umgekehrt. Dies spricht für die Annahme, dass Wissen ein entscheidender Bestandteil zur Stärkung der anderen Dimensionen ist.

Der höchste Korrelationskoeffizient zwischen den Dimensionen des Modells ($r = .33$) ist bei dem Paar *Auswahl- und Nutzungskompetenz* und *Handlungskompetenz* zu beobachten. Dieser Zusammenhang ist aufgrund der Nähe von Nutzung und Handlung im Alltag augenscheinlich nachvollziehbar.

4.3.3.3. Differenzierte deskriptive Auswertung

Um ein detaillierteres Kompetenzbild der Probandengruppe zu erhalten, werden Gruppen nach folgenden Überlegungen gebildet. Anhand von drei Merkmalen können die Teilnehmer differenziert werden: Geschlecht, Alter und Schulform. Die Geschlechterverteilung ist annähernd 50 % : 50 %. Bildet man für die Altersklassen die beiden Gruppen *<= 11 Jahre* und *>= 12 Jahre*, so erhält man eine Altersverteilung von 53,5 % : 46,5 %, was annähernd ebenfalls als eine Gleichverteilung betrachtet werden kann. Die dritte Option, eine Unterteilung nach der Schulform, ergibt keinen Sinn, da 75 % der Befragten das Gymnasium, aber nur 15 % die Realschule Plus und nur 10 % die IGS besuchen und somit keine Gleichverteilung vorliegt. Ferner spricht für den Wegfall der Schulform, dass die Schüler in den Klassenstufen 5 und 6, der so-

genannten Orientierungsstufe, durch die schulformunabhängigen Lehrpläne nicht schulformspezifisch differenziert unterrichtet werden, sodass die Schulform keinen (großen) Einfluss auf die Umfrage haben sollte. Somit ergeben sich letztendlich vier Probandengruppen.[166]

Gruppe	Merkmal
I	Jungen bis 11 Jahre
II	Jungen ab 12 Jahre
III	Mädchen bis 11 Jahre
IV	Mädchen ab 12 Jahre

Tab. 4.9: Klasseneinteilung der Probanden

Vor der weiteren Bearbeitung wurden insgesamt noch weitere 28 Datensätze herausgelöscht, da diese bei exakter Betrachtung den Eindruck hinterließen, den Fragebogen nicht mit der notwendigen Ernsthaftigkeit ausgefüllt zu haben. Dies war im Vorfeld bei der Gesamtgruppenerhebung noch nicht aufgefallen.

Ferner wird für die detaillierte deskriptive Auswertung nur noch auf eine begrenzte Anzahl an Items zurückgegriffen. Zwei entscheidende Kriterien für die Itemauswahl sind, dass jede Dimension des Datenschutzkompetenzmodells vertreten und dass das jeweilige Item von der Gesamtmenge der Schüler beantwortet worden ist.[167] Der Bereich *Wissen* wird wie in der ersten Auswertung additiv betrachtet, sodass hier zwei "Items" einfließen. Die Risikobewertungskompetenz fließt mit acht Items, die Auswahl- und Nutzungskompetenz mit vier Items, die Urteilskompetenz mit drei Items und die Handlungskompetenz wieder mit vier Items ein. Dies macht in der Summe 21 Items. Da ein Frageblock zu der Risikobewertungskompetenz sieben Items umfasst und ganz klar auf die Risikoeinschätzung abzielt, ist diese Dimension, wie im Fragebogen insgesamt auch, stärker vertreten.

[166] Bei Hinzunahme der Schulform wären es insgesamt zwölf Gruppen geworden, worunter zudem die Übersichtlichkeit gelitten hätte.

[167] Wenn z. B. mehr als 60 % der Befragten mit *weiß nicht* geantwortet haben, dann ist das Item ungeeignet.

Die folgende Tabelle listet die ausgewählten Items auf:

Code[168]	Item	Dimension
C1	Was versteht man unter einem "Trojaner"? Ein Trojaner ist ein Computerprogramm, das ...	W
C2	Was ist ein "Cookie"? Ein Cookie ist ...	W
C3	Was ist eine "Firewall"? Eine Firewall ist ...	W
C4	Was verbirgt sich hinter dem Begriff "Browserverlauf"? Im Browserverlauf werden ...	W
C5	Welche der folgenden URLs garantiert einen mit hoher Wahrscheinlichkeit datenabhörsicheren Zugriff auf die Webseite?	W
E1b	Sind folgende Aussagen wahr oder falsch? [Man muss Deine Erlaubnis einholen, wenn man ein Foto oder Video von dir hochlädt, auf dem Du klar zu erkennen bist.]	W
E1d	Sind folgende Aussagen wahr oder falsch? [Wenn eine Firma dein Internetverhalten über mehrere Seiten verfolgen möchte, muss sie zuerst dein Einverständnis einholen.]	W
E1e	Sind folgende Aussagen wahr oder falsch? [Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.]	W
E2b	Sind folgende Aussagen wahr oder falsch? [Betreiber Sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar nicht nutzen.]	W
E2c	Sind folgende Aussagen wahr oder falsch? [Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.]	W
E2d	Sind folgende Aussagen wahr oder falsch? [Durch das Surfen im „Private Browsing“-Modus kann die Rekonstruktion des eigenen Surfverhaltens erschwert werden, da keine Browserinformationen gespeichert werden.]	W
E2e	Sind folgende Aussagen wahr oder falsch? [Online-Shops (z.B. Amazon) werten das Nutzungsverhalten von Kunden aus und erstellen auf dieser Basis Kaufempfehlungen oder entsprechend zugeschnittene Werbung.]	W
A2	Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken nicht zu veröffentlichen? ...	RK
F1a	Was sind für dich Risiken im Internet? [Die unerwünschte Weitergabe von persönlichen Daten in Dritte]	RK

Tab. 4.10a: Itemauswahl für die differenzierte deskriptive Auswertung

[168] Der Code entspricht den Fragen im finalen Fragebogen der Studie (vgl. Anhang A4.7).

Code	Item	Dimension
F1b	Was sind für dich Risiken im Internet? [Das Ausspionieren meiner persönlichen Daten]	RK
F1c	Was sind für dich Risiken im Internet? [Der Empfang von Spam-Mails]	RK
F1d	Was sind für dich Risiken im Internet? [Die Beleidigungen und Belästigungen im Internet]	RK
F1e	Was sind für dich Risiken im Internet? [Das Versenden unerwünschter E-Mails in meinem Namen]	RK
F1f	Was sind für dich Risiken im Internet? [Andere wissen, was ich mache, oder kennen meinen Aufenthaltsort]	RK
F1g	Was sind für dich Risiken im Internet? [Die Veröffentlichung peinlicher/intimer Chats/Fotos/...]	RK
G1a	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze Pop-Up- Blocker oder Adblocker.]	ANK
G1b	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze eine Firewall.]	ANK
G1c	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze eine Verschlüsselungssoftware beim E-Mailen und Chatten.]	ANK
G1d	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [...aktualisiere regelmäßig meine Anti-Viren-Software.]	ANK
B1/B2	Hast Du die Privatsphäreeinstellungen in <Name>[169] geändert? Wenn ja, was? [Ich habe nichts geändert, weil ich den Einstellungen des Anbieters vertraue / Sichtbarkeit meines Profils ...]	UK
B3c	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Es ist mir wichtig, selbst bestimmen zu können, wer durch das Internet etwas über mich erfährt und wer nicht.]	UK
H1d	Wie sehr treffen die folgenden Aussagen auf dich zu? [Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.]	UK
B3a	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Ich achte darauf, welche Informationen ich selbst ins Internet stelle.]	HK
H1i	Wie sehr treffen die folgenden Aussagen auf dich zu? [E-Mails, bei denen ich die Vermutung habe, dass es sich um unerwünschte Nachrichten (Spam) handelt, lösche ich sofort.]	HK
H1j	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich ändere in regelmäßigen Abständen alle meine Passwörter.]	HK
H1k	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.]	HK

Tab. 4.10b: Itemauswahl für die differenzierte deskriptive Auswertung

[169] An dieser Stelle wird der Name des favorisierten Sozialen Netzwerks eingeblendet.

Die Auswertung dieser Daten und eine Beschreibung befindet sich im Anhang A4.10. Es folgt an dieser Stelle eine Zusammenfassung der Ergebnisse begleitet von ausgewählten Diagrammen und sortiert nach den Dimensionen des Modells. Die Gesamtbeurteilung der Kompetenz orientiert sich an der Skala in Tabelle 4.7. Die Berechnung des prozentualen Anteils ist im Anhang A4.8 beschrieben.

Dimension *Wissen*:

Die Gruppe der Wissensfragen ist in zwei Blöcke eingeteilt. Im ersten Block werden Fachbegriffe abgefragt, die über Multiple-Choice zu beantworten sind.[170] Hierbei ist je eine Aussage richtig, wobei *weiß nicht* als falsche Antwort gewertet wird. Am Ende wird die Summe der korrekten Antworten betrachtet.

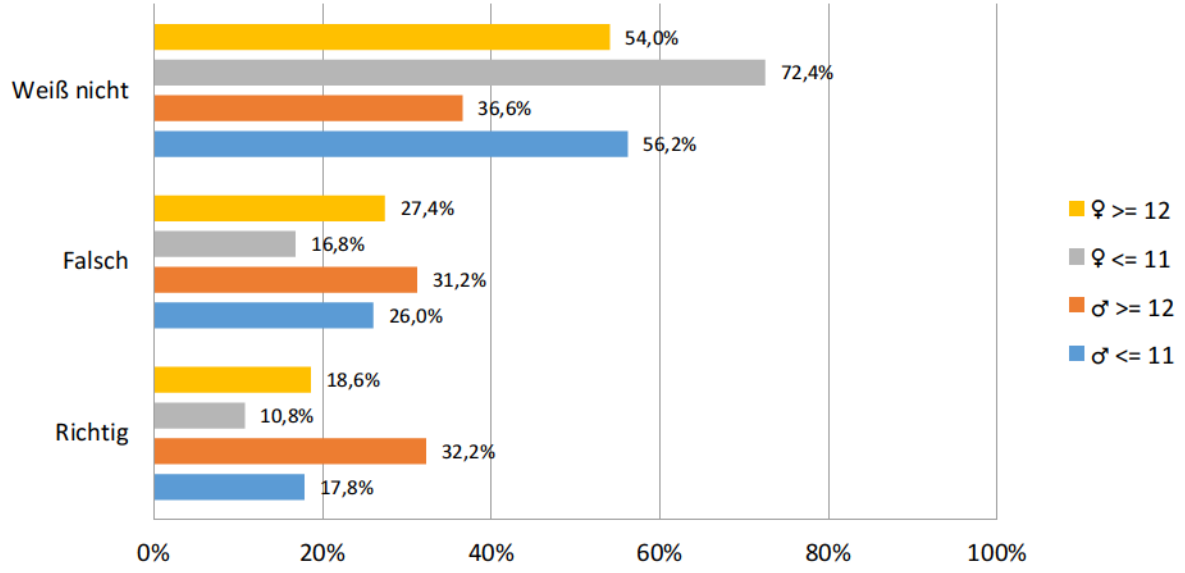


Abb. 4.14: Anteil aller abgegebenen Antworten im ersten Wissensteil (Anhang Abb. A4.10-20)

[170] Die Ratewahrscheinlichkeit für die jeweils korrekte Antwort der Multiple-Choice-Aufgaben beträgt 1/4 (unter der Annahme, dass *weiß nicht* nicht geraten wird).

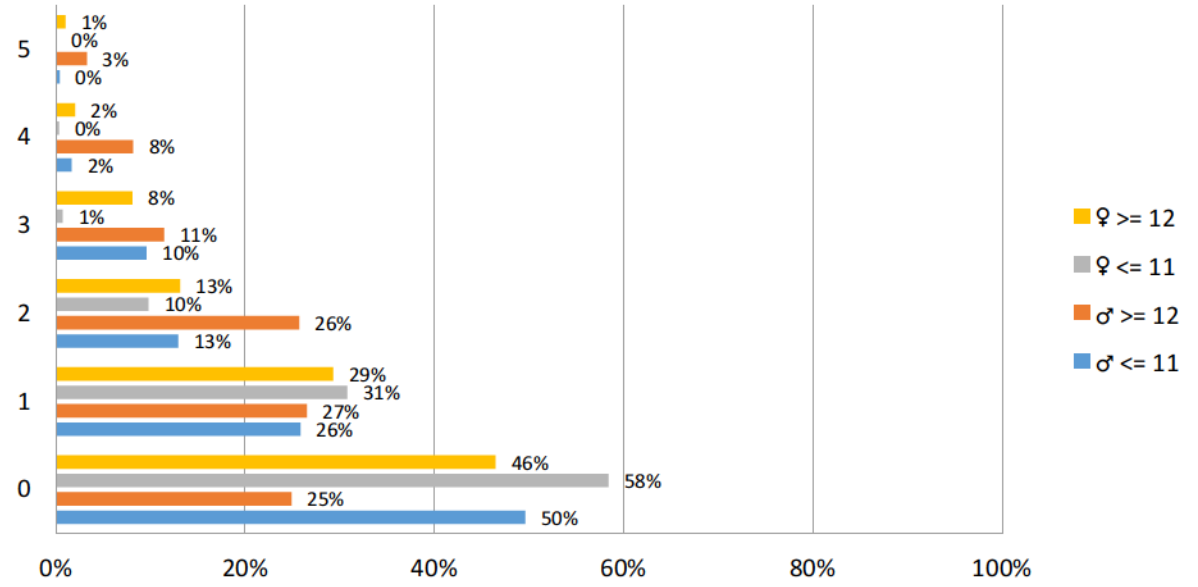


Abb. 4.15: Anzahl an richtigen Antworten im ersten Wissensteil (Anhang Abb. A4.10-21)

Im zweiten Block werden Aussagen um die Themen *Datenschutzerklärung*, *Urheberrecht*, *Tracking* und *Nutzung von Nutzerdaten durch Dritte* getroffen und die Probanden entscheiden, ob diese wahr oder falsch sind; als dritte Antwortoption steht *weiß nicht* zur Verfügung, welche als falsche Antwort gewertet wird. Am Ende wird die Anzahl der korrekten Antworten aufsummiert.

Die Berechnung des Anteils korrekter Antworten ergibt folgendes Bild:

Klasse	Block C	Block E	Summe	Note
Mädchen >= 12	18,6%	41,1%	29,9%	5
Mädchen <= 11	10,8%	31,4%	21,1%	5
Jungen >= 12	32,2%	43,3%	37,8%	5
Jungen <= 11	17,8%	36,6%	27,2%	5

Tab. 4.11: Bewertung der Dimension Wissen

Unabhängig von Alter und Geschlecht ist das Wissen in allen Gruppen als *mangelhaft* zu bezeichnen (Abb. 4.14 und 4.15). Beim Faktenwissen schneiden beide Geschlechter schlechter als im zweiten Frageblock E ab. Dies könnte damit zusammenhängen, dass die Jugendlichen von den in Block E geschilderten Fälle/Situationen schon einmal gehört haben und daher richtig antworten, während Fachbegriffe in der Regel erst im Fachunterricht (Informatik/ITG) vermittelt werden, der in den Schulen kaum stattfindet. Die Vorstellung, was sich z. B. hinter dem Begriff *Firewall* verbirgt, ist vage. Insgesamt sind die Jungen stärker als die Mädchen und die älteren Teilnehmer stärker als die jungen Probanden. Dies kann damit begründet werden, dass einerseits die Jungen aufgrund ihrer Interessenlage und der noch nicht ausreichenden Förde-

rung von Mädchen im MINT-Bereich das Interesse bei den Jungen für Informatik und informatische Fragestellungen größer ist und andererseits die älteren Befragten aufgrund ihrer Erfahrung im Umgang mit dem Netz und seinen Anwendungen den jüngeren überlegen sind. Trotzdem ist das Wissen insgesamt so schwach, dass dringender Handlungsbedarf in den Schulen besteht.

Dimension *Risikobewertungskompetenz*:

Zur Beurteilung der Risikobewertungskompetenz sind für die differentielle Auswertung zwei Frageblöcke der Studie übernommen worden. Im ersten Block A2 wird die persönliche Einschätzung zur Sensibilität veröffentlichter personenbezogener Daten in Sozialen Netzwerken abgefragt. Die Antworten lassen kein eindeutiges Bild oder keine eindeutige Tendenz in Bezug auf Alter oder Geschlecht erkennen. Je nach Item sind die Einschätzungen unterschiedlich. Ganz grob lässt sich aber erkennen, dass die Gruppe der Mädchen einerseits und die Gruppe der jüngeren Probanden andererseits bei der Angabe von persönlichen Daten eher zurückhaltender und vorsichtiger sind (Abb. 4.16 bis 4.19).

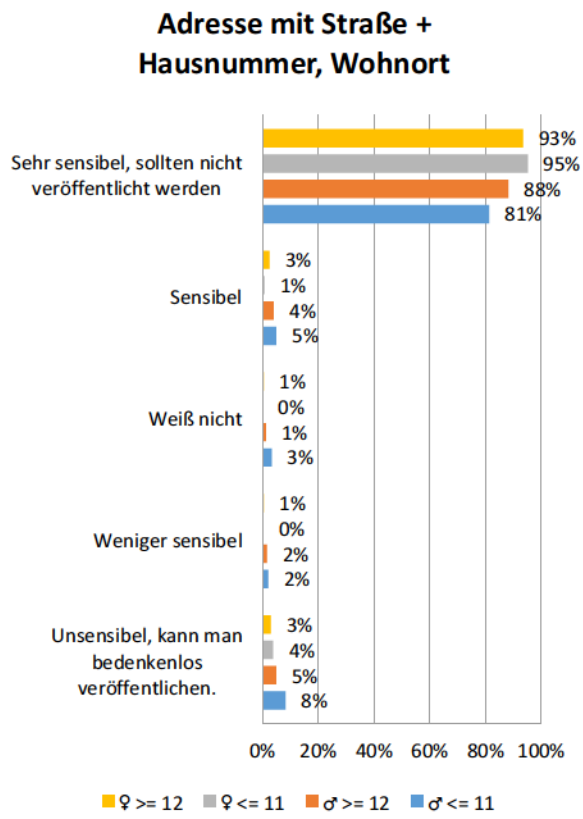


Abb. 4.16: Einschätzung der Sensibilität persönlicher Daten zur Veröffentlichung in Sozialen Netzwerken: Adresse (Anhang Abb. A4.10-5)

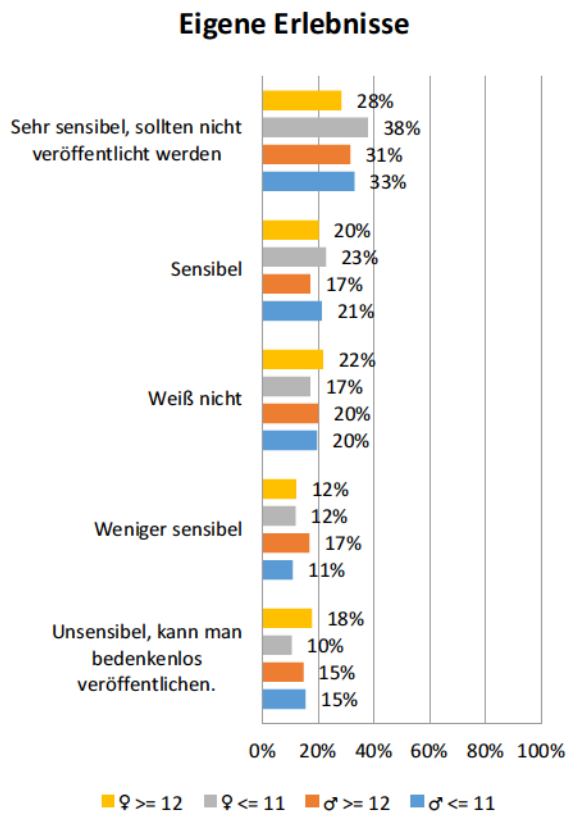


Abb. 4.17: Einschätzung der Sensibilität persönlicher Daten zur Veröffentlichung in Sozialen Netzwerken: Eigene Erlebnisse (Anhang Abb. A4.10-13)

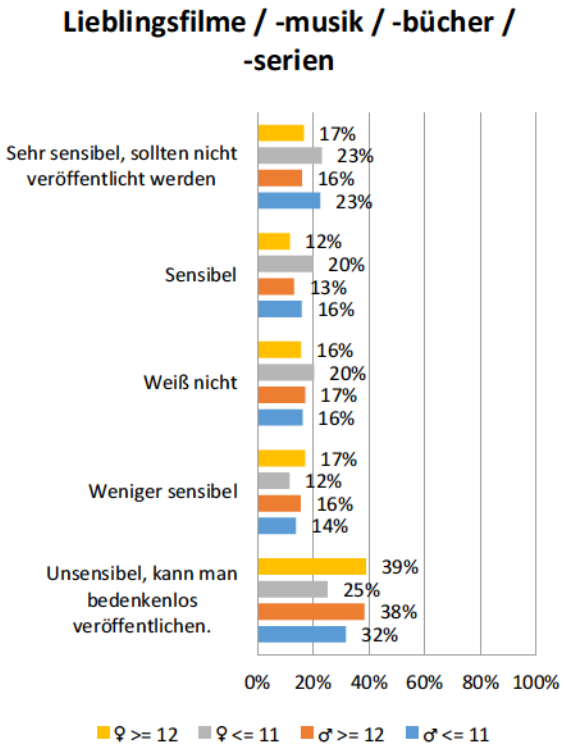


Abb. 4.18: Einschätzung der Sensibilität persönlicher Daten zur Veröffentlichung in Sozialen Netzwerken: Lieblingsfilme (Anhang Abb. A4.10-11)

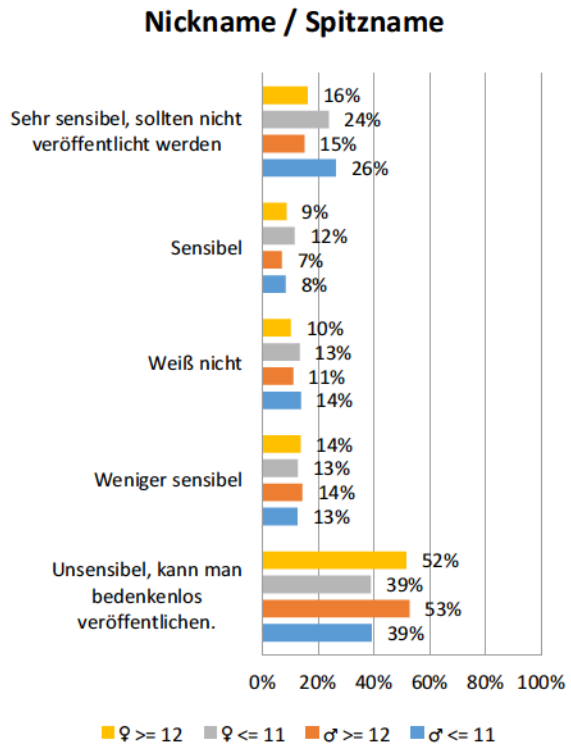


Abb. 4.19: Einschätzung der Sensibilität persönlicher Daten zur Veröffentlichung in Sozialen Netzwerken: Nickname (Anhang Abb. A4.10-3)

Im zweiten Block F1 geht es um die Einschätzung diverser Risiken für personenbezogene Daten im Rahmen der Internetnutzung.[171] Man kann beobachten, dass die jüngeren Mädchen diejenigen sind, die das Risiko eher hoch einschätzen. Dem folgen mit einem kleinen Abstand die jüngeren Jungen, die wiederum teilweise dicht auf mit den älteren Jungen liegen. Die älteren Mädchen schätzen die Situationen teilweise weniger riskant ein. Dies kann durchaus daran liegen, dass hierbei die Erfahrung in der Internet- und Computernutzung eine Rolle spielt. Ein Mensch, der sehr viel Zeit im Netz verbringt und von unterschiedlichen Vorfällen gehört oder gar selbst erlebt hat, wird die vorgegebenen Situationen anders als ein Unerfahrener einschätzen (Abb. 4.20 und 4.21).

[171] Die Fälle waren: *Veröffentlichung peinlicher Fotos, den eigenen Aufenthaltsort frei geben, Versand unerwünschter E-Mails im Namen des Schülers, Beleidigung und Belästigung im Web, Empfang von Spam-Mails, Ausspionieren persönlicher Daten* und *unerwünschte Weitergabe persönlicher Daten an Dritte*.

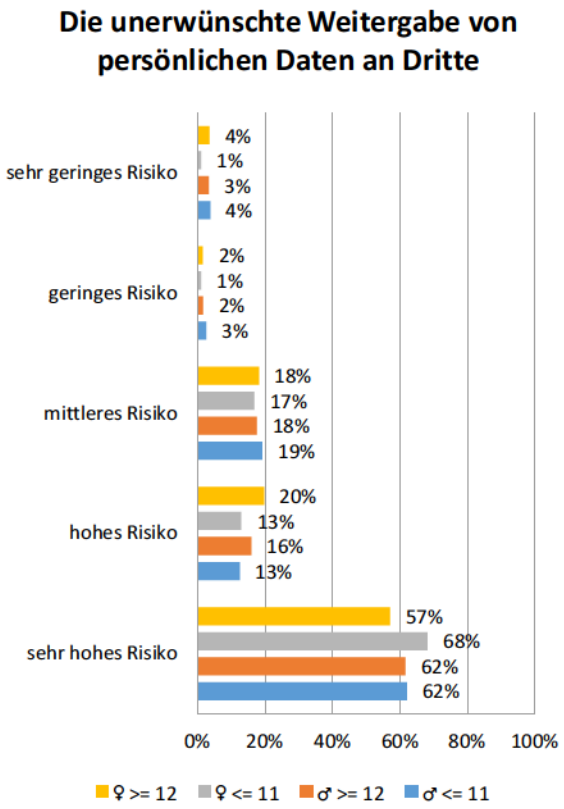


Abb. 4.20: Einschätzung von Internetrisiken (Anhang Abb. A4.10-24)

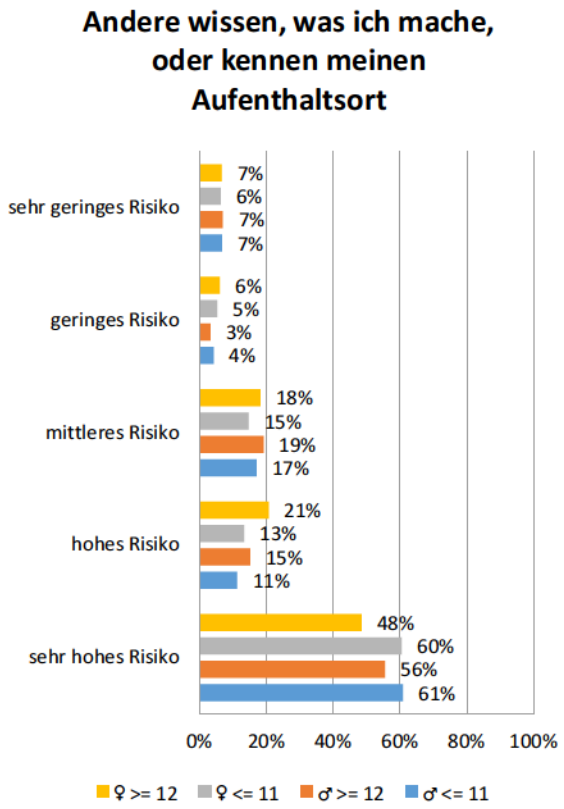


Abb. 4.21: Einschätzung von Internetrisiken (Anhang Abb. A4.10-29)

Die Berechnung der Einschätzungen ergibt folgendes Bild:

Klasse	Block A2	Block F1	Summe	Note
Mädchen >= 12	63,1%	61,0%	62,4%	4
Mädchen <= 11	70,3%	70,6%	70,4%	3
Jungen >= 12	63,2%	62,8%	63,0%	4
Jungen <= 11	68,0%	67,1%	67,7%	3

Tab. 4.12: Bewertung der Dimension Risikobewertungskompetenz

Bei den Einschätzungen liegt bei allen Beteiligten die Risikobewertungskompetenz wenigstens im ausreichenden Bereich. Da die jüngeren Teilnehmer eher die Risiken erkennen, dürften sie tendenziell auch noch vorsichtiger und sorgsamer im Umgang mit persönlichen Daten sein, sodass ihnen nach den errechneten Zahlen in diesem Bereich ein befriedigend zugewiesen werden kann. Dieses vorsichtige Verhalten kann einerseits aus den Ratschlägen Anderer folgen oder aber auch aus dem in diesem Alter doch eher vorsichtigen Verhalten erwachsen. Ältere Jugendliche sind aufgrund ihrer Entwicklung auch eher bereit Risiken zu übersehen oder einzugehen, um ein Ziel zu erreichen.

Dimension *Auswahl- und Nutzungskompetenz*:

Zur Untersuchung dieser Dimension stehen technischen Maßnahmen zur sicheren Internetgestaltung im Vordergrund. Dazu wurde der Einsatz von Werbefilter, Firewall, Verschlüsselungssoftware und Anti-Viren-Software erfragt (Abb. 4.22 und 4.23).

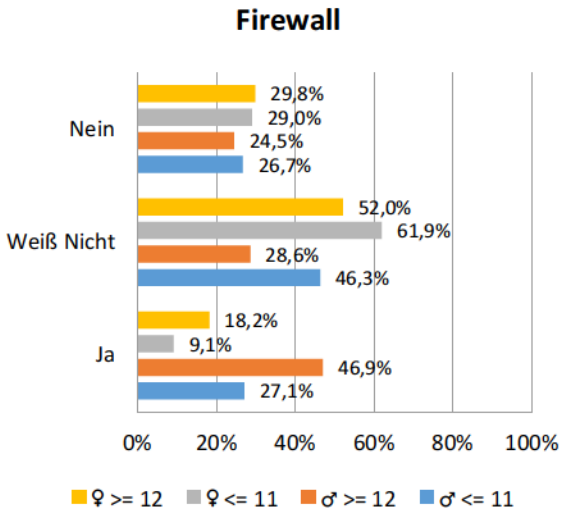


Abb. 4.22: Technische Maßnahmen zur sicheren Internetnutzung: Firewall (Anhang Abb. A4.10-32)

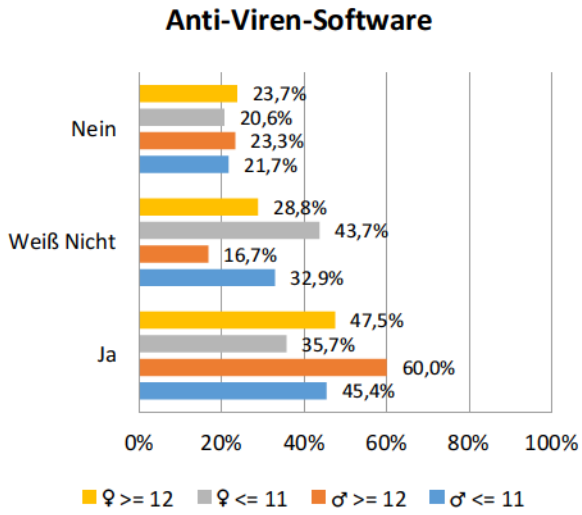


Abb. 4.23: Technische Maßnahmen zur sicheren Internetnutzung: Anti-Viren-Software (Anhang Abb. A4.10-34)

Unabhängig von Geschlecht und Alter wird ein Werbefilter von im Schnitt 17 % genutzt, gefolgt von der Firewall (26 %), der Verschlüsselungssoftware (30 %) und der Anti-Viren-Software mit 47 %. Da eine Firewall zur Grundeinstellung beim Internetsurfen gehört, überrascht es, dass nur so wenige diese nutzen. Vermutlich ist diese systembedingt eingeschaltet und die Jugendlichen kennen sie nicht (was zu dem Ergebnis der Antwort auf die Funktion einer Firewall aus der Dimension *Wissen* passt). Verwunderlich ist dafür der hohe Anteil an Schülern, die eine Verschlüsselungssoftware nutzen. Da die Frage sowohl das Mailen als auch das Chatten erfasst, kann davon ausgegangen werden, dass die Jugendlichen das Chatten vor Augen haben[172], da das Mailen in dieser Altersgruppe keine Bedeutung hat. Ob dem aber so ist, kann nicht geklärt werden. Weniger überraschend ist, dass eine Anti-Viren-Software von vielen genutzt wird, denn der Begriff ist den Schülern bekannt, jedoch ist der Anteil der Nutzer viel zu gering.

Betrachtet man die Nutzung des Werbefilters und der Firewall, so sind es vorzugsweise die älteren Jungen, gefolgt von den jüngeren Jungen, gefolgt von den älteren Mädchen und den jüngeren Mädchen, die diese Werkzeuge nutzen. Dieses Bild könnte an der stärkeren Affinität

[172] Beginnt man einen Chat in *WhatsApp*, dann steht dort, dass die „Nachrichten … in diesem Chat … mit Ende-zu-Ende-Verschlüsselung geschützt“ sind.

der Jungen zu diesem Thema liegen. Die Verschlüsselungssoftware wird überraschenderweise von den älteren Mädchen, gefolgt von den Jungen genutzt. Eine begründete Vermutung kann nicht abgeleitet werden. Bei der Anti-Viren-Software sind es vorzugsweise die älteren Teilnehmer (Jungen 60 %, Mädchen 48 %), die eine solche nutzen. Den jüngeren Jungen mit 30 % folgen die jüngeren Mädchen mit 20 %.

Gerade weil es sich bei dieser Frage um technische Dinge handelt, lässt sich damit der höhere Anteil der Jungen gegenüber den Mädchen erklären. Die Ausnahme der Verschlüsselungssoftware könnte an Verständnisschwierigkeiten liegen[173], aber die Nicht-Nutzung könnte auch eine Faulheit der Jugendlichen sein. Der nicht unerhebliche Anteil der Befragten, die diesen Werkzeugen keine Bedeutung zuordnen konnten, fordert eine schulische Aufklärung über die technischen Zusammenhänge.

Die Berechnung der Anteile ergibt folgendes Ergebnis:

Klasse	Summe	Note
Mädchen >= 12	28,9%	5
Mädchen <= 11	19,7%	5
Jungen >= 12	41,0%	5
Jungen <= 11	30,1%	5

Tab. 4.13: Bewertung der Dimension Auswahl- und Nutzungskompetenz

Zusammenfassend errechnet sich für alle Gruppen ein Durchschnittswert unter 50 %, was einer mangelhaften Auswahl- und Nutzungskompetenz entspricht.

Dimension *Urteilskompetenz*:

Ein ausgewähltes Item beschäftigt sich mit der Frage nach der Anzahl der Änderungen in den Profileinstellungen Sozialer Netzwerke (Abb. 4.24). Sie werden bevorzugt von den Älteren – insbesondere von den Mädchen – vorgenommen, was damit begründet werden kann, dass sie die größere Erfahrung aufgrund ihres Alters besitzen und zudem die Mädchen eher auf die Veröffentlichung ihrer Daten achten. Umgekehrt könnte den Jüngeren das Wissen über die Art und Weise der Einstellungsänderungen fehlen. Da die Profileinstellungen auch sehr aufwendig und umständlich sein können, könnte das ein Argument sein, warum die Jungen aufgrund einer Faulheit eher nichts ändern und dem Anbieter vertrauen. Dass solche Änderungen kompliziert sein können, spricht auch für die große Anzahl derer unter den Jüngeren, die nichts ändern.

[173] Die Schüler wissen möglicherweise nicht, ob ihre Chats verschlüsselt sind oder was E-Mail-Verschlüsselung bedeutet und wie sie diese Funktion anwenden. Dieses Item ist sehr unglücklich gewählt, da daraus nicht abgeleitet werden kann, ob beim Mailen und/oder beim Chatten die Funktion genutzt wird und ob die Jugendlichen wissen, ob ihre Chats vom Anbieter verschlüsselt werden.

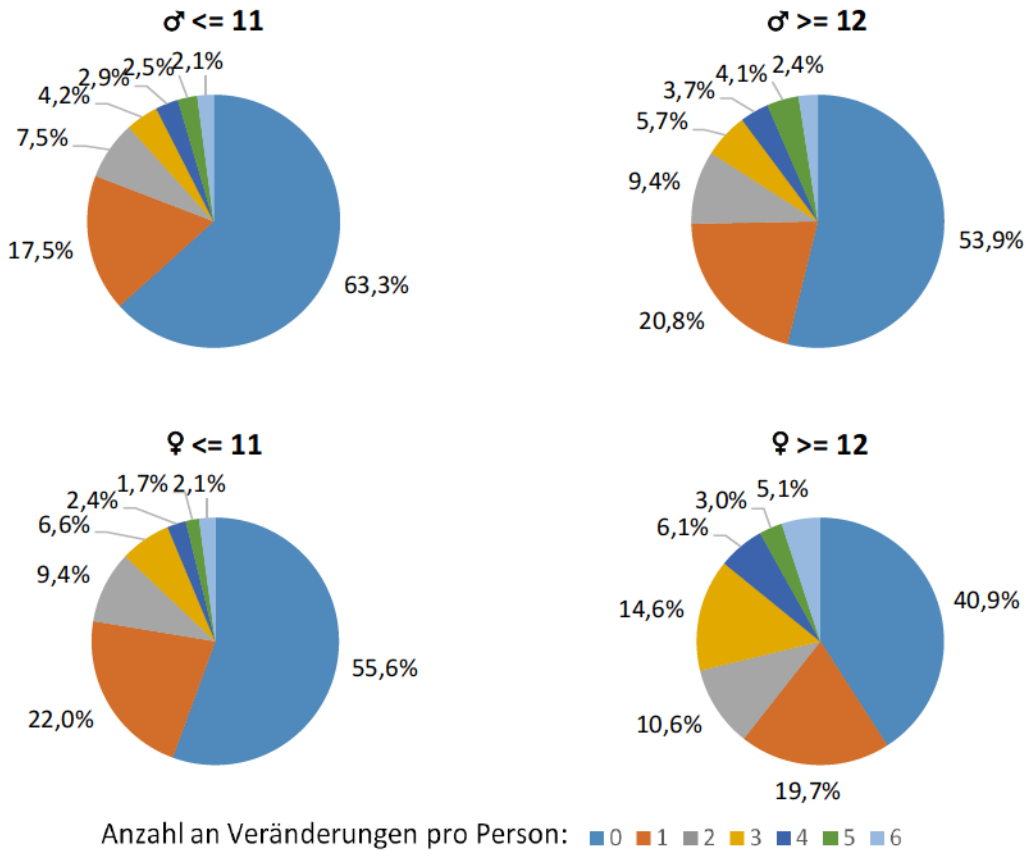


Abb. 4.24: Anzahl der Änderungen von Privatsphäreneinstellungen in Sozialen Netzwerken (Anhang Abb. A4.10-16)

Die Bestimmung darüber, wer etwas über den Betroffenen im Internet erfährt, wird von allen genutzt, wobei die Mädchen deutlich achtsamer sind (Abb. 4.25).

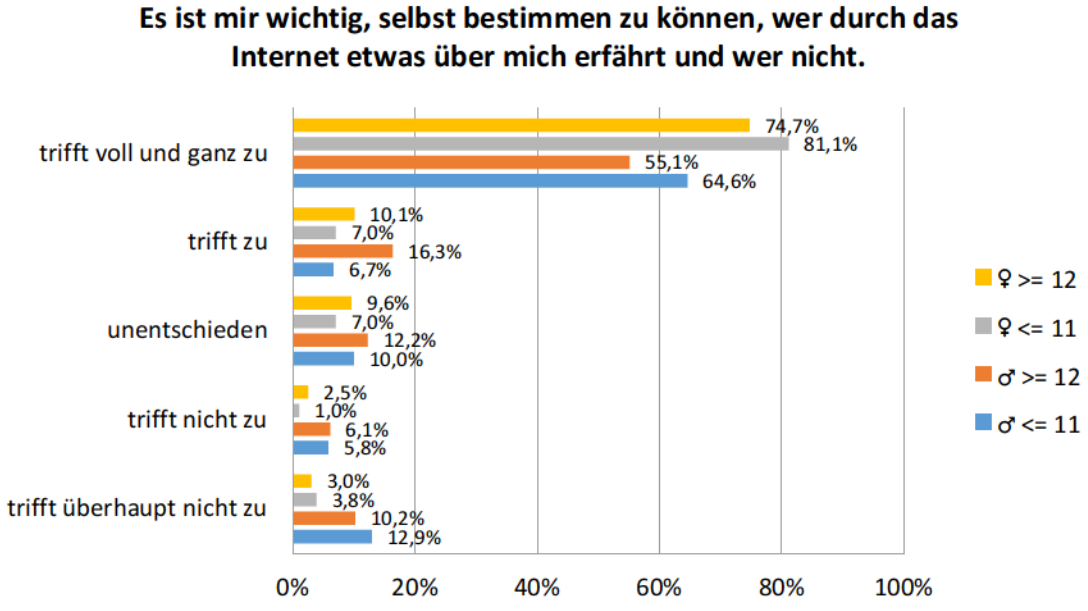


Abb. 4.25: Darstellung der eigenen Person im Internet (Anhang Abb. A4.10-19)

Reizvoll klingende Werbebanner werden eher von den Jüngeren angeklickt. Dies könnte daran liegen, dass die Älteren – auch aus gemachter Erfahrung – wissen, welche Lockangebote sich z. B. dahinter verbergen können und sie damit vorsichtiger sind (Abb. 4.26).

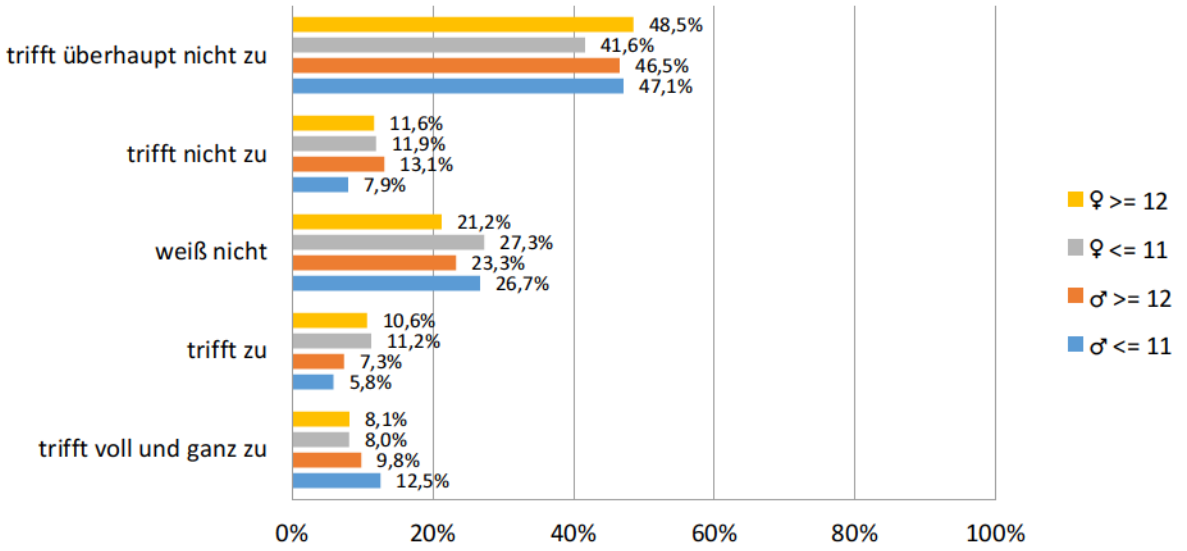


Abb. 4.26: Unkonzentriertes Anklicken reizvoller Werbebanner (Anhang Abb. A4.10-35)

Fasst man die Ergebnisse der drei Items zusammen, so kann man feststellen, dass insbesondere die Mädchen diejenigen sind, die eine bessere Urteilskompetenz besitzen. Innerhalb der Geschlechter sind es die Älteren, die vorsichtiger agieren.

Die Berechnung führt zu folgendem Ergebnis:

Klasse	B1/2	B3-3	H1-4	Summe	Note
Mädchen >= 12	59,1%	84,8%	60,1%	68,0%	3
Mädchen <= 11	44,4%	88,1%	53,5%	62,0%	4
Jungen >= 12	46,1%	71,4%	59,6%	59,0%	4
Jungen <= 11	36,7%	71,3%	55,0%	54,3%	4

Tab. 4.14: Bewertung der Dimension Urteilskompetenz

Die Urteilskompetenz ist bei den älteren Mädchen befriedigend, während die anderen Gruppen nur mit einem ausreichenden Ergebnis abschneiden.

Dimension *Handlungskompetenz*:

Darauf zu achten, welche Informationen man über sich ins Internet stellt, wird vor allem von den Mädchen – und hier insbesondere von den jüngeren – sehr stark genutzt. Bei den Jungen sind es die älteren, die hier vorsichtiger sind. Aufgrund der Zahlen kann hier von einer sehr

guten Handlungskompetenz bei den Mädchen und einer guten bei den Jungen gesprochen werden (Abb. 4.27).

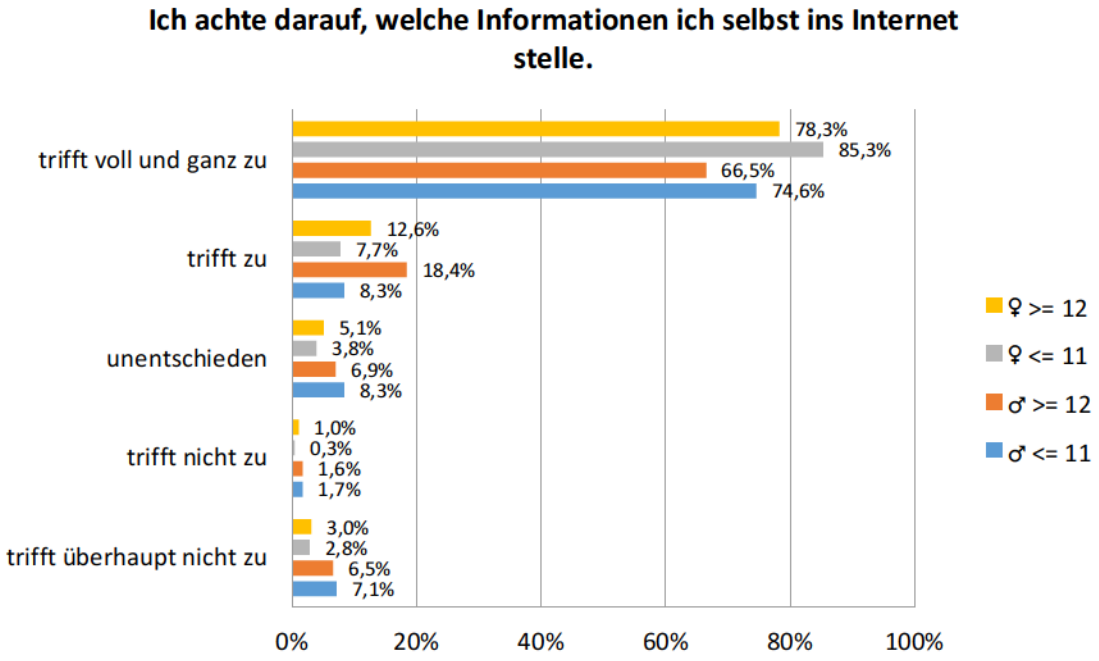


Abb. 4.27: Darstellung der eigenen Person im Internet (Anhang Abb. A4.10-18)

Bei der Frage nach der Löschung von E-Mails bei Spam-Verdacht, ist es die Gruppe der jüngeren Mädchen, die schnell reagiert. Die anderen Gruppen liegen zu nahe beieinander, sodass kein deutlicher Unterschied in Alter und Geschlecht ausgemacht werden kann. Eine regelmäßige Änderung von Passwörtern wird von allen Befragten sehr selten vorgenommen, wobei wiederum die jüngeren Mädchen sich um ca. 10 % (im positiven Sinne) von den anderen Gruppen abhebt. Bei der Frage zur regelmäßigen Aktualisierung der Software treten Jungen in den Vordergrund, während insbesondere die jüngeren Mädchen es nicht machen. Da dies wiederum eine eher technische Angelegenheit darstellt, zeigt sich auch hier ein ähnliches Bild wie in den vorangegangenen technischen Fragen. Zusammenfassend kann festgestellt werden, dass die befragten Jugendlichen viel zu selten ihre Passwörter ändern und ihre Software aktualisieren. Dies kann neben Unkenntnis auch durch Faulheit verursacht sein.

Die Berechnung der Anteile ergibt folgendes Ergebnis:

Klasse	B3-1	H1-9	H1-10	H1-11	Summe	Note
Mädchen >= 12	90,9%	56,5%	21,2%	40,4%	52,3%	4
Mädchen <= 11	93,0%	66,1%	32,1%	35,6%	56,7%	4
Jungen >= 12	84,9%	57,5%	22,1%	50,2%	53,7%	4
Jungen <= 11	82,9%	58,0%	23,8%	51,3%	54,0%	4

Tab. 4.15: Bewertung der Dimension Handlungskompetenz

Allen Gruppen wird aufgrund ihres Antwortverhaltens eine ausreichende Handlungskompetenz attestiert.

Zusammenfassung:

Wenn auch in allen Gruppen der Wissensbereich als mangelhaft bezeichnet werden muss, sind es die älteren Jugendlichen, die ein größeres Wissen als die jüngeren Befragten besitzen. Im Bereich der Risikobewertungskompetenz sind die jüngeren, die ein befriedigendes Ergebnis erzielten, den mit ausreichend abschließenden älteren Teilnehmern geringfügig überlegen, was für ein vorsichtigeres Verhalten spricht. Die Erfahrung im Umgang mit der Internetnutzung und die mit dem Alter höhere Risikobereitschaft erklären das schlechtere Abschneiden der älteren Jugendlichen. Obwohl unabhängig von Alter und Geschlecht bei allen Teilnehmern die Auswahl- und Nutzungskompetenz als mangelhaft zu bewerten ist, sind die diagnostizierten Defizite bei den Mädchen größer als bei den technisch interessierten Jungen. Aufgrund der Erfahrung der Internetnutzung sind auch hier die Älteren den Jüngeren überlegen. Die Urteilskompetenz, die insgesamt als ausreichend (bei den älteren Mädchen sogar als befriedigend) bezeichnet werden kann, ist bei den Mädchen ausgeprägter, da sie im Gegensatz zu den Jungen überlegter handeln und damit vorsichtiger agieren. Unabhängig von Alter und Geschlecht ist die Handlungskompetenz noch ausreichend, wobei in dieser Dimension keine großen Unterschiede zwischen den Gruppen zu verzeichnen sind.

4.4. Zusammenfassung der Auswertungsergebnisse und Diskussion

Ziel der Online-Befragung war es, eventuell vorhandene Mängel an Datenschutzkompetenz bei Jugendlichen im Alter von zehn bis 13 Jahre aufzudecken. Als Referenz diente das Datenschutzkompetenzmodell (vgl. Kapitel 3), aus dem Datenschutzkompetenzen abgeleitet worden sind, die für alle Internetnutzer – unabhängig vom Alter – gelten. Da die Jugendlichen sich aber erst in der Anfangsphase befinden, in der sie teilweise eigenständig die Welt des Internets erkunden, musste damit zu rechnen sein, dass sie sich nicht wie Erwachsene verhalten und damit nicht so sicher und so datenschutzkompetent auftreten werden. Daher wurde bei der Auswahl der Items auf das Alter entsprechend geachtet.[174]

Die Studie hat gezeigt, dass die befragten Jugendlichen insgesamt betrachtet eine schwach ausreichende Datenschutzkompetenz besitzen. Während im Bereich der Risikobewertungskompetenz und Urteilskompetenz durchaus noch ausreichende Leistungen gemessen worden sind, kann im Bereich des Wissens, der Auswahl- und Nutzungskompetenz und Handlungskompetenz nur von mangelhaften Ergebnissen gesprochen werden.

Eine differenzierte Betrachtung der Antworten nach Alter und Geschlecht ergibt keinen gravierenden Unterschied zu dem Gesamtergebnis. Auffällig ist jedoch, dass bei der Auswertung

[174] So wurden z. B. bei der Auswahl der Wissensfragen Begriffe ausgewählt, die Schüler des entsprechenden Alters kennen müssen, oder Anwendungsfälle genannt, mit denen Schüler in Berührung kommen.

der Handlungskompetenz unabhängig von Alter und Geschlecht ausreichende Leistungen verbucht werden können (im Gegensatz zur Gesamtauswertung mit mangelhafter Leistung). Dies liegt daran, dass im Rahmen der differenzierten Auswertung nur eine Teilmenge aller Items betrachtet worden ist. Im Fall der Handlungskompetenz sind somit diejenigen Items entfallen, die zum mangelhaften Abschneiden in der Gesamtauswertung geführt haben.

Die Benotung aus den deskriptiven Auswertungen ist zusammenfassend in der folgenden Tabelle dargestellt:

	Gesamtgruppe	jüngere Mädchen	ältere Mädchen	jüngere Jungen	ältere Jungen
W	5	5	5	5	5
RK	4	3	4	3	4
ANK	5	5	5	5	5
UK	4	4	3	4	4
HK	5	4	4	4	4

Tab. 4.16: Notenverteilung der deskriptiven Auswertungen

Es kann die geringe Tendenz abgelesen werden, dass die Mädchen im Vergleich zu den Jungen und die Jüngeren im Vergleich zu den Älteren ein eher vorsichtigeres Verhalten bei der Internetnutzung zeigen. Gründe für diese Beobachtung könnten sein, dass Mädchen in dem untersuchten Alter generell eine eher überlegte Handlungsweise und damit vorsichtigeres Agieren zeigen; Jungen sind experimentierfreudiger und weniger ängstlich. Dass die älteren Jugendlichen im Allgemeinen besser abschneiden, kann damit begründet werden, dass ihre Kompetenz im Umgang mit Computer (respektive Smartphone) schon wegen des Alters größer ist. Das fehlende Wissen im Bereich dieser Fragen mag damit zu tun haben, dass die Befragten die Informatiksysteme ungezwungen und als gegeben hinnehmen und diese einfach „nur“ nutzen. Über den Hintergrund (Funktionsweise, …) wird sich keine Gedanken gemacht. Aufgrund der Technikaffinität der Jungen gegenüber den Mädchen sind bei Fragenstellungen dieser Art die Jungen den Mädchen geringfügig überlegen.

Die an dieser Stelle gemachten Beobachtungen decken sich mit den existierenden Studien. Wie schon in Abschnitt 2.3.2 geschrieben, werden die Chancen und Risiken der Internetnutzung wahrgenommen, was aber nicht zu einer Verstärkung der Sicherheitsanforderungen führt. Den Jugendlichen fehlen der fachliche Hintergrund und das Verständnis. Insbesondere folgende Aspekte konnten aus vorangegangenen Studien zum großen Teil bestätigt werden:

- Der Datenschutzinstinkt ist gut ausgeprägt, kann aber den komplexen Entwicklungen kaum Stand halten.
- Beobachtungen zeigen, dass sich inzwischen vermehrt Schüler auf Sozialen Netzwerken anmelden, denen die notwendige Kompetenz fehlt.
- Der Wissensstand zu Datenschutz und Persönlichkeitsrechten ist recht heterogen.
- Laut Studien achten gerade die Älteren (ab 12 Jahren aufwärts) darauf, welche Informationen sie über sich hochladen. In der vorliegenden Untersuchung waren es jedoch

die Jüngeren die vorsichtiger agieren, wobei die Differenz zu den Älteren nur 3,4 % beträgt.

- Je älter die Befragten sind, desto eher werden Änderungen in den Profileeinstellungen Sozialer Netzwerke vorgenommen, wobei laut vorangegangenen Studien dies eher die Jungen statt die Mädchen tun. In der durchgeführten Untersuchung waren dies jedoch eher die Mädchen, wobei die Differenz zwischen Jungen und Mädchen nur 3 % beträgt.

Die geringfügigen Abweichungen in den beiden letzten Punkten könnten damit erklärt werden, dass zwischen den Daten der früheren Studien und der durchgeführten Untersuchung ein Zeitraum liegt, in dem es durchaus zu Änderungen in der Einstellung der Jugendlichen im Umgang mit personenbezogenen Daten gekommen ist.

In einem zweiten Teil der Auswertung wurde der Frage nachgegangen, ob zwischen den Dimensionen des Datenschutzkompetenzmodells ein Zusammenhang herrscht oder nicht. Dazu wurden Korrelationen zwischen den Daten untersucht. Es konnte gezeigt werden, dass solche existieren und die Dimensionen des Modells sich gegenseitig bedingen. Aufgrund der Zahlen kann die Schlussfolgerung gezogen werden, dass die einzelnen Dimensionen des Datenschutzkompetenzmodells nicht getrennt voneinander betrachtet und unterrichtet werden dürfen, da sie sich gegenseitig schwach beeinflussen. Dies bedeutet wiederum, dass bei einer Förderung der Datenschutzkompetenz darauf zu achten ist, dass alle Dimensionen entsprechend repräsentiert sind. Somit ist es nicht getan, den Schülern nur Wissen zu vermitteln, weil dies dann beispielsweise die Handlungskompetenz nach sich zieht. Die Unterrichtsreihen und -beiträge müssen so gestaltet sein, dass alle Dimensionen ausgebildet werden. Dieser Aspekt wird in die Handlungsempfehlungen (Kapitel 6) einfließen.

„Die Ergebnisse empirischer sozialwissenschaftlicher Forschung [sind] immer auch von den Erhebungsverfahren/Instrumenten abhängig …, mit denen sie gewonnen werden“ (Wolf 1995, S. 322). Rückblickend kann der Autor feststellen, dass das aufgezeigte Vorgehen Mängel aufzeigt. Sicherlich war es richtig, auf schon existierende Items veröffentlichter Studien zurückzugreifen und diese durch andere Personen bewerten zu lassen, jedoch hätte im Zuge dieses Verfahrens die unterschiedliche Art der Items nicht gemischt werden dürfen und das Auswertungsverfahren vorab differenzierter geplant werden müssen. So ergab die Anwendung z. B. einer explorativen Faktorenanalyse keine aussagekräftigen Ergebnisse. Zudem sind aufgrund der Datenlage nur Spekulationen über die Verhaltensgründe möglich. Wären Interviews mit den Jugendlichen geführt worden (z. B. mit einer ausgewählten Anzahl der Studienteilnehmer), so hätte man möglicherweise Verhaltensmotive erfahren. Bei einer erneuten Umfrage mit anderen oder ähnlichen Items ist darauf zu achten, dass bei den Konstrukten zudem Operatoren geringerer Komplexität gewählt werden müssen.

Letztendlich konnte durch die Erhebung immerhin gezeigt werden, dass teilweise gravierende Mängel der Datenschutzkompetenz bei den Jugendlichen, die sich am Beginn der eigenständigen Auseinandersetzung mit dem Internet befinden, vorhanden sind, die es zu beheben gilt. Passende Handlungsempfehlungen für den Informatikunterricht, die in Kapitel 6 vorgestellt werden, erwachsen aus den Ergebnissen der durchgeführten Erhebung.

4.5. Schülerwünsche zum Thema *Datenschutz*

Im Rahmen der Studie wurde den Schülern auf der letzten Seite des Fragebogens die Frage gestellt, worüber Sie mehr Informationen erhalten möchten. Zur Antwort standen:

- „Mehr Information zum Schutz meiner Daten im Internet“
- „Mehr Information zur rechtlichen Situation in Bezug auf den Schutz meiner Daten“
- „Mehr Information zu technischen Möglichkeiten des Schutzes meiner Daten“
- „Mehr Information zu den Gefahren beim Surfen im Internet“

Die Antwortmöglichkeiten waren *Ja*, *Egal*, *Nein*.

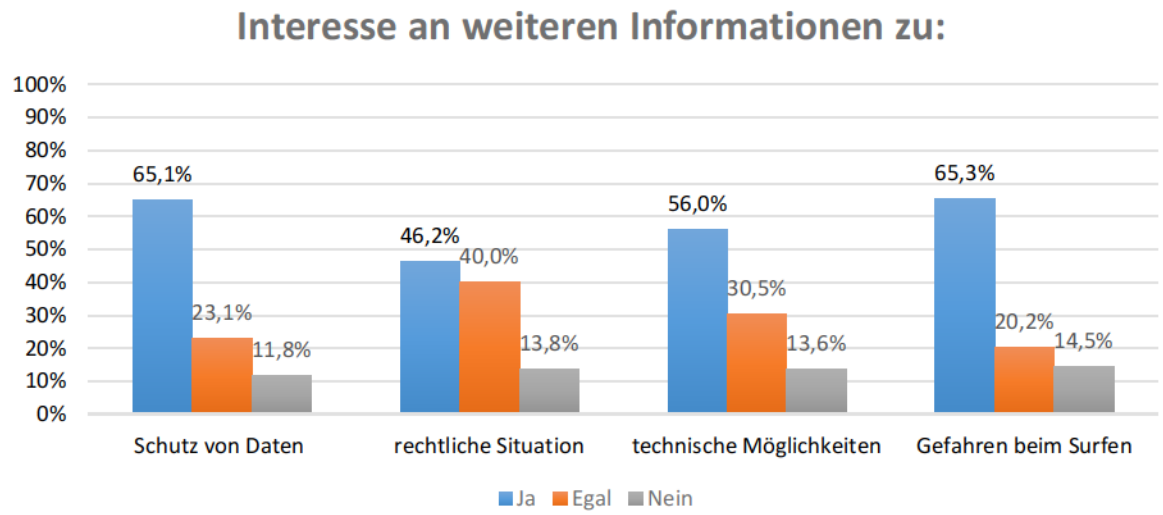


Abb. 4.28: Interessenbekundung der Schüler (Anhang Abb. A4.9-26)

Die Gefahren beim Internetsurfen und der Schutz der Daten sind jeweils von rund 65 % der Schüler als die Themen eingestuft worden, zu denen mehr Information gewünscht wird. Während immerhin noch gut mehr als die Hälfte sich für technische Maßnahmen zum Datenschutz interessiert, sind es nur noch etwa 45 %, die Fragestellungen zu rechtlichen Situationen besprochen haben möchten. Kein Interesse an diesen Themen haben im Schnitt rund 13 % der Befragten. Damit ist klar ausgesagt, dass ein starkes Interesse rund um das Thema *Datenschutz* existiert, wobei Aufklärung und konkrete Schutzanwendungen im Fokus stehen. Somit ist eine Motivation für das Thema auf jeden Fall bei der Mehrheit der Schüler vorhanden.

Ferner wurde den Teilnehmern das Angebot gemacht, in einem Freitextfeld Wünsche und Anregungen bezüglich dieser Studie und zum Thema Datenschutz zu nennen. Insgesamt gab es rund 150 sinnvolle Rückmeldungen, die sich in zwei Gruppen einteilen lassen. Die eine Gruppe betraf Rückmeldungen zu der Studie selbst, während die andere Gruppe Fragen oder Bitten rund um das Thema *Datenschutz* darstellte. Eine Aufzählung aller Rückmeldungen ist an dieser Stelle nicht möglich, sodass diese hier zusammengefasst vorgestellt werden.

Rückmeldungen zur Studie selbst waren, dass ein Teil der Befragten die Studie „interessant, was so alles passieren kann“, „toll“, „spannend“ bis hin zu „cool“ fanden, ein anderer Teil die Fragen als „zu schwer“, „nicht beantwortbar, weil kein Computer/Handy“ besitzen, „zu kompliziert“, „zu lang“ bzw. „zu umfangreich“ einstufte, weil „teilweise die Sachen gar nicht genutzt werden“, man die Dinge „nicht kennt“ oder die „Begriffe unbekannt“ sind. Wiederum andere wünschten sich eine „Musterlösung“ der Studie, welche eine Person „als Quiz“ interpretierte. Mehr „Aufklärung“ wurde gewünscht, da man „nichts dazu gelernt“ habe. Kritisiert wurde, dass „unpassende“ oder „nicht genügend Antwortmöglichkeiten“ zur Verfügung standen (z. B. „kenne ich nicht“) und dass der Zwang zum Antworten bestand.

Interessant ist auch, dass ein Teilnehmer sich fragte, wie man aus den Fragen Ergebnisse ableiten könne. Und ein Anderer eine Rückmeldung erbat und dafür seine E-Mail-Adresse hinterließ. Zuletzt wurde angemerkt, dass es doch „ironisch“ sei, „bei einer Datenschutz-Umfrage am Ende nach persönlichen Daten zu fragen“.

Dieses Bild an Antwortauszügen, deren Zitate von unterschiedlichen Teilnehmern zusammengefügt worden sind, entspricht auch dem der ausgewerteten Daten, nämlich korrekt beantwortete als auch unbeantwortete Items. Der Autor muss eingestehen, dass doch viele der Schüler mit den Fragestellungen und der Art zu antworten überfordert waren.

Deutlich länger und ausführlicher waren Rückmeldungen und Wünsche zum Thema *Datenschutz*, von denen hier beispielhaft nur einige vorgestellt werden sollen. Ein besserer „E-Mail-Schutz“, „bessere Anti-Viren-Programme“ bzw. „weniger Viren“, Schutz vor „perversen Seiten“, ein „sicheres Internet“ und sicherere/weniger „Soziale Netzwerke“, die „dann Dinge über einen wissen“, sind den Schülern sehr wichtig, sodass man sich keine „Sorgen/Ängste von Hackern“ machen müsse, wobei der Wunsch geäußert wurde, dass es solche nicht mehr gäbe. Eine „Internetüberwachung“ und „ein sauberes Internet“ waren gewünscht. Aufklärung wurde insbesondere in folgenden Bereichen favorisiert: zum „Datenschutz“ allgemein, zum „sicheren Surfen und den Gefahren“, zum „Verhalten bei Viren-Infektion“, über „Internet-Begriffe und Netzwerke“ und vor allem auch dem „Mobbing“ und dem „Verhalten in Chaträumen“. Einige wünschten sich einen „besseren Kinderschutz im Internet“, „Warnungen vor gefährlichen Apps oder Abo-Fallen“ und „Warnungen vor Spam, die dann automatisch gelöscht werden“, wobei die „Anzeige legaler Seiten deutlich gemacht“ werden solle. Viele Teilnehmer stellten Fragen wie „Wie surfe ich richtig? Was sind Cookies?“ und „Was passiert beim Haken mit persönlichen Daten? Was passiert, wenn man Handy-Nummer und E-Mail veröffentlicht?“, „Was passiert, wenn aus Versehen der Wohnort veröffentlicht wird?“, „Was muss man machen, um vor Hackern sicher zu sein?“, „Welche Seiten kann man guten Gewissens nutzen? Welche sind 100% sicher und virenfrei?“ und „Wie kann man im Netz anonym bleiben?“. „Sichere Account-Einstellungen bei You-Tube, Snapchat und Sozialen Netzwerken“, „Gefahr beim Betreiben eines You-Tube-Channels“, „Passwörter-Erstellung“ und die „Sicherung von Daten“ stellten einen anderen Bereich an Fragen dar. Ebenfalls wurde kritisiert, dass ein „Verständnis von Datenschutzerklärungen“ erfolgen solle und „wichtige Dinge sollten vorne und nicht hinten auf der Webseite stehen“, wobei hier vermutlich Dinge wie AGB gemeint sind.

Auch der Bereich Online-Spiele wurde thematisiert. Im Sektor *Handy* waren es „Sorgen um die Standorterkennung“, um die „Handy-Spionage“ und „ein unbemerktes Hacking“, wobei sich auch gefragt wurde, „wieso … man durch Haken Informationen anderer Leute sehen“ kann.

Bemerkenswert ist, dass ein Teilnehmer sich ein Fach wünschte, in dem diese Themen rund um Datenschutz besprochen werden könnten, d. h. es ist der Wunsch nach einem Pflichtfach Informatik vorhanden. Wiederum eine andere Person meinte, dass man schon die „Grundschule besuchen und informieren“ müsse, damit „jüngere Schüler besser aufgeklärt“ seien.

Die immense Anzahl zum Teil gleicher Rückmeldungen zeigt, dass die Schüler einerseits in Sorge leben und den Wunsch haben, Hilfestellungen zum Schutz vor Gefahren und Verbrechern zu bekommen. Eine Sensibilität seitens vieler Schüler ist schon vorhanden, nur mit einer korrekten Beurteilung der Situation sind viele überfordert. Das Antwortverhalten spiegelt auch diese Einschätzung wieder.

4.6. Zweites Zwischenergebnis

Die zweite Forschungsfrage lautet:

> In welchen Dimensionen des in dieser Arbeit hergeleiteten Datenschutzkompetenzmodells weisen Schüler der Klassenstufe 5 bis 7 einen Mangel an Datenschutzkompetenz auf?

Es konnte gezeigt werden, dass in allen Dimensionen des Modells Mängel bei den Jugendlichen im Alter von zehn bis 13 Jahren herrschen. Auch wenn sie im Bereich der Risikobewertungskompetenz und der Urteilskompetenz ausreichend vorbereitet sind, so ist doch in allen Feldern ein großer Ausbildungsbedarf vorhanden. Die zu Beginn gestellte Leitfrage, wie gut die Kinder und Jugendlichen auf die digitale Welt vorbereitet seien, muss aufgrund der Datenlage als mangelhaft bezeichnet werden. Wenn auch an einigen Stellen tendenziell ein korrektes Verhalten bei der Internetnutzung zu erkennen ist, so überwiegen eindeutig die Schwächen. Die Jugendlichen sind nicht datenschutzkompetent ausgebildet, sodass im (Informatik-)Unterricht der Datenschutzkompetenz-Erziehung ein entsprechender Raum eingeräumt werden muss. Jede einzelne Kompetenz im Sinne der Dimensionen des Datenschutzkompetenzmodells ist gezielt zu fördern, weshalb passende Unterrichtselemente zu entwickeln sind. Daher werden in dem folgenden Kapitel Unterrichtsprojekte vorgestellt, die im Rahmen studentischer Abschlussarbeiten im Zeitraum Frühjahr 2015 bis Herbst 2019 entstanden sind. Dem schließt sich ein Kapitel zu Handlungsempfehlungen für den (Informatik-)Unterricht an.

„Medienkompetenz ist identisch mit der Fähigkeit,
kritisch denken zu können."
Joseph Weizenbaum (1997)[175]

5. Unterrichtsprojekte und Arbeiten im praktischen Umfeld der Schule

Wie die in Kapitel 4 beschriebene Studie zeigt, kann die untersuchte Schülergruppe nicht als datenschutzkompetent bezeichnet werden. In allen Dimensionen, die in dem Datenschutzkompetenzmodell (vgl. Kapitel 3) beschrieben sind, können deutliche Mängel diagnostiziert werden. Dies deckt sich auch mit den Erkenntnissen vorangegangener Studien (vgl. Abschnitt 2.3.2). Daher muss die logische Konsequenz sein, Wege aufzuzeigen und Mittel bereit zu stellen, um diesen Defiziten entgegenzuwirken.

In dem vorliegenden Kapitel werden sechs Projektbeispiele vorgestellt, die im Rahmen von Bachelor- und Masterarbeiten, die der Autor betreut hat, in der Gruppe *Didaktik der Informatik* an der Universität Koblenz-Landau in den letzten Jahren entstanden sind. Dabei sind unterschiedliche Zielsetzungen verfolgt worden. Zum einen sind es Vorarbeiten und Vorüberlegungen zur Datenschutzkompetenzförderung und zum anderen konkret ausgearbeitete und durchgeführte Unterrichtsprojekte, sodass Erfahrungsberichte zur Umsetzung vorliegen. Die Einschätzung und Bewertung dieser Praxisbeispiele ist jedoch subjektiv und wurde nicht wissenschaftlich ausgewertet. Für jedes Projekt werden die zu fördernden Datenschutzkompetenzen herausgearbeitet, um den Bezug zum Datenschutzkompetenzmodell herzustellen.

Wenn auch in Abschnitt 2.2.2.2 Beispiele für einen fachübergreifenden Ansatz vorgestellt werden, wie es auch in (Wagner 2012) gefordert wird, da eine Thematisierung von Datenschutz alle Fächer betrifft, wird dieser Ansatz im Folgenden nicht weiterverfolgt, da im ersten Schritt eine Fokussierung auf informatische Inhalte im Vordergrund steht.

[175] Redebeitrag auf der Frankfurter Buchmesse, zitiert nach: Magenau, Jörg (1997): buchmessern – Kein Ort zum [illegible] n. In: TAZ vom 20.10.1997, S. 16. https://taz.de/!1377388/ (zuletzt geprüft am 28.12.2019)

5.1. Projekte zur Förderung der Datenschutzkompetenz bei Jugendlichen

Anhand folgender Tabelle wird ein erster Überblick über die sechs Abschlussarbeiten gegeben:

Nummer	Thema	Altersstufe	Inhalte
5.1.1	Datenschutz in der Orientierungsstufe	Klasse 5 – 6	Ausgehend von existierenden und selbst entwickelten Unterrichtsmaterialien wird eine Unterrichtsreihe zum Thema *Datenschutz* mit dem Ziel entwickelt, eine intrinsische Motivation dafür bei den Schülern zu entwickeln. Das Projekt wurde im Unterricht durchgeführt und evaluiert. Ferner wurde die Arbeit im Rahmen einer Lehrerfortbildung vorgestellt.
5.1.2	Datenschutz im Kontext Sozialer Netzwerke unter Verwendung von *InstaHub*	Klasse 5 – 6 mit Ausblick in die Sek. I	Unter Nutzung von InstaHub wird eine intrinsische Motivation zu Datenschutz in Sozialen Netzwerken initiiert und diese auf die allgemeine Internetnutzung übertragen. (Dem schließt sich ein Exkurs zum Thema *Datenbanken* an.) Das Projekt wurde in verkürzter Form im Unterricht durchgeführt und evaluiert.
5.1.3	Soziale Netzwerke und Relationen unter Verwendung von *InstaHub*	Sek. II mit Ausblick in die Sek. I	Drei Lehr-Lern-Settings zu den Themen *Mathematische Relationen*, *Datenbanken in Sozialen Netzwerken* und *Datenschutz* werden entwickelt, um Freundschaftszusammenhänge in Sozialen Netzwerken zu beleuchten. Die Visualisierung der Relationen erfolgt über das entwickelte Tool *InstaHubRelation*.
5.1.4	Newsfeedfunktion in *InstaHub* und Personalisierte Algorithmen	Sek. II	Es wird eine *InstaHub*-Erweiterung für Newsfeeds und für einen personalisierten Algorithmus vorgestellt und eine Unterrichtsreihe entwickelt, in denen die Schüler die Hintergründe und Gefahren von Filterblasen erlernen. Das Projekt wurde im Unterricht durchgeführt und evaluiert.
5.1.5	Weiterentwicklung des IniK-Projekts[176] *Planspiel Datenschutz 2.0*	Sek. II	Es werden die technischen und inhaltlichen Grenzen der Version 2.0 des Planspiels vorgestellt. Dem folgen Vorschläge zur Überwindung dieser Probleme und die Entwicklung auf die heutige Schülergeneration abgestimmten Rollen und Settings.

Tab. 5.1a: Auflistung der studentischen Abschlussarbeiten

[176] IniK steht für *Informatik im Kontext*; vgl. dazu Abschnitt 2.4.

Nummer	Thema	Altersstufe	Inhalte
5.1.6	Unterrichtsreihe zum Thema *Datenschutz und Datensicherheit* im kontextorientierten Ansatz	Sek. II	Es wird eine Reihe mit dem Ziel vorgestellt, Risiken bei der Nutzung des Smartphones zu erkennen und zu vermeiden. Es gilt, die Schüler zu sensibilisieren und eine Verhaltensänderung zu wecken.

Tab. 5.1b: Auflistung der studentischen Abschlussarbeiten

In den jeweiligen Unterabschnitten werden je nach Ziel der Arbeit folgende Aspekte betrachtet: Ausgehend von der Forschungsfrage der Arbeit werden die zu fördernden Datenschutzkompetenzen gemäß Tabelle 3.8 genannt und die Lernziele/Kompetenzen für die Lerngruppe formuliert. Der Vorstellung der Unterrichtseinheit (gegebenenfalls mit einer knappen Evaluation) folgen ein Ausblick und Weiterentwicklungsvorschläge.[177]

5.1.1. Unterrichtsreihe *Datenschutz in der Orientierungsstufe*

(Thielen 2018) beschreibt in seiner Arbeit eine Unterrichtsreihe zum Thema *Datenschutz*, die auf eine Lerngruppe in der Orientierungsstufe ausgerichtet ist. Leitfrage der Arbeit ist, „wie … eine Unterrichtsreihe zum Thema Datenschutz aussehen [kann], sodass Schülerinnen und Schüler erstens dafür ein Interesse entwickeln und zweitens sich dann, aus der intrinsischen Motivation heraus, in das Thema vertiefen?“ (Thielen 2018, S. 6). Die von ihm geplante Reihe wurde in dieser Form in einer 6. Klasse an einem Gymnasium im Rahmen des Mathematikunterrichts[178] gehalten und anschließend evaluiert.

Dabei stehen insbesondere folgende zu fördernden Kompetenzen im Vordergrund (vgl. Tab. 3.8):

- DSK1: Schüler kennen Grundbegriffe im Umgang mit Internetnutzung. (Dimension Wissen)
- DSK2: Schüler ordnen den Begriff "Datenschutz-Erklärung" im Kontext der Internetnutzung ein und kennen die daraus abgeleiteten Rechte und Pflichten. (Dimension Wissen)
- DSK4: Schüler wissen um das Verhalten (insb. nicht-europäischer) Unternehmen, personenbezogene Daten anderweitig als für den vorgesehenen Zweck zu verwenden. (Dimension Wissen)
- DSK5: Schüler kennen Maßnahmen, um das Internet-Surfverhalten zum eigenen Schutz anzupassen, und wenden technische und weitere Maßnahmen zur sicheren Internetnutzung an. (Dimensionen Wissen und Handlungskompetenz)

[177] Die Ideen der Umsetzung stammen von den jeweiligen Autoren (unter der Beratung des Autors der vorliegenden Arbeit), ohne dass dies an jeder Stelle explizit genannt wird; wörtliche Zitate aus den Abschlussarbeiten sind entsprechend kenntlich gemacht.

[178] Da das Schulfach *Informatik* nicht angeboten wird, wurde auf den Mathematikunterricht ausgewichen. Die letzte Einheit der Reihe (sichere Passwörter) gab dem Fachlehrer die Möglichkeit, daran anknüpfend das Thema *Kombinatorik* im Mathematikunterricht zu behandeln.

- DSK6: Schüler bewerten die Sensibilität personenbezogener Daten. (Dimension Risikobewertungskompetenz)
- DSK7: Schüler schätzen den Wirkradius und die Gefahr (selbst-)veröffentlichter (persönlicher) Daten ab. (Dimension Urteilskompetenz)
- DSK11: Schüler bewerten das Ausmaß von Kenntnissen persönlicher Informationen durch Dritte und reagieren angemessen. (Dimensionen Urteilskompetenz und Handlungskompetenz)
- DSK15: Schüler wenden Maßnahmen zum Schutz von Zugängen (zu Systemen, Portalen, …) an. (Dimension Handlungskompetenz)
- DSK16: Schüler berücksichtigen Risiken der Internetnutzung und handeln dementsprechend. (Dimension Handlungskompetenz)

(Thielen 2018, S. 33) nennt als Hauptlernziele:

- „Die Schülerinnen und Schüler können Grundbegriffe des Datenschutzes erklären.
- Die Schülerinnen und Schüler sind in der Lage, das Risiko in datenschutzkritischen Situationen objektiv einzuschätzen.
- Die Schülerinnen und Schüler beherrschen einen sensiblen Umgang mit ihren persönlichen Daten und können Handlungsmuster anwenden, um diese zu schützen."

Dabei setzt (Thielen 2018, S. 39) folgende Schwerpunkte:

- „Das Erkennen von persönlichen Daten sowie das Schaffen eines Bewusstseins für die Gefahren durch deren Verarbeitung,
- Das Herausbilden eines Verständnisses für die Funktionsweise von Schadsoftware und die Vermittlung von empfohlenen Schutzmaßnahmen,
- Das Durchschauen der Problematik von zu vielen Berechtigungen bei Apps und dem damit verbundenen, nicht offensichtlich zugestimmten Sammeln von Daten,
- Das Wissen über die Erstellung von Bewegungsprofilen und der davon ausgehenden Gefahr der Überwachung,
- Die Erkenntnis der Funktion von Cookies und dem Browserverlauf zur Erstellung von Profilen,
- Das Kennenlernen von Tools zum Selbstdatenschutz,
- Das Vermitteln von Rechten und Gesetzen im Datenschutz für die Verbraucher,
- Sowie die Erarbeitung von Regeln zu Passwörtern, um die Sicherheit von Daten in Onlinediensten zu erhöhen."

Zu Beginn der Reihe steht die Erkenntnis, was personenbezogene Daten sind und welche Risiken durch eine Veröffentlichung bestehen. Da Smartphones bzw. deren Apps als „Datenschnüffler" fungieren, können daraus die Gefahren der Datenpreisgabe abgeleitet werden. Der darauffolgende Block ist als Stationenlernen ausgerichtet. „Die Themenwahl lag dabei bei Schadsoftware, Profilbildung durch Browserinformation und Bewegungsdaten sowie der Berechtigungen von Apps bis hin zum Datenschutz in Recht und Gesetz sowie Selbstdatenschutz durch Tools" (Thielen 2018, S. 68). Mit einer Einheit zum Thema *Passwörter, Passwortregeln und Passwortstärke* wird die Reihe abgeschlossen. Es wurde bei der Planung auf eine abwechslungsreiche Methodik (insbesondere durch die Stationenarbeit) und eine innere Differenzierung geachtet.

Der Student stellt am Ende fest, dass die gesamte Reihe an sich, trotz einiger Schwächen, als gelungen bezeichnet werden kann. Die Schwächen resultierten aus schulischen Rahmenbedingungen, die bei einer Überarbeitung zu berücksichtigen wären, der falsch eingeschätzten und sehr lebhaften Lerngruppe und seiner eigenen stark geringen Professionalität als Lehrkraft.

Drei Wochen nach der gehaltenen Unterrichtsreihe wurde zur Überprüfung des Projekterfolgs eine Umfrage innerhalb der Lerngruppe gestartet, die sich aus Items der in Kapitel 4 vorgestellten Studie zusammensetzt. Da die Lerngruppe zuvor schon daran teilgenommen hatte, waren die Items den Schülern nicht unbekannt. Eine Vergleichbarkeit der Zahlenwerte ist jedoch extrem schwierig, da aus der vom Autor durchgeführten Studie die Probandengruppe nicht herausgefiltert werden kann. Trotzdem wurden die ausgewerteten Daten, die in (Thielen 2018, S. 118) nachzulesen sind, den Ergebnissen der Studie gegenübergestellt. Insgesamt kann gesagt werden, dass keine deutliche Verbesserung der Werte zu beobachten ist. Daraus aber den Schluss zu ziehen, dass die Reihe erfolglos wäre, ist nicht gerechtfertigt. Stattdessen zeigen die Ergebnisse, dass das Thema Datenschutz an anderer Stelle wieder aufgegriffen und weiter vertieft werden muss, um eine Verbesserung des Lernerfolgs zu garantieren.

Thielen schlägt vor, die Stationen des zweiten Teils der Reihe gleichzeitig auch in leichter Sprache für Schüler mit Sprachproblemen zu formulieren. Da in vielen Fällen eine Smartphone-Nutzung schon in der Grundschule beobachtet wird, ist eine Anpassung der Reihe auf die Primarstufe denkbar. Zudem ist die Datenschutzkompetenzförderung ein Thema für einen fächerverbindenden Unterricht, wobei sich damit die Frage stellt, ob die Vermittlung effektiver wäre. Die Gestaltung als Projekt innerhalb einer Schulprojektwoche scheint dafür ein passender Ansatz zu sein.

5.1.2. Datenschutz im Kontext Sozialer Netzwerke unter Verwendung von *InstaHub*

Wie die in dem Abschnitt zuvor beschriebene Unterrichtsreihe greift auch diese Masterarbeit das Thema *Datenschutz* für die Orientierungsstufe auf. Da die Nutzung Sozialer Netzwerke und ähnlicher Plattformen schon bei Kindern im Alter ab 8 Jahren nachgewiesen ist (vgl. Abschnitt 2.3.2), bietet es sich an, die Thematik im Zusammenhang mit Sozialen Netzwerken zu bearbeiten. InstaHub als ein speziell für den Informatikunterricht konzipiertes Soziales Netzwerk kann in diesem Zusammenhang genutzt werden. Die Forschungsfrage der Masterarbeit lautet: „Wie gestaltet sich eine Unterrichtsreihe zum Thema Datenschutz im Kontext Sozialer Netzwerke in der Orientierungsstufe eines Gymnasiums?“ (Savelsberg 2019, S. 7)

Durch diese Unterrichtsreihe sollen folgende Datenschutzkompetenzen insbesondere gefördert werden (vgl. Tab. 3.8):

- DSK1: Schüler kennen Grundbegriffe im Umgang mit Internetnutzung. (Dimension Wissen)

- DSK2: Schüler ordnen den Begriff "Datenschutz-Erklärung" im Kontext der Internetnutzung ein und kennen die daraus abgeleiteten Rechte und Pflichten. (Dimension Wissen)
- DSK3: Schüler geben ihre Rechte aus der informationellen Selbstbestimmung an. (Dimension Wissen)
- DSK5: Schüler kennen Maßnahmen, um das Internet-Surfverhalten zum eigenen Schutz anzupassen, und wenden technische und weitere Maßnahmen zur sicheren Internetnutzung an. (Dimensionen Wissen und Handlungskompetenz)
- DSK6: Schüler bewerten die Sensibilität personenbezogener Daten. (Dimension Risikobewertungskompetenz)
- DSK7: Schüler schätzen den Wirkradius und die Gefahr (selbst-)veröffentlichter (persönlicher) Daten ab. (Dimension Urteilskompetenz)
- DSK8: Schüler bewerten den Datenschutz im Bereich der Social Media und ziehen Rückschlüsse für das eigene Verhalten. (Dimensionen Risikobewertungskompetenz und Urteilskompetenz)
- DSK11: Schüler bewerten das Ausmaß von Kenntnissen persönlicher Informationen durch Dritte und reagieren angemessen. (Dimensionen Urteilskompetenz und Handlungskompetenz)
- DSK16: Schüler berücksichtigen Risiken der Internetnutzung und handeln dementsprechend. (Dimension Handlungskompetenz)
- DSK17: Schüler nutzen kostenlose Alternativen (gegenüber kostenpflichtigen Produkten) aus dem Internet. (Dimension Auswahl- und Nutzungskompetenz)

Um die Förderung der Datenschutzkompetenz, das Hauptziel, zu erreichen, teilt Savelsberg die Reihe in verschiedene Einheiten, die unterschiedliche Lernziele verfolgen.

Phase	Inhalte
Einheit 1: Einstieg	• „Schüler nutzen *InstaHub* sachgerecht. • Schüler entnehmen vorgegebenen Profilen alle Informationen und sortieren diese entsprechend.“ (Savelsberg 2019, S. 49)
Einheit 2: Das sichere Profil	• „Schüler unterscheiden zwischen positiven und negativen Kriterien für ein Onlineprofil. • Schüler bewerten ein vorgegebenes Profil anhand einer Kriterienliste und begründen ihre Entscheidung.“ (Savelsberg 2019, S. 52)
Einheit 3 – 4: Passwortsicherheit	• „Schüler benennen schützenswerte Informationen eines Profils. • Schüler nutzen Werkzeuge, um die Passwortsicherheit zu überprüfen. • Schüler erstellen sichere Passwörter. • Schüler nennen Schadsoftwarearten und ihre Eigenschaften. • Schüler nennen Zusammenhänge zwischen Schadsoftware und Passwortsicherheit.“ (Savelsberg 2019, S. 55)
Einheit 5 – 6: Nutzungsbedingungen & Co	• „Schüler benennen Eigenschaften der Nutzungsbedingungen, Datenschutzrichtlinien und Cookie-Richtlinien eines Sozialen Netzwerks. • Schüler nutzen und kennen Privatsphäre-Einstellungen innerhalb eines Sozialen Netzwerks. • Schüler benennen Eigenschaften von User-Tracking und Cookies und erläutern die Zusammenhänge. • Schüler nutzen eine Mind-Map zur Visualisierung ihrer Informationen.“ (Savelsberg 2019, S. 58)
Einheit 7 – 8: Sicher im Netz unterwegs	• „Schüler nennen verschiedene Datenschutz-Plug-Ins. • Schüler nennen Eigenschaften, Vorteile sowie Nachteile verschiedener Datenschutz-Plug-Ins. • Schüler installieren ein Plug-In für den eigenen Browser und nutzen dieses.“ (Savelsberg 2019, S. 61)
Exkurs: Datenbanken in InstaHub	• „Schüler modellieren Datenbanken in einem ERM-ähnlichen Modell. • Schüler lesen Daten aus einer Datenbanktabelle aus. • Schüler nutzen Selektion zum Auslesen der Tabellen. • Schüler löschen, verändern und fügen Daten in Tabellen ein.“ (Savelsberg 2019, S. 64)

Tab. 5.2: Lernziele der Einheiten der Unterrichtsreihe

Die Konzeption der Reihe ergibt sich aus der folgenden Übersicht:

Teilbereich der Reihe		**Inhalt**
Datenschutz in Sozialen Netzwerken	aus Sicht der Anwender	Welche Informationen sind schützenswert? Was ist ein sicheres Profil? Bewertung von gegebenen Profilen
	aus Sicht der Sozialen Netzwerke	Was sind Nutzungsbedingungen? Wo finde ich diese? Welche Schutzmaßnahmen bieten mir Soziale Netzwerke? Warum sammeln diese meine Daten?
Browsersicherheit/ Sicherheit im Netz		Wie werden Daten gesammelt (u. a. User Tracking)? Welche Möglichkeiten habe ich, um mich im Internet generell abzusichern (Plug-Ins, Proxyserver, Browserindividualisierung, …)? Wissen um Tools, Nutzen von Tools
Exkurs: Datenbanken	Nutzen und Modellieren von Datenbanken	Wie werden Daten gespeichert? Modellbildung, Nutzen von InstaHub mit SQL-Befehlen per Dropdown-Menü

Tab. 5.3: Konzeption der Unterrichtsreihe (Savelsberg 2019, S. 44)

Die Begründung des Datenschutzes bildet den Einstieg in die Reihe. Ziel ist es, selbst ein Gefühl zu bekommen, dass eventuell schon preisgegebene Daten schützenswert sind. Unter Verwendung von InstaHub werden diverse Profile bewertet, wozu ein zuvor entwickelter Kriterienkatalog für ein sicheres Profil, das öffentlich ist, als Basis dient. Abschließend sollen die Schüler in der Lage sein, das eigene Profil in einem realen Sozialen Netzwerk einzuschätzen und gegebenenfalls notwendige Änderungen vorzunehmen.

Durch die Auseinandersetzung mit Nutzungsbedingungen Sozialer Netzwerke und das Sammeln persönlicher Daten der Anwender kann der Datenschutzaspekt von der Seite des Betreibers eines Sozialen Netzwerks beleuchtet werden. Dabei werden die Optionen zum Schutz berücksichtigt, die dem Nutzer zur Verfügung stehen. Durch eigene Recherche sollen die Informationen zusammengetragen werden.

Der nächste Block betrachtet die generelle Sicherheit im Internet. Durch die Vorstellung von Tools und Plug-Ins für den Browser (Browserindividualisierung) erhalten die Lernenden eine Zusammenstellung, aus denen sie für sich passende Elemente auswählen können. Dadurch, dass die Schüler diese Tools und Plug-Ins selber testen, können sie die Vor- und Nachteile herausarbeiten und abschließend bewerten.

Der dritte Kernpunkt, der ein Exkurs darstellt, bildet das Thema *Datenbanken* mit den Schwerpunkten der Nutzung, der Modellierung und der Arbeitsweise. Unter Verwendung einer vereinfachten Oberfläche sollen mit Hilfe von InstaHub einfache Operationen auf die Datenbanktabelle angewendet werde. Aufgrund der Komplexität des Gegenstands wird auf die Thematisierung der Sicherheit von Datenbanksystemen verzichtet.

Die ersten beiden Unterrichtseinheiten der Reihe wurden an einem Tag in je einer Doppelstunde in zwei Klassen einer 5. Jahrgangsstufe im Rahmen des ITG-Unterrichts eines Gymnasiums durchgeführt. Aufgrund schulischer Vorgaben konnte der Student nicht die gesamte Reihe durchlaufen.

Savelsberg stellt fest, dass „das Thema [in der ersten Lerngruppe] sehr gut von den Schülern angenommen wurde und vermeintliche Einstiegsschwierigkeiten, durch fehlende Vorkenntnisse im Bereich des Datenschutzes, ausblieben. Dennoch wurde klar, dass besonders die Aufgabenstellungen aufgrund ihrer Formulierung ein Hindernis darstellten“ (Savelsberg 2019, S. 68). Die Nutzung von InstaHub stellte keine Probleme dar, wobei in der zweiten Lerngruppe stärker mit der Plattform gespielt statt gearbeitet worden ist. Für diese Gruppe sind die Aufgaben nach dem ersten Unterrichtsversuch zur Vermeidung von Verständnisproblemen überarbeitet worden. Da diese Klasse als die schwächere der Beiden von dem Fachlehrer charakterisiert worden ist, konnte das Ziel der Doppelstunde nicht ganz erreicht werden. Jedoch zeigte sich wie in der Gruppe zuvor eine durch das Thema motivierte Gruppe. Eine Evaluation der gesamten Reihe steht noch aus.

Eine Weiterentwicklungsmaßnahmen der Unterrichtsreihe (Savelsberg 2019, S. 70) ist die Vereinfachung der Aufgabenstellungen (gegebenenfalls mit Verdeutlichung durch Screenshots und Symbolen) auf den Arbeitsblättern.[179] Zudem würden wegen des Alters der Schüler eine farbliche Gestaltung und eine Integration von Grafiken die Arbeitsblätter visuell qualitativ aufwerten. Die Hilfestellung auf den Arbeitsblättern könnten optional auf Karteikarten geschrieben werden, die bei Bedarf an die Schüler abgegeben werden, sodass eine übersichtlichere Binnendifferenzierung möglich wird. Da die Diskussionen durch die Lehrkraft teilweise erst initiiert werden mussten, ist ein Vorschlag, die Profilbeschreibungen in InstaHub provokativer zu formulieren. Dadurch kann erreicht werden, dass die Lernenden die Problematik des Umgangs mit persönlichen Daten besser erkennen. Zudem ist eine inhaltliche Erweiterung des Themas *Schadsoftware* angedacht. Die Installation und Nutzung von Browser-Plug-Ins beispielsweise könnten im Sinne einer Flipped-Classroom-Methode durch Lernvideos vermittelt werden.

5.1.3. Soziale Netzwerke und Relationen unter Verwendung von *InstaHub*

Die Ausgangsidee dieser Masterarbeit ist die Frage, wie in Sozialen Netzwerken Freundschaftsvorschläge für Nutzer entstehen. (Biehl 2019) beschreibt eine Möglichkeit, dem unter Verwendung von InstaHub nachzugehen, wobei dafür mathematische Relationen eine Grundlage bilden. „Um ein reflektiertes Verhalten von Schülerinnen und Schülern in Sozialen Netzwerken und dem Internet im Allgemeinen zu schulen, wird … eine Unterrichtsreihe beschrieben, welche die Funktionsweise Sozialer Netzwerke, die dort vorliegenden Verknüpfungen

[179] Teilweise ist dies auf den Arbeitsblättern in (Savelsberg 2019) schon geschehen.

(Relationen) und den Umgang mit persönlichen Daten behandelt“ (Biehl 2019, S. 6). Eine Erweiterung für *InstaHub* wurde erstellt, um die Relationen zu visualisieren.

Dabei stehen insbesondere folgende zu fördernden Kompetenzen im Vordergrund (vgl. Tab. 3.8):

- DSK1: Schüler kennen Grundbegriffe im Umgang mit Internetnutzung. (Dimension Wissen)
- DSK5: Schüler kennen Maßnahmen, um das Internet-Surfverhalten zum eigenen Schutz anzupassen, und wenden technische und weitere Maßnahmen zur sicheren Internetnutzung an. (Dimensionen Wissen und Handlungskompetenz)
- DSK6: Schüler bewerten die Sensibilität personenbezogener Daten. (Dimension Risikobewertungskompetenz)
- DSK7: Schüler schätzen den Wirkradius und die Gefahr (selbst-)veröffentlichter (persönlicher) Daten ab. (Dimension Urteilskompetenz)
- DSK8: Schüler bewerten den Datenschutz im Bereich der Social Media und ziehen Rückschlüsse für das eigene Verhalten. (Dimensionen Risikobewertungskompetenz und Urteilskompetenz)
- DSK10: Schüler beurteilen den Missbrauch von Online-Konten (wie z. B. E-Mail, Banking, Einkauf und Dienstleistungen). (Dimension Risikobewertungskompetenz)
- DSK11: Schüler bewerten das Ausmaß von Kenntnissen persönlicher Informationen durch Dritte und reagieren angemessen. (Dimensionen Urteilskompetenz und Handlungskompetenz)
- DSK12: Schüler bewerten die Gefahren bei der Online-Kommunikation (z. B. durch Mailen, Chatten und Surfen) und reagieren angemessen. (Dimensionen Risikobewertungskompetenz und Handlungskompetenz)
- DSK16: Schüler berücksichtigen Risiken der Internetnutzung und handeln dementsprechend. (Dimension Handlungskompetenz)

Innerhalb der Arbeit werden drei Unterrichtsentwürfe zu den Themen *Relationen*, *Soziale Netzwerke* und *Datenschutz* beschrieben. Da Relationen in dem heutigen Mathematikunterricht nicht mehr thematisiert werden, werden die Grundlagen dazu vorneweg gestellt.

Die Lernziele für die Einheit *Relationen* lauten:

- „Die Schülerinnen und Schüler geben die Definition der zweistelligen Relation wieder.
- Die Schülerinnen und Schüler erkennen Relationen im Alltag und in der Mathematik als solche und weisen ihnen die entsprechenden Relationseigenschaften zu.
- Die Schülerinnen und Schüler nutzen verschiedene Darstellungsformen von Relationen.
- Die Schülerinnen und Schüler beschreiben Datensätze in verteilten Tabellen, stellen die relationalen Eigenschaften heraus und nennen die Vor- und Nachteile, die Datensätze auf kleiner Tabellen zu verteilen.“ (Biehl 2019, S. 9)

Nach einem problemorientierten Einstieg zu einer Gruppenbildung werden die Relationseigenschaften vorgestellt und durch Übungen in Partnerarbeit gefestigt. Dem schließen sich Darstellungsformen von Relationen und Verknüpfungen zwischen Relationen an.

Die Einheit *Relationen* kann durch einen Kurs mit dem Thema *relationale Datenbanken und Abfragen mit SQL* und durch Entity-Relationship-Diagrammen vertieft werden. Aus mathematischer Sicht könnten weitere Relationseigenschaften wie Asymmetrie, Eindeutigkeiten und Totalitäten angesprochen werden, um den Zusammenhang zum Funktionsbegriff herzustellen.

Die Lernziele für die Einheit *Soziale Netzwerke* lauten:

- „Die Schülerinnen und Schüler beschreiben den Zusammenhang zwischen der Anzahl an Verbindungen in einem Sozialen Netzwerk und der dargestellten Relation.
- Die Schülerinnen und Schüler unterscheiden Informationen, welche in der Administrator- oder Nutzeransicht eines Sozialen Netzwerks verfügbar sind.
- Die Schülerinnen und Schüler lesen Informationen aus einem Netzwerkgraphen aus.
- Die Schülerinnen und Schüler erklären, wie anhand von Daten neue Informationen gewonnen werden können.“ (Biehl 2019, S. 29)

Nach der Vorstellung der Funktionsweise der InstaHub-Erweiterung *InstaHubRelations* durch die Lehrkraft nutzen die Lernenden unter Verwendung eines Arbeitsblattes das Tool. In einem ersten Schritt werden die in der ersten Einheit erarbeiteten Begriffe und Zusammenhänge auf InstaHubRelations angewendet. Danach laden die Schüler die Netzwerkgraphen ihres Hubs, um darin die Freundschaftszusammenhänge zwischen den Nutzern zu identifizieren und durch Manipulationen im Sinne des Administrators, den sie vertreten, zu beeinflussen. Überlegungen, wie Nutzer für Werbung ausgesucht werden, wie die Anzahl von Klicks auf Werbeanzeigen erhöht werden kann und wie Informationen, die Administratoren von Sozialen Netzwerken benötigen, um passende Werbung zu schalten, runden die Einheit ab. Der letzte Aspekt führt direkt in die letzte Einheit über.

Sowohl aus informatischer als auch mathematischer Sicht stellt das Thema *Graphentheorie* eine interessante Erweiterung dar. Eine Vertiefung des Themas Netzwerke und/oder die technische Umsetzung Sozialer Netzwerke wären andere Anschlussalternativen.

Die Lernziele für die Einheit *Datenschutz* lauten:

- „Die Schülerinnen und Schüler identifizieren persönliche Daten, welche über sie gesammelt werden und ziehen Schlussfolgerungen über die daraus ableitbaren persönlichen Informationen.
- Die Schülerinnen und Schüler benennen und erklären Risiken und Gefahren im Zusammenhang mit persönlichen Informationen.
- Die Schülerinnen und Schüler kennen und nutzen Software/Tools, um den Risiken und Gefahren entgegenzuwirken.
- Die Schülerinnen und Schüler reflektieren ihren eigenen Umgang mit Sozialen Netzwerken und Anwendungen kritisch.“ (Biehl 2019, S. 40)

Zu Beginn der Einheit erhalten die Schüler je nach Gruppenzuweisung für die Gruppenarbeit die Kontoauszüge, die Bewegungsdaten oder eine Liste der Webaktivitäten eines InstaHub-Nutzers, dessen Profil sie in InstaHub einsehen können. Die Aufgabe ist es, auf Basis der für die Gruppenarbeit ausgegebenen Informationen das Nutzer-Profil zu vervollständigen und die Tätigkeiten über einen Zeitraum von zwei Wochen zu protokollieren. Dadurch wird eine Sensibilisierung erzeugt, wenn personenbezogene Daten öffentlich werden. In einer zweiten Phase findet eine Recherche zu Schutzsoftware und deren Einsatzmöglichkeiten statt.

Themen wie *Big Data und Data Mining* oder *informationelle Selbstbestimmung und DSGVO* bieten Vertiefungs- und Erweiterungsmöglichkeiten an.

Da eine Erprobung dieser Unterrichtsreihe noch nicht vorliegt, können an dieser Stelle keine Evaluationsergebnisse vorgestellt werden. (Biehl 2019, S. 59) nennt abschließend Möglichkeiten das für die Sekundarstufe II konzipierte Setting in die Mittelstufe zu übertragen und verweist dabei auch auf (Savelsberg 2019) und (Thielen 2018). Für die Weiterentwicklung von InstaHub sind noch weitere Punkte vorgesehen wie ein „dynamisches Auslesen der Datenbank, sodass Änderungen im Sozialen Netzwerk direkt dargestellt werden können, eine Suchfunktion zum schnelleren Auffinden bestimmter Knoten im Netzwerkgraphen, unterschiedliche Ansichten für Administrator und Netzwerknutzer [und die Darstellung von] Prestige und Zentralität der Nutzer … statt in der Tabelle im Graphen“ (Biehl 2019, S. 71).

5.1.4. Weiterentwicklung der Newsfeeds-Funktion in *InstaHub* und Entwicklung einer Sek. II-Unterrichtsreihe zum Thema *Personalisierte Algorithmen in Sozialen Netzwerken*

Hintergrund dieses Projekts ist die Frage der Funktionsweise von Personalisierten Algorithmen und die Entstehung von Filterblasen. Durch die Verwendung des Sozialen Netzwerks *InstaHub* kann anhand der Newsfeeds kontextorientiert in das Thema eingeführt werden.

Durch diese Unterrichtsreihe sollen insbesondere folgende Datenschutzkompetenzen gefördert werden (vgl. Tab. 3.8):

- DSK4: Schüler wissen um das Verhalten (insb. nicht-europäischer) Unternehmen, personenbezogene Daten anderweitig als für den vorgesehenen Zweck zu verwenden. (Dimension Wissen)
- DSK5: Schüler kennen Maßnahmen, um das Internet-Surfverhalten zum eigenen Schutz anzupassen, und wenden technische und weitere Maßnahmen zur sicheren Internetnutzung an. (Dimensionen Wissen und Handlungskompetenz)
- DSK6: Schüler bewerten die Sensibilität personenbezogener Daten. (Dimension Risikobewertungskompetenz)
- DSK7: Schüler schätzen den Wirkradius und die Gefahr (selbst-)veröffentlichter (persönlicher) Daten ab. (Dimension Urteilskompetenz)

- DSK8: Schüler bewerten den Datenschutz im Bereich der Social Media und ziehen Rückschlüsse für das eigene Verhalten. (Dimensionen Risikobewertungskompetenz und Urteilskompetenz)
- DSK11: Schüler bewerten das Ausmaß von Kenntnissen persönlicher Informationen durch Dritte und reagieren angemessen. (Dimensionen Urteilskompetenz und Handlungskompetenz)
- DSK16: Schüler berücksichtigen Risiken der Internetnutzung und handeln dementsprechend. (Dimension Handlungskompetenz)

Als Lernziele für die Reihe nennt (Steil 2019, S. 33): „Die Schüler …

- beobachten und beschreiben die Auswirkungen ihres Nutzungsverhaltens auf den Newsfeed in Sozialen Netzwerken, …
- erläutern die Begriffe … Algorithmische Personalisierung,
- nennen Faktoren, die die Sortierung der Feed-Beiträge beeinflussen, …
- erläutern, wieso ein und dieselbe Google-Suchanfrage bei verschiedenen Nutzern unterschiedliche Ergebnisse liefert …
- erläutern, wie bestimmte Daten die Ergebnisse der Google-Suche beeinflussen, …
- nennen Vor- und Nachteile Algorithmischer Personalisierung,
- bewerten den Einsatz Algorithmischer Personalisierung bei Google, Amazon und in Sozialen Netzwerken,
- erläutern den Begriff *Filterblase*,
- beurteilen die Gefahren, die durch eine Filterblase entstehen können, …
- zeigen Wege auf, um sich über einen Sachverhalt differenziert zu informieren."

Die Unterrichtsreihe ist so konzipiert, dass die Schüler durch die Analyse von Google-Suchergebnissen an das Thema der Personalisierten Algorithmen herangeführt werden. Nachdem erste Vermutungen erarbeitet worden sind, setzen sich die Lernenden mit den Newsfeeds und deren Darstellung in InstaHub auseinander. Durch die Bestimmung von Einflussfaktoren auf die Newsfeed-Sortierung formulieren die Schüler einen Pseudocode-Algorithmus, der dem EdgeRank-Algorithmus von *Facebook* nachempfunden ist. Mit diesem Hintergrundwissen können der Begriff *Filterblase* und die Auswirkungen dessen zur Diskussion gestellt werden. Die Festigung der Thematik erfolgt durch ein Schreibgespräch, indem der Schutz vor Datenmissbrauch und Filterblase und die Folgen der personalisierten Algorithmisierung in Zentrum stehen. Durch einen Filmbeitrag zum Einfluss von Cambridge Analytica auf die US-Präsidentschaftswahlen 2016 wird das Thema abgeschlossen.

Am Ende der Unterrichtsreihe, die in einem GK Informatik 13 gehalten worden ist, fand eine schriftliche Befragung der Schüler zu dieser Reihe statt. Insgesamt gab es eine positive Rückmeldung, da die Lernenden an Themen im Zusammenhang mit Sozialen Medien (Themenbereich *Datenschutz und Filterblase*) wegen der Alltagsrelevanz und der persönlichen Betroffenheit sehr interessiert waren. „Ein erweitertes Wissen auf diesem Gebiet könnte auch zu einer veränderten und differenzierteren Wahrnehmung bestimmter Internetseiten führen. Dies war laut Feedback nach der durchgeführten Unterrichtseinheit noch nicht der Fall" (Steil 2019, S. 50). Die Analyse personalisierter Suchergebnisse fand die Gruppe interessant, ebenso wie die

Formulierung des Pseudocodes und die beispielhafte Analyse sozialer Netzwerke. Jedoch galt der Einsatz von InstaHub als wenig gelungen, was an den technischen Problemen innerhalb der Stunde und den unzureichenden Kenntnissen der Schüler mit diesem Werkzeug lag. Durch Ausprobieren in InstaHub könnten die Lernenden die Sortierkriterien selber entdecken. Die viele Partnerarbeit (starke Schülerorientierung) wurde als positiv herausgestellt, das Schreibgespräch fand nicht bei allen Schülern Anklang.

„Gespalten waren die Meinungen bei der Frage, ob ihnen durch algorithmische Personalisierung Informationen vorenthalten werden. Es ließe sich an Fallbeispielen oder auch mittels Selbstversuch erforschen, inwieweit die Filterblase tatsächlich Einfluss auf den Informationsfluss hat. Das Interesse der Schüler hierfür wäre angesichts der Umfrageergebnisse auf jeden Fall gegeben“ (Steil 2019, S. 51).

Im Rahmen eines Leistungskurses bietet sich die Möglichkeit an, den an den EdgeRank-Algorithmus angelehnten Algorithmus um Suchkriterien wie Seitenbesuche oder Relationen zwischen Nutzern zu erweitern. Auf jeden Fall sind weitere Aspekte rund um das Thema *Datenschutz* stärker zu verknüpfen, da die Jugendlichen sich dies besonders wünschen.

5.1.5. Weiterentwicklung des Planspiels *Datenschutz 2.0*

Das in Abschnitt 2.4 vorgestellte Planspiel *Datenschutz 2.0*, welches vor gut zehn Jahren entwickelt worden ist, stellt einen Beitrag innerhalb des IniK-Projekts[180] dar. Es ist zum jetzigen Zeitpunkt im Unterricht so nicht mehr einsetzbar, da einerseits aufgrund der DSGVO das Abspeichern der E-Mail-Adressen nicht mehr gesetzeskonform ist und andererseits die PHP-Version, in der das Planspiel programmiert ist, nicht mehr vom Provider unterstützt wird. Zudem sind die Rollenbeschreibungen wenig spannend und nicht mehr zeitgemäß. Daher hat sich (Noll 2019, S. 7) die folgenden Fragen gestellt:

- „Wie kann das Planspiel interessanter für die heutige Jugend gemacht und wie könnte dieses umgesetzt werden?
- Wie können die technischen und gesetzlichen Problematiken gelöst werden, sodass das Planspiel wieder genutzt werden kann?“

Die Antwort auf die zweite Frage ist, dass durch eine Aktualisierung des Quellcodes die Lauffähigkeit gesichert und durch eine eindeutige URL des (fiktiven) Providers, der für das Spiel benötigt und durch die Lehrkraft vor Spielbeginn angelegt wird, die Speicherung persönlicher Daten umgangen werden kann.

Die Umsetzung der ersten Frage erfolgte durch Überarbeitung des Designs und der Thematik, um den aktuellen Lebensweltbezug der Schüler herzustellen. Da das Smartphone für die Schüler einen Alltagsgegenstand darstellt, wurde für das Design der Spielphase ein Smartphone gewählt. Die einzelnen Spielstationen, die überarbeitet worden sind, sind in Apps hinterlegt und als Icons auf dem virtuellen Smartphone-Display dargestellt. Die einzelnen aktualisierten

[180] IniK steht für *Informatik im Kontext*; vgl. dazu Abschnitt 2.4.

und überarbeiteten Rollenbeschreibungen sind in eine Rahmenhandlung eingebunden.[181] Abschließend wurde der Spielverlauf den neuen Gegebenheiten angepasst. „Das Planspiel kann in unterschiedlichen Stufen und im Grund- und Leistungsfach unterrichtet werden, da der Schwierigkeitsgrad des Planspiels aufgrund der Einstellbarkeit der Sichten auf die Daten variabel ist“ (Noll 2019, S. 70).

Das Konzept des Planspiels ist geblieben und besteht aus einer Spiel- und einer Auswertungsphase. Jedoch sind beide Phasen im Gegensatz zu der vorangegangenen Version miteinander durch die Rahmenhandlung verzahnt, sodass der Spieleverlauf insgesamt als „flüssiger“ angenommen werden kann. Da einerseits der Zeitansatz für die Anfertigung der Masterarbeit begrenzt war und andererseits zu Beginn der Arbeit einige technische Dinge zu klären gewesen waren, konnte dieses Projekt jedoch nicht im Unterricht umgesetzt werden. Zudem ist zum jetzigen Zeitpunkt das Spiel auch noch nicht lauffähig, da erst noch die geplante Oberfläche programmiert werden muss. Hierzu ist eine Bachelorarbeit im Bereich der Computervisualistik ausgeschrieben.

Folgende Kompetenzen sollen insbesondere durch diese Unterrichtsreihe gefördert werden (vgl. Tab. 3.8):

- DSK1: Schüler kennen Grundbegriffe im Umgang mit Internetnutzung. (Dimension Wissen)
- DSK6: Schüler bewerten die Sensibilität personenbezogener Daten. (Dimension Risikobewertungskompetenz)
- DSK7: Schüler schätzen den Wirkradius und die Gefahr (selbst-)veröffentlichter (persönlicher) Daten ab. (Dimension Urteilskompetenz)
- DSK8: Schüler bewerten den Datenschutz im Bereich der Social Media und ziehen Rückschlüsse für das eigene Verhalten. (Dimensionen Risikobewertungskompetenz und Urteilskompetenz)
- DSK9: Schüler bewerten und beurteilen die Gefahren von ungünstigen Internettätigkeiten (wie z. B. Cybermobbing, Spam-Mail und Trickbetrug). (Dimensionen Risikobewertungskompetenz und Urteilskompetenz)
- DSK11: Schüler bewerten das Ausmaß von Kenntnissen persönlicher Informationen durch Dritte und reagieren angemessen. (Dimensionen Urteilskompetenz und Handlungskompetenz)
- DSK12: Schüler bewerten die Gefahren bei der Online-Kommunikation (z. B. durch Mailen, Chatten und Surfen) und reagieren angemessen. (Dimensionen Risikobewertungskompetenz und Handlungskompetenz)
- DSK16: Schüler berücksichtigen Risiken der Internetnutzung und handeln dementsprechend. (Dimension Handlungskompetenz)

[181] Die Rahmenhandlung ist die Geburtstagsfeier einer 18-jährigen Schülerin, in deren Verlauf einige gesetzwidrige Dinge geschehen, zu deren Aufklärung die Datenspuren der gespielten Rollen herangezogen werden.

Als Ausblick und zur Weiterentwicklung schlägt der Student vor, dass eine Benachrichtigungsfunktion für eingegangene Nachrichten implementiert wird, um den Realitätsbezug zu erhöhen. Zur Erleichterung der Kommunikation wäre eine Integration eines vollständigen Sozialen Netzwerks denkbar, wobei die Nutzungsmöglichkeit von InstaHub[182] in diesem Zusammenhang zu prüfen ist. Das zurzeit im Planspiel integrierte Netzwerk ist sehr einfach gehalten und besitzt eine geringe Funktionalität. In dieses Netzwerk könnte man auch die virtuelle Gastgeberin der Rahmenhandlung einbinden, deren Reaktionen über eine KI gesteuert werden könnten. Hier ist aber der Aufwand der KI-Programmierung zum Nutzen abzuschätzen. „Um mehr Interaktionen zwischen den Rollen zu ermöglichen, müssten die Schüler in den Rollenbeschreibungen mehr Freiheit und die nötigen Funktionen, wie bspw. die Markierungs- oder Teilfunktion, bekommen“ (Noll 2019, S. 71). Gefahr besteht jedoch darin, dass die Lernenden letztendlich ihre Rolle nicht ausreichend spielen, was in der zweiten Spielphase zu Problemen führen würde. Mit Hilfe eines Chatbots könnte das Thema *Cybermobbing* integriert werden, ohne dass ein Schüler die Opferrolle spielen müsste. Zur Erhöhung des Lebensweltbezugs könnten einige Apps (z. B. Web-Shop-App, Suchmaschinen-App und Streaming-App) durch eine im Hintergrund laufende Datenbank so gesteuert werden, dass die Schüler nicht erkennen, dass das Planspiel aus einer simplen Eingabe von Daten basiert. Als letzter Schritt wäre denkbar, das gesamte Spiel in eine reale App zu übertragen, sodass es auch auf einem Smartphone gespielt werden könnte.

5.1.6. Eine Unterrichtsreihe zum Thema *Datenschutz und Datensicherheit* im kontextorientierten Ansatz

Abschließend wird in diesem Kapitel eine Bachelorarbeit vorgestellt, die eine Unterrichtsreihe für die Sekundarstufe II zum Thema *Datenschutz und Datensicherheit* beschreibt. Dabei steht ein kontextorientierter Ansatz im Vordergrund, bei dem die Nutzung von Smartphone-Applikationen als Anlass dient. Die schon existierenden IniK[183]-Reihen *E-Mail (nur) für Dich?* und *Planspiel Datenschutz 2.0* sollen um einen neuen Kontext ergänzt werden.

„Erstes Ziel der Einheit soll sein, dass die Schüler Risiken bei der Smartphone-Nutzung erkennen und vermeiden. … [Es] soll ein Bewusstsein beim Einsatz von mobilen Medien entstehen und nach Möglichkeit anschließend ein bewussteres Nutzungsverhalten bei den Schülern einsetzen“ (Böhm 2015, S. 29). Im Kontext sollen sie „lernen, die Welt durch die informatische Brille zu sehen. Die Selbstverständlichkeit der Nutzung von Informatiksystemen bedarf einer Aufklärung der Nutzer“ (Böhm 2015, S. 48).

[182] InstaHub ist ein für den Schulunterricht entwickeltes Netzwerk zu den Themen *Datenbanken* und *Datenschutz*, wobei im vorliegenden Fall des Planspiels die Schüler nur als Nutzer mit ihren Rollen und nicht als Administratoren fungieren dürfen.

[183] IniK steht für *Informatik im Kontext*; vgl. dazu Abschnitt 2.4.

Da die Abschlussarbeit vor Beginn der finalen Entwicklung des Datenschutzkompetenzmodells entstand, werden an dieser Stelle im Nachgang die Datenschutzkompetenzen gelistet, die durch die Reihe insbesondere gefördert werden (vgl. Tab. 3.8)[184]:

- DSK2: Schüler ordnen den Begriff "Datenschutz-Erklärung" im Kontext der Internetnutzung ein und kennen die daraus abgeleiteten Rechte und Pflichten. (Dimension Wissen)
- DSK4: Schüler wissen um das Verhalten (insb. nicht-europäischer) Unternehmen, personenbezogene Daten anderweitig als für den vorgesehenen Zweck zu verwenden. (Dimension Wissen)
- DSK5: Schüler kennen Maßnahmen, um das Internet-Surfverhalten zum eigenen Schutz anzupassen, und wenden technische und weitere Maßnahmen zur sicheren Internetnutzung an. (Dimensionen Wissen und Handlungskompetenz)
- DSK6: Schüler bewerten die Sensibilität personenbezogener Daten. (Dimension Risikobewertungskompetenz)
- DSK7: Schüler schätzen den Wirkradius und die Gefahr (selbst-)veröffentlichter (persönlicher) Daten ab. (Dimension Urteilskompetenz)
- DSK10: Schüler beurteilen den Missbrauch von Online-Konten (wie z. B. E-Mail, Banking, Einkauf und Dienstleistungen). (Dimension Risikobewertungskompetenz)
- DSK11: Schüler bewerten das Ausmaß von Kenntnissen persönlicher Informationen durch Dritte und reagieren angemessen. (Dimensionen Urteilskompetenz und Handlungskompetenz)
- DSK12: Schüler bewerten die Gefahren bei der Online-Kommunikation (z. B. durch Mailen, Chatten und Surfen) und reagieren angemessen. (Dimensionen Risikobewertungskompetenz und Handlungskompetenz)
- DSK15: Schüler wenden Maßnahmen zum Schutz von Zugängen (zu Systemen, Portalen, …) an. (Dimension Handlungskompetenz)
- DSK16: Schüler berücksichtigen Risiken der Internetnutzung und handeln dementsprechend. (Dimension Handlungskompetenz)
- DSK17: Schüler nutzen kostenlose Alternativen (gegenüber kostenpflichtigen Produkten) aus dem Internet. (Dimension Auswahl- und Nutzungskompetenz)

Als Lernziele formuliert (Böhm 2015, S. 33):

- „Die Schüler sollen Datenerhebung unter dem Aspekt Datenschutz bewerten.
- [Die Schüler sollen] Datensicherheit unter Berücksichtigung kryptologischer Verfahren erklären und beachten.
- [Die Schüler sollen] Qualitätsmerkmale für Software kennen und beachten.
- Sie sollen die Funktionsweise von Smartphones und deren Apps beschreiben können.
- [Die Schüler sollen] die Qualität von Applikationen bezüglich des Datenschutzes [erkennen] und [bewerten].

[184] In den vorangegangenen Fällen fand die Zuordnung der Datenschutzkompetenzen im Rahmen der Entwicklung der Unterrichtsreihe statt; wegen des frühen Zeitraums der beschriebenen Reihe findet die Zuordnung im Nachhinein statt.

- Die Schüler [sollen] die Sicherheit der von ihnen betriebenen Kommunikation einschätzen können.
- [Die Schüler sollen] durch eine kritische Betrachtung von Datenerhebung … die Gefahren des Missbrauchs ihrer personenbezogenen Daten erkennen, sowie den Schutz dieser Daten durch die Verwendung sicherer Apps verbessern können. Dies bezieht sich auch auf den Umgang mit den mobilen Geräten und deren Anwendungsmöglichkeiten, die sie verantwortungsvoll einsetzen sollen."

Die Unterrichtsreihe gliedert sich der IniK-Vorlage folgend in vier Phasen. Die erste Phase, die Begegnungsphase, trägt den Titel *Spionage mit dem Smartphone*. Aus der eigenen Erfahrung sollen die Lernenden Probleme benennen, die sie durch die Smartphone-Nutzung kennen.[185] Mit Bezug darauf sind die Begriffe *Datenschutz* und *Datensicherheit* voneinander abzugrenzen. Mit der Fokussierung auf den Datenschutz wird mittels eines Videos „die Möglichkeit der Überwachung einer Person mit Hilfe seines Smartphones thematisiert" (Böhm 2015, S. 36). Die Schüler erhalten in einer differenzierten Gruppenarbeit auf Basis des Videobeitrags die Aufträge, einerseits die von der Spionage-App gesammelten Daten festzuhalten und andererseits die Begründung eines Wanzen-Vorwurfs und die Dateninteressenten zu nennen. Anhand des entworfenen Tafelbilds kann das Sicherheitsziel der Vertraulichkeit von Kommunikation entwickelt werden.

Mit dem Titel *Apps im Sandkasten* ist die zweite Phase, die Neugier- und Planungsphase, überschrieben. Durch das Konzept der Sandbox und der Rechtevergabe lernen die Schüler das Zusammenspiel zwischen App und Betriebssystem kennen. Unter Verwendung eines Videos, das App-Berechtigungen erklärt, wägen die Lernenden die Vor- und Nachteile des Sandbox-Prinzips ab. Durch Verwendung der App *aSpotCat* überprüfen sie nun die Rechtevergabe an Apps auf dem eigenen Smartphone, wodurch die Betroffenheit verstärkt werden kann. Um die Datenschutzrechte zu thematisieren, werden in einer differenzierten Gruppenarbeit folgende Aspekte behandelt: „(1) Sicherheit von öffentlichen Hotspots bzw. unbekannten WLAN-Netzwerken, (2) Standortbestimmung durch GPS und Netzwerke, (3) Sicherheit von Verbindungstechniken (z. B. Bluetooth) [und] (4) Softwareupdates, Sicherheit des Play Store und Malware" (Böhm 2015, S. 38). In einem abschließenden Rollenspiel in Form einer Podiumsdiskussion wird das erworbene Wissen genutzt, um den Vorwurf gegen *WhatsApp* als Superwanze zu bewerten.

Innerhalb der Erarbeitungsphase *Vertraulichkeit herstellen* werden zu Beginn Fremdzugriffschutz durch Passwörter und die Verschlüsselung bei *WhatsApp* thematisiert. Die Qualität von Passwörtern kann über ein Tool zum Passwort-Check geprüft werden, wobei für das Problem des Versands im Klartext sensibilisiert wird. Presseberichte zur Entschlüsselung von WhatsApp-Nachrichten dienen zur Diskussion über die Sicherheitsziele *Authentizität* und *Integrität* von Nachrichten. Wegen der Vielzahl an Apps müssen die Schüler lernen, die Qualität der Produkte zu beurteilen. Anhand ausgewählter App-Arten (wie z. B. Prozessüberwachung, Fernzugriff und Virenscanner) können die Lernenden in Partnerarbeit dies üben und im Kurs diskutieren.

[185] Diese können durch die im BSI-Katalog genannten Gefährdungslagen bei der Nutzung ergänzt werden.

Mit der berühmten Aussage *Ich habe nichts zu verbergen!* wird die vierte Phase, die Vernetzungs- und Vertiefungsphase betitelt. „Selbst wenn die Möglichkeiten gegeben sind, ausgespäht zu werden, bedeutet dies nicht, dass jeder Schüler die Notwendigkeit erkennt, sein Verhalten bezüglich der Preisgabe seiner Daten zu ändern“ (Böhm 2015, S. 42). Anhand eines *Sixtus vs. Lobo*-Videobeitrags können die Argumente für oder wider der Netztransparenz vorgestellt werden, um die Interessenten an Daten und deren Motive zu besprechen. Zur Diskussion stehen im Weiteren Themen wie *Staatstrojaner*, *PRISM*, *Vorratsdatenspeicherung* und *informationelle Selbstbestimmung*. Wichtig ist hierbei aufzuzeigen, wie anhand diverser Informationsquellen durch Selbststudium Sachverhalte und Zusammenhänge recherchiert werden können. „Abschließend sollen eine Reflexion und Bewertung der Inhalte dieser Reihe erfolgen, sowie deren Bedeutung in weiteren Lebensbereichen festgestellt werden“ (Böhm 2015, S. 42).

Da die vorgestellte Unterrichtsreihe aus Zeitgründen des Studenten nicht durchgeführt worden ist, liegen auch keine Erfahrungen über die Umsetzung vor. Anpassungsvorschläge für die Sekundarstufe I sind eine Überarbeitung der Materialien in einem geringen Aufwand, da sie von *klicksafe*[186] „in verschiedenen Schwierigkeitsgraden zur Verfügung stehen“ (Böhm 2015, S. 44). Offen bleibt jedoch die Frage, in welchem Fach die Thematisierung erfolgen soll (insbesondere auch im Hinblick auf die häufig nicht ausreichende Expertise der Lehrkräfte).

Anknüpfungspunkte dieser Reihe sind die schon existierenden IniK-Reihen *E-Mail (nur?) für Dich* und *Planspiel Datenschutz 2.0*, die aufgrund der vermehrten Nutzung von Smartphones dementsprechend aktualisiert werden könnten. Eine Erweiterung der Reihe kann durch Themen wie *Angriffsmethoden auf Passwörter*, *verschiedene Arten von Schadprogrammen*, *Arbeitsweise von Betriebssystemen*, *E-Commerce und Datensicherheit*, *Big Data und Datenbanken*, *Wirtschaftsspionage*, *Personenüberwachung*, *der Interessenkonflikt von Geheimdiensten bezüglich des Schutzes persönlicher Daten* oder *dem Bestreben von Krankenkassen, Gesundheitsapps zu nutzen* erfolgen. Im Sinne eines fächerverbindenden Unterrichts können Verbindungen zu den Fächern Mathematik (Sicherheit von Passwörtern), Physik (Datenübertragung) und Sozialkunde (informationelle Selbstbestimmung) hergestellt werden.

[186] Siehe www.klicksafe.de (zuletzt geprüft am 22.11.19).

5.2. Zusammenfassung

In dem vorliegenden Kapitel wurden sechs studentische Abschlussarbeiten im schulpraktischen Umfeld zur Förderung der Datenschutzkompetenz vorgestellt. Diese Projekte sind unabhängig voneinander entstanden und stehen in keinem direkten Bezug zueinander, wobei in drei Fällen *InstaHub* genutzt worden ist.

Alle sechs Projekte zielen darauf ab, folgende Datenschutzkompetenz zu fördern:

- DSK6: Schüler bewerten die Sensibilität personenbezogener Daten. (Dimension Risikobewertungskompetenz)
- DSK7: Schüler schätzen den Wirkradius und die Gefahr (selbst-)veröffentlichter (persönlicher) Daten ab. (Dimension Urteilskompetenz)
- DSK11: Schüler bewerten das Ausmaß von Kenntnissen persönlicher Informationen durch Dritte und reagieren angemessen. (Dimensionen Urteilskompetenz und Handlungskompetenz)
- DSK16: Schüler berücksichtigen Risiken der Internetnutzung und handeln dementsprechend. (Dimension Handlungskompetenz)

In fünf Projekten spielt die Datenschutzkompetenz DSK5 eine Rolle:

- DSK5: Schüler kennen Maßnahmen, um das Internet-Surfverhalten zum eigenen Schutz anzupassen, und wenden technische und weitere Maßnahmen zur sicheren Internetnutzung an. (Dimensionen Wissen und Handlungskompetenz)

Folgende Kompetenzen werden in vier Projekten gefördert:

- DSK1: Schüler kennen Grundbegriffe im Umgang mit Internetnutzung. (Dimension Wissen)
- DSK8: Schüler bewerten den Datenschutz im Bereich der Social Media und ziehen Rückschlüsse für das eigene Verhalten. (Dimensionen Risikobewertungskompetenz und Urteilskompetenz)

In der Hälfte der Projekte zählen folgende Kompetenzen zur Förderung:

- DSK2: Schüler ordnen den Begriff "Datenschutz-Erklärung" im Kontext der Internetnutzung ein und kennen die daraus abgeleiteten Rechte und Pflichten. (Dimension Wissen)
- DSK4: Schüler wissen um das Verhalten (insb. nicht-europäischer) Unternehmen, personenbezogene Daten anderweitig als für den vorgesehenen Zweck zu verwenden. (Dimension Wissen)
- DSK12: Schüler bewerten die Gefahren bei der Online-Kommunikation (z. B. durch Mailen, Chatten und Surfen) und reagieren angemessen. (Dimensionen Risikobewertungskompetenz und Handlungskompetenz)

In zwei Projekten spielen die folgenden Datenschutzkompetenzen eine Rolle:

- DSK10: Schüler beurteilen den Missbrauch von Online-Konten (wie z. B. E-Mail, Banking, Einkauf und Dienstleistungen). (Dimension Risikobewertungskompetenz)

- DSK15: Schüler wenden Maßnahmen zum Schutz von Zugängen (zu Systemen, Portalen, …) an. (Dimension Handlungskompetenz)
- DSK17: Schüler nutzen kostenlose Alternativen (gegenüber kostenpflichtigen Produkten) aus dem Internet. (Dimension Auswahl- und Nutzungskompetenz)

Folgende Kompetenzen werden in je einem Projekt gefördert:

- DSK3: Schüler geben ihre Rechte aus der informationellen Selbstbestimmung an. (Dimension Wissen)
- DSK9: Schüler bewerten und beurteilen die Gefahren von ungünstigen Internettätigkeiten (wie z. B. Cybermobbing, Spam-Mail und Trickbetrug). (Dimensionen Risikobewertungskompetenz und Urteilskompetenz)

Aus der Liste der in Tab. 3.8 genannten Kompetenzen sind Folgende durch die vorgestellten Projekte nicht abgedeckt:

- DSK13: Schüler bewerten und beurteilen die Risiken einer unbemerkten Infektion durch Schadsoftware. (Dimensionen Risikobewertungskompetenz und Urteilskompetenz)
- DSK14: bewerten die Gefahren durch unüberlegte Handlungen (z. B. Anklicken von Links in Mails, Ausführen von Downloads und Anklicken von Werbeanzeigen). (Dimension Urteilskompetenz)

Drei Projekte stehen durch das Werkzeug *InstaHub* in Zusammenhang zueinander und können eine größere Einheit darstellen. Das Projekt *Planspiel Datenschutz 3.0* könnte nach Fertigstellung mit InstaHub verknüpft werden. Dorn, der Entwickler von InstaHub, hat aber gegenüber dem Autor Bedenken geäußert, zu viele Fragestellungen und Probleme mit InstaHub zu bearbeiten. Er befürchtet, dass ein zu mächtiges Tool am Ende wegen seiner Unübersichtlichkeit dann nur noch selten genutzt werden würde. Auch wenn alle Projekte sich letztendlich um die Förderung der Datenschutzkompetenz durch den Informatikunterricht bemühen, so müssen immer die Rahmenbedingungen (Alter der Schüler, Ausstattung der Schule, …) beachtet werden.

Die dritte Forschungsfrage (*Wie könnte dem Mangel an Datenschutzkompetenz begegnet bzw. dieser behoben werden?*) ist mit den vorgestellten Projekten noch nicht beantwortet, jedoch sind erste Schritte in diese Richtung aufgezeigt worden. In dem folgenden vorletzten Kapitel wird versucht, eine zufriedenstellende Antwort auf die letzte Forschungsfrage zu geben.

„Zunächst [steht] die Schaffung des Problembewusstseins im Vordergrund."
(Kramer und Spaeing 2014, S. 371)

6. Handlungsempfehlungen zur Förderung einer Datenschutzkompetenz

Die Förderung einer Datenschutzkompetenz bei Schülern ist eine Aufgabe, der sich Schule und Unterricht (und hier insbesondere der Informatikunterricht, sofern angeboten) zu stellen haben. Ergebnisse von Studien (vgl. Abschnitt 2.3.2 und Kapitel 4) zeigen, dass an dieser Stelle ein Handlungsbedarf notwendig ist. In dem nun folgenden, letzten Kapitel sollen Vorschläge aufgezeigt werden, wie eine Förderung von Datenschutzkompetenz aussehen könnte.

Bei der Komplexität und Breite des Themenfelds *Datenschutz* ist es illusorisch, alles nur Erdenkliche in einer einzelnen Unterrichtsreihe abdecken zu können. Daher müssen die hier gemachten Überlegungen davon ausgehen, dass immer verschiedene Aspekte des Themas im Vordergrund stehen. Aufgrund der Ergebnisse der korrelativen Untersuchung (vgl. Abschnitt 4.3.3.2) werden die Kompetenzen resp. Dimensionen des Datenschutzkompetenzmodells nicht unabhängig voneinander, sondern gleichzeitig zu fördern sein. Demzufolge wird es auch nicht DIE Handlungsempfehlung geben können, sondern ein Konglomerat solcher.

Es ist davon auszugehen, dass aufgrund einer intrinsischen Motivation ein hohes Interesse bei allen Schülern für das Thema existiert, da jeder Schüler in irgendeiner Form davon betroffen ist und in dem Kontext *Datenschutz* aufwächst. Dies ist eine gute Voraussetzung, denn nach der Kompetenzdefinition von Weinert (vgl. Abschnitt 2.1.5) ist motivationale Bereitschaft ein Kennzeichen von Kompetenz. Jedoch sind die Inhalte und Methoden dem Alter entsprechend anzupassen. Im Sinne eines Spiralcurriculums können einzelne Themen wiederholt und in einem zweiten Schritt vertieft werden. Dies führt letztendlich dazu, dass die Sensibilisierung für die Problematik *Datenschutz* über die Schulzeit erhalten bleibt.

In dem folgenden ersten Abschnitt werden Beiträge und Inhalte aus der Literatur zur Förderung einer Datenschutzkompetenz vorgestellt, die Handlungsempfehlungen benennen. Dem schließen sich konkrete aus der Studie abgeleitete Lernzielbeschreibungen an, die sich an dem Datenschutzkompetenzmodell orientieren. Da sich das Nutzungsverhalten, aber auch verwendete Informatiksysteme und entsprechende Software im Laufe der Zeit immer wieder ändern werden, sollen die Empfehlungen so gestaltet sein, dass sie relativ zeitlos und systemunabhängig sind und sich daher den veränderten Bedingungen leicht anpassen lassen.

6.1. Vorschläge zur Ausbildung einer Datenschutzkompetenz in der Literatur

An unterschiedlichen Stellen wurden in der Vergangenheit Vorschläge für die Ausgestaltung von Bildungsplänen zur Förderung einer Datenschutzkompetenz unterbreitet.

Die Gesellschaft für Informatik hat 2006 eine *Empfehlung zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung* herausgegeben, in der je nach Schultyp, Fächer und Alter der Schüler mit einer unterschiedlichen Gewichtung ausgewählte Inhalte der IT-Sicherheit gefordert werden. Besondere Beachtung dient der selbstständigen Bearbeitung der an der Alltagswelt der Schüler orientierten Aufgabenstellungen. Für die Themen mit gesellschaftlichen Bezug und Auswirkungen sind vor allem die Sozialwissenschaften gefordert. Beispielhaft werden mit dem Bezug zum Thema *Datenschutz* „Schutz der Privatsphäre im Internet (Regeln in Chaträumen usw.)“ und „Nachverfolgung des individuellen Verhaltens: Kundenkarten, Überwachungskameras, Biometrie, RFID-Technologie, etc.“ genannt (Gesellschaft für Informatik e. V. 2006, S. 9). Um innerhalb des Informatikunterrichts Interesse zu wecken, sollten Unterrichtsprojekte implementiert werden, um beispielhafte Schwachstellen aufzuzeigen. Dies kann durch unterschiedliche Methoden wie Rollenspiele, Referate oder Projekte erfolgen. Sowohl Themen mit aktuellem Bezug zur IT-Sicherheit, Beispiele aus der Praxis als auch gesetzliche Regelungen gehören in den Unterrichtskanon der Informatik, aber auch anderer Fächer. Beispielhaft könnten folgende Fragen im Fokus stehen: „Welche Daten werden während der Internetnutzung von wem gespeichert und warum?“, „Was sind Cookies? Wie können sie meinen Rechner gefährden?“, „Werden Passwörter, Dateien etc. auch temporär auf der Festplatte gespeichert?“ oder „Was bedeuten Zertifikate?“ (Gesellschaft für Informatik e. V. 2006, S. 10). Diese Empfehlungen wurden bei der Entwicklung der Standards für die Informatikbildung und der Informatiklehrpläne berücksichtigt, jedoch weniger in anderen Fächern (wie z. B. Sozialkunde bzw. Gesellschaftswissenschaften). Da Informatik kein Pflichtfach an allen deutschen Schulen ist, kann die Empfehlung nur bedingt im Unterricht Anwendung finden.

Schon (Wagner 2012, S. 85) stellt fest, dass „ein Bildungskonzept zum Datenschutz … auf Informationen und der Vermittlung von Wissen aufbauen [muss]. Allerdings reicht dies nicht aus. Es ist deshalb notwendig, die bloße Wissensvermittlung zu verbinden mit der Entwicklung einer Werteorientierung, eines wachen Bewusstseins und einer inneren Haltung“. Handlungsempfehlungen für den Unterricht verlangen eine Sensibilisierung bei den Jugendlichen, dass fortwährend eine Prüfung dahingehend erfolgen muss, was für den Betroffenen selbst und seine Privatsphäre gut ist, aber auch der demokratischen Ordnung nicht schadet. Auf Basis dieser Prüfung gilt es, die passende Entscheidung zu treffen. Dabei spielen „die Fähigkeit zur Datenvermeidung und zum Selbstdatenschutz“ eine entscheidende Rolle neben der „freiheitssichernde[n] Kraft des Datenschutzes“ (Wagner 2012, S. 86). Ferner betont Wagner die Flexibilität der Bildungskonzepte, da sie dem „jeweiligen Stand der digitalen Entwicklung und an den aktuellen Datenschutzfragen“ aufgrund der Aktualität anzupassen sind (Wagner 2012, S. 85). Die Entwicklung neuer Strategien wegen der sich permanent ändernden Risiken und Herausforderungen steht dabei im Fokus.

In (Wagner 2010, S. 559) schlägt er sechs Punkte als Inhalte für ein Bildungskonzept vor:

1. „Das informationelle Selbstbestimmungsrecht und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme müssen vermittelt werden, ebenso ihre Fundierung in der Privatsphäre und deren Bedeutung für den Einzelnen und die Gesellschaft. …
2. Die Bürgerinnen und Bürger müssen außerdem über die Gefahren, die ihren Datenschutzgrundrechten drohen, aufgeklärt werden: über die Gefahren, die vom Staat ausgehen, von der Wirtschaft, aber auch von ihnen selbst. …
3. Es muss vermittelt werden, welche Möglichkeiten die Bürgerinnen und Bürger haben, um diesen Gefahren selbst begegnen zu können. Selbstdatenschutz ist in diesem Zusammenhang das Stichwort …
4. Die allgemeinen und bereichsspezifischen Datenschutzvorschriften enthalten eine Vielzahl von Rechten, wie Auskunfts- und Löschungsansprüche, die den Bürgerinnen und Bürgern helfen sollen, ihre grundgesetzlich verbürgten informationellen Rechtspositionen zu verteidigen. Den meisten Menschen sind diese Rechte aber nicht bekannt und werden daher auch nicht von ihnen wahrgenommen. …
5. Bei allen Bemühungen um digitale Selbstverteidigungsmöglichkeiten darf nicht verloren gehen, dass es auch im Internet nicht nur um Datenschutzrechte, sondern auch um Datenschutzpflichten geht. …
6. Die Auseinandersetzung mit den Risiken der digitalen Entwicklung und ihren Vorteilen sollte am Ende auch dazu befähigen, kritisch mit den neuen Medien umzugehen und sie zumindest zu hinterfragen.“

In dem Beitrag *Datenschutz – Selbstschutz – Medienkompetenz: Wie viel informationstechnische Grundbildung braucht der kompetente Mediennutzer?* stellt (Wagner 2001) klar, dass der Mensch ein nicht zu unterschätzendes Sicherheitsrisiko darstellt. „Sicherheitsbestimmungen werden nur eingehalten, wenn ein Bewusstsein für die Sicherheitsrisiken vorliegt.“ Mit Hilfe von Fallbeispielen und aktuellen Bezügen kann ein Zugang in die Thematik erfolgen, dem sich „die Beschreibung und die Demonstration dessen, was der Computer alles kann und was über das Netz alles möglich ist“ anschließt (Wagner 2001, S. 7). Bei der Fülle an Inhalten muss eine didaktische Reduktion erfolgen, die aber nicht ausschließlich quantitativ zu verstehen ist. „«Nicht weniger wichtiger als eine solche quantitative Begrenzung ist jedoch die qualitative Strukturierung durch die ‹Rückführung komplexer Sachverhalte auf ihre wesentlichen Elemente›...» (Jank und Meyer 1991, S. 81).“[187] Im Zusammenhang mit dem Thema *Datenschutz* bedeutet dies, dass ein Bewusstsein entwickelt werden muss, das über eine reine Handhabung und Nutzung von Informatiksystemen hinausgeht.

Das Erfordernis von Datenschutz muss bei den Schülern über ihre Gegenwart und Lebensumstände erfolgen. Während Erwachsene durch ökonomische Risiken schon sensibilisiert werden können, verwundert es Jugendliche, die sich unter anderem durch Markenartikel und Konsumstile definieren, nicht, durch Personalisierte Algorithmen gezielt Werbung zu erhalten.

[187] Zitiert nach (Wagner 2001, S. 8)

„Statt sie auf ethische und demokratische Normen zu verpflichten, die jenseits ihres Erfahrungshorizonts liegen, könnte man mit der Frage beginnen, in welchen Situationen es für den einzelnen wichtig wird, Informationen vor dem Zugriff anderer zu schützen, und aufzeigen, welche abgestuften Möglichkeiten des Datenschutzes es gibt“ (Wagner 2001, S. 12). Ganz wichtig ist dabei herauszustellen, dass trotz einer suggerierten Privatheit das Internet als ein offener und für alle zugänglicher Kommunikationsraum fungiert. „Je nachdrücklicher die Notwendigkeit eines Sicherheitsbewusstseins im Unterricht vermittelt wird, desto grösser ist auch die Gefahr, sich resignativ mit den Sicherheitsrisiken abzufinden, da sie angesichts der Komplexität nicht beherrschbar erscheinen“ (Wagner 2001, S. 13).

Über die Resignation aus ihrer Unterrichtsreihe, die in Abschnitt 2.4 beschrieben ist, berichten (Berendt et al. 2014), in der eine Schülerin dahingehende Kritik übt, dass die Orientierung der Inhalte nach Erwachsenen-Kriterien erfolgt sei, aber ein Bezug zu ihrer aktuellen Lebenswelt fehle. Es überwiegt bei den Jugendlichen das Mitteilungsbedürfnis gegenüber der Angst vor theoretischen Auswirkungen auf das spätere Leben. Auch die Gefahren auf die demokratische Grundordnung durch Tracking werden verstanden, weil aber eine direkte Betroffenheit nicht erkannt wird, ziehen sie keine Konsequenzen. Vieles wirkt für sie zu abstrakt, da Konsequenzen und Folgen nicht direkt erkennbar und zudem unpersönlich sind (Berendt et al. 2014, S. 53). Die Autoren des Beitrags kommen zu dem Schluss, dass sie mit dem Ansatz der Datensparsamkeit bei der heutigen Schülergeneration keinen Erfolg haben. Belehrungen zur Datenvermeidung oder bewussten Datenpreisgabe sind genauso fruchtlos, wie eine Fokussierung auf die eigene Privatheit. Daher schlagen sie z. B. eine Aufklärung über die verwendete Software und einen Zugang über Verschlüsselung und Anonymisierung der Kommunikation vor (Berendt et al. 2014, S. 54).

Im folgenden Abschnitt werden Überlegungen des Autors zur Förderung einer Datenschutzkompetenz präsentiert.

6.2. Ableitung von Lernzielbeschreibungen aus den Ergebnissen der Untersuchung

Im Folgenden werden in Form von Lernzielbeschreibungen zu erwerbendes Wissen und zu erwerbende Kompetenzen nach den Dimensionen des Datenschutzkompetenzmodells geordnet und aufgelistet, die sich aus den Ergebnissen der Untersuchung ableiten (vgl. Kapitel 4). Da die Frage der Methodik unter anderem abhängig vom Alter der Schüler, vom Auffassungsvermögen und der Disziplin der jeweiligen Lerngruppe und der Ausstattung der Schulen (z. B. mit Rechnern) ist, steht der Aspekt der Methodik im Hintergrund und wird in einigen wenigen Fällen nur angerissen. Zudem ist in der jetzigen Schulsituation die Frage offen, durch welches andere Fach, wenn kein Informatikunterricht in der Sekundarstufe I angeboten wird, die Kompetenzen gefördert und die Lernziele angestrebt werden sollen. Dies hat ebenfalls Einfluss auf die Wahl der Methodik.

Wie schon in Abschnitt 2.2.2.2 beschrieben, können Themen anderer Fächer unter dem Aspekt *Datenschutz* behandelt werden. Hier ist je nach Vertiefung dieser Themen mit einem entsprechenden Fachlehrer ein fächerverbindender Unterricht anzustreben. Diese Tatsache wird im Folgenden jedoch nicht weiter verfolgt.

Die folgenden Lernzielbeschreibungen richten sich größtenteils an Schüler der Orientierungsstufe, da die Ableitung aus der Studie erfolgt, an der die Mehrheit der Teilnehmer dieser Schulstufen entstammte. Die Aufzählung folgt den Dimensionen des Datenschutzkompetenzmodells und legt keine zu behandelnde Reihenfolge der Themen fest. Die Darstellung erfolgt in tabellarischer Form:

Nr.	**Lernzielbeschreibung**	**DSK<Nr>**
	Konkretisierung	
	Möglichkeiten der Verknüpfung der Lernzielbeschreibungen	

Tab. 6.1: Tabellenvorlage Lernzielbeschreibung

Die Nummer in der linken Spalte setzt sich aus der Nummer der Dimension und einer davon durch einen Punkt getrennten fortlaufenden Zahl zusammen. Dieser folgt die Lernzielbeschreibung und in der letzten Spalte die entsprechend damit korrespondierende Datenschutzkompetenz aus Tabelle 3.8. Darunter folgt die dazugehörige Konkretisierung und eine Auflistung möglicher Verknüpfungen zwischen der jeweiligen Lernzielbeschreibung und den anderen Lernzielbeschreibungen. Es ist sinnvoll, diese Querverbindungen zu nutzen, da die bivariate Analyse gezeigt hat (vgl. Abschnitt 4.3.3.2), dass die Dimensionen des Datenschutzkompetenzmodells zusammenhängen und die Kompetenzförderung daher ganzheitlich und nicht nach Dimensionen getrennt erfolgen sollte.

Wissen

In dieser Dimension schnitten die Schüler im Rahmen der Untersuchung mangelhaft ab. Daher müssen folgende Kompetenzen gefördert werden:

1.1	**Die Schüler beschreiben und erläutern die Begriffe *Administrator, Betriebssystem, Blog, Browser, Browserverlauf, Chat, Client, Cloud, Cookie, Firewall, Gateway, Hacking, Internet, Internetadresse (URL), Intranet, IP-Adresse, LAN, Link, Login, Malware, Netzwerk, offline, online, Passwort, Phishing, Protokoll (http, https, …), Provider, Router, Server, Social Media, Spam, Spoofing, Spyware, Suchmaschine, Switch, Tracking, Trojaner, URL-Verschlüsselung*, Verschlüsselung, *Virus, Webseite, Wikipedia, WLAN, Wurm, Zertifikat.***	**DSK1**
	Diese Grundbegriffe sind nicht alle auf einmal im Unterricht zu behandeln, da die Schüler damit überfordert wären. Je nach Inhalt werden die Begriffe immer erst an entsprechender Stelle eingeführt (z. B. beim Thema *Netzwerke* die Begriffe *Server*, *Router*, usw. und beim Thema *Malware* die Begriffe *Virus*, *Trojaner*, usf.). Empfehlenswert ist, dass die Lernenden sich ein eigenes Glossar (vergleichbar einem Vokabelheft) anlegen, sodass sie jederzeit darauf zugreifen können. Das eigene Glossar hat den Vorteil, dass durch das Schreiben der Begriffe und Erklärungen sich diese besser einprägen, die eigenen Worte das Verständnis erhöhen und keine falschen Informationen aus anderen Quellen (insb. aus dem Internet) übernommen werden. Mit der Zeit entsteht ein Nachschlagewerk, welches über die gesamte Schulzeit genutzt werden kann.	
	Dieses Lernziel erstreckt sich wegen einigen sehr grundlegenden Begriffen über den gesamten Bereich, insb. aber zu folgenden Lernzielen: 1.2, 1.3, 1.6, 1.8, 1.9, 2.2, 2.6, 2.7, 3.1, 4.1, 4.4, 4.5, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6 und 5.7	

Tab. 6.2-a: Lernzielbeschreibung 1.1 Dimension Wissen

1.2	**Die Schüler beschreiben und erläutern die Bedeutung einer (abhör-)sicheren URL und erkennen diese in dem Adressfeld eines Browsers.**	**DSK1**
	Hier muss herausgearbeitet werden, dass anhand der URL und dem Schlosssymbol in der Adressleiste des Browsers eine sichere Verbindung gewährleistet ist, aber dass dies nicht bedeutet, dass die entsprechende Webseite „sicher“ ist. Dies kann anhand von Screenshots ausgewählter Phishing-Seiten (z. B. Banken) geschehen.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 5.3	

Tab. 6.2-b: Lernzielbeschreibung 1.2 Dimension Wissen

1.3	**Die Schüler nennen die Bedeutung und die Funktion einer Datenschutzerklärung und kennen ihre Rechte in diesem Zusammenhang.**	**DSK2**
	Da Datenschutzerklärungen langatmige und durch die juristische Sprache schwer verständliche Texte sind, können diese im Unterricht nicht vollständig inhaltlich behandelt werden. Aber anhand konkreter Datenschutzerklärungen kann dies offensichtlich demonstriert werde. Die Lehrkraft weist auf die Funktion einer solchen Erklärung hin und erläutert daran die Datenschutzprinzipien. Es ist darauf zu achten, dass der Webseitenbetreiber sich daran orientiert. Der juristische Hintergrund (DSGVO) kann bei einer lernstarken Gruppe genannt werden.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 1.4	

Tab. 6.2-c: Lernzielbeschreibung 1.3 Dimension Wissen

1.4	**Die Schüler beschreiben ihr Recht der Einsicht in die über sie erhobenen, verarbeiteten und gespeicherten Daten.**	**DSK3**
	Das Recht auf informationelle Selbstbestimmung ist ein für diese Altersstufe sehr anspruchsvolles Thema. Das Resultat dieses Rechts kann mit der zuvor genannten Kompetenz 1.3 verknüpft werden. Eine Verknüpfung zum Datenmissbrauch ist über Kompetenz 1.7 möglich.	
	Verknüpfung mit Lernzielbeschreibung: 1.3, 1.7, 2.4	

Tab. 6.2-d: Lernzielbeschreibung 1.4 Dimension Wissen

1.5	**Die Schüler geben an, in welchen Fällen eine Erlaubnis zur Veröffentlichung von Fotos einzuholen sind, auf denen sie deutlich erkennbar sind.**	**DSK3**
	Dieses Thema spricht Jugendliche unmittelbar an. Da Jugendliche unbedacht Fotos teilen und in Sozialen Medien veröffentlichen, ist es von sehr großer Bedeutung, diesen Punkt an passender Stelle zu thematisieren. Beispiele dieser Form von Rechtsverletzung und den daraus resultierenden Folgen tragen zum besseren Verständnis bei. Hierzu gibt es entsprechende Unterrichtsmaterialien (vgl. Abschnitt 2.4).	
	Verknüpfung mit Lernzielbeschreibung: 2.1, 2.5, 3.2 und 4.2	

Tab. 6.2-e: Lernzielbeschreibung 1.5 Dimension Wissen

1.6	**Die Schüler geben an, unter welchen Umständen ein Tracking des Surfverhaltens erlaubt ist.**	**DSK3**
	Nachdem die Arbeitsweise von Tracking und der Nutzen für den Webseitenanbieter erläutert sind (hier bietet sich z. B. der Einsatz der Software *Lightbeam*[188] an), muss die Rechtmäßigkeit des Trackings besprochen werden.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 1.7, 1.9, 2.3, 2.6, 4.2, 4.5 und 5.3	

Tab. 6.2-f: Lernzielbeschreibung 1.6 Dimension Wissen

[188] Siehe https://de.wikipedia.org/wiki/Lightbeam (zuletzt geprüft am 21.12.2019); obwohl das Add-on eingestellt sein soll (vgl. https://www.soeren-hentzschel.at/firefox/lightbeam-eingestellt/; zuletzt aufgerufen am 11.01.20), funktioniert es mit der aktuellen Software-Version von Mozilla-Firefox (72.0.1) noch.

1.7	**Die Schüler beschreiben und erläutern, inwiefern personenbezogene Daten von Online-Händlern, Betreibern Sozialer Plattformen und Geheimdienste zweckentfremdet genutzt und ausgewertet werden.**	**DSK4**
	An den Beispielen von *Prism*[189] oder des Sammelns von Nicht-Mitglieder-Daten bei *Facebook*[190] kann den Schülern das Verhalten von Institutionen und Händlern verdeutlicht werden. Es ist davon auszugehen, dass die Lernenden, ohne die Tragweite dieses Vorgehens vollständig zu erfassen (insb. im Hinblick auf die weit entfernte Zukunft), ein solches Verhalten nicht begrüßen werden und dementsprechend gewarnt sind.	
	Verknüpfung mit Lernzielbeschreibung: 1.4, 1.6, 2.1, 2.4 und 2.6	

Tab. 6.2-g: Lernzielbeschreibung 1.7 Dimension Wissen

1.8	**Die Schüler schätzen den Modus *Private Browsing* in Bezug auf seine Sicherheit und seinen Schutz beim Surfen ein.**	**DSK5**
	Das häufige Missverständnis zwischen dem Modus und dem Glauben, anonym im Netz unterwegs zu sein, muss geklärt werden. Es können genau die Punkte genannt und erlernt werden, die beim *Private Browsing* anders sind, und dabei ist hervorzuheben, welche Punkte gleich sind, zum Beispiel die Mitteilung der IP-Adresse und der Browser-Fingerprint.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 1.9, 3.1 und 5.3	

Tab. 6.2-h: Lernzielbeschreibung 1.8 Dimension Wissen

1.9	**Die Schüler nennen Maßnahmen, um die Nachverfolgung im Netz zu erschweren.**	**DSK5**
	In der Literatur und im Netz (z. B. Materialien von *Klicksafe*[191]) sind eine ausreichende Anzahl an Verhaltensregeln (z. B. regelmäßiges Löschen von Cookies, des Browserverlaufs oder Nutzung datenschutzfreundlicher Suchmaschinen) für eine sichere Internetnutzung zu finden, auf die die Lehrkraft zurückgreifen kann. Zur Festigung der Lerninhalte können die Schüler auch ein Plakat mit solchen Regeln selber entwerfen und im Klassenzimmer aufhängen. Zugleich können auch technische Maßnahmen (vgl. Lernzielbeschreibung 3.1) und das allgemeine Tracking-Verhalten (vgl. Lernzielbeschreibung 1.6) thematisiert werden.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 1.6, 1.8 und 3.1	

Tab. 6.2-i: Lernzielbeschreibung 1.9 Dimension Wissen

[189] Siehe https://de.wikipedia.org/wiki/PRISM (zuletzt geprüft am 21.12.2019)
[190] Siehe https://www.heise.de/newsticker/meldung/Was-Facebook-ueber-Nicht-Mitglieder-weiss-921350.html (zuletzt geprüft am 21.12.2019)
[191] Siehe www.klicksafe.de (zuletzt geprüft am 21.12.19)

Risikobewertungskompetenz

In dieser Dimension schnitten die Schüler im Rahmen der Untersuchung ausreichend ab. Daher müssen folgende Kompetenzen gefördert werden:

2.1	**Die Schüler bewerten, begründen und entscheiden über die Sensibilität personenbezogener Daten und deren Veröffentlichung (z. B. in Sozialen Netzwerken).**	**DSK6 + DSK8**
	Wie aus der Untersuchung ersichtlich ist (vgl. Abschnitt 4.3.3.1), erkannten die Schüler, dass z. B. Adresse oder Handy-Nummer extrem sensible Daten sind, während ein Vorname als einzelnes Datum noch unproblematisch ist. Die Begründungen dafür sind von den Schülern zu erarbeiten. Anders sieht dies jedoch aus, wenn mehrere Daten miteinander verknüpft werden und damit ein Profil erstellt wird, das für das digitale „Ich" steht. Diese Problematik muss mit Unterstützung der Lehrkraft thematisiert werden. Methodisch könnte hierzu das Planspiel *Datenschutz* eingesetzt werden, das gleichzeitig das Tracking im Internet beinhaltet. Abschließend sollte eine Art Skala von den Schülern erstellt werden, aus der dann die Sensibilität des jeweiligen Datums ersichtlich ist. Auch wenn die „klassischen" Sozialen Netzwerke nicht mehr die Bedeutung wie vor rund zehn Jahren einnehmen, muss über die Sensibilität persönlicher Daten gesprochen werden, da in vielen Situationen – auch außerhalb des Internets (z. B. Arztbesuch) – personenbezogene Daten eine Rolle spielen.	
	Verknüpfung mit Lernzielbeschreibung: 1.5, 1.7, 2.3, 2.4, 2.6, 4.1, 4.2 und 4.3	

Tab. 6.3-a: Lernzielbeschreibung 2.1 Dimension Risikobewertungskompetenz

2.2	**Die Schüler bewerten und begründen die Bedeutung einer verschlüsselten Datenübermittlung und der Identifikationsmöglichkeit des Gesprächspartners bei Messengern-Diensten.**	**DSK8**
	Da Messenger-Dienste einen sehr hohen Stellenwert bei den Jugendlichen einnehmen (vgl. Abschnitt 2.3.2), müssen diese und ihre Funktionen thematisiert werden. Da *WhatsApp* als beliebtester Dienst fast ausschließlich bekannt ist, bietet es sich an, Alternativen vorzustellen und deren Vorteile herauszustellen. In diesem Zusammenhang kann das Prinzip der Datenverschlüsselung (schon mit einfachen symmetrischen Verfahren) den Schülern nahegebracht werden.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 5.1	

Tab. 6.3-b: Lernzielbeschreibung 2.2 Dimension Risikobewertungskompetenz

2.3	**Die Schüler schätzen die Gefahr der unerwünschten Weitergabe persönlicher Daten an Dritte und das Ausspionieren persönlicher Daten ab.**	**DSK6**
	In fast schon regelmäßigen Abständen finden sich in der aktuellen Presse Berichte über gehackte Datenbanken, den Verkauf oder die Weitergabe von personenbezogenen Daten usf. Durch diese immer wiederkehrenden Informationen zeigt sich für die Schüler, dass dieses grundlegende Problem im Umgang mit persönlichen Daten aktuell ist, was die Motivation stärkt, und weiterhin besteht. Als passendes Beispiel eines Whistleblowers eignet sich der Fall *Edward Snowden*, der trotz der Enthüllungen vor einigen Jahren an Brisanz nichts eingebüßt hat. An dieser Stelle können der Mut eines Whistleblowers und das Vertrauen „unter Freunden" beleuchtet werden. Mit beidem kann man affektive Lernziele anstreben, welche im Informatikunterricht eher selten sind. Wichtig ist in diesem Zusammenhang auch die Sensibilität personenbezogener Daten mit in den Fokus zu nehmen, denn je sensibler die Daten sind (z. B. Konto- oder Kreditkartendaten), desto schwerwiegender können die Folgen eines Missbrauchs ausfallen. Welche verbrecherischen Absichten hinter einem Datenmissbrauch stehen können, müssen sich die Schüler mit auseinandersetzen. Passende Beispiele, um die Schülervermutungen zu untermauern, finden sich im Rahmen einer Internetrecherche.	
	Verknüpfung mit Lernzielbeschreibung: 1.6, 2.1, 2.4, 2.6, 4.2 und 4.3	

Tab. 6.3-c: Lernzielbeschreibung 2.3 Dimension Risikobewertungskompetenz

2.4	**Die Schüler bewerten und begründen den Missbrauch personenbezogener Daten.**	**DSK10**
	Dieser Aspekt knüpft unmittelbar an die vorher genannte Lernzielbeschreibung an. Durch konkrete Vorfälle können die Bewertungen erfolgen.	
	Verknüpfung mit Lernzielbeschreibung: 1.4, 1.7, 2.1, 2.3, 4.2 und 4.3	

Tab. 6.3-d: Lernzielbeschreibung 2.4 Dimension Risikobewertungskompetenz

2.5	**Die Schüler diskutieren und erörtern die Netiquette im Internet.**	**DSK9**
	Die Probleme des (Internet-)Mobbings oder der Hasskommentare in Foren sind zu thematisieren. Fallbeispiele finden sich zu genüge in vorhandenen Unterrichtsmaterialien. Neben der Erarbeitung der Netiquette-Regeln muss für den Fall des Mobbings auch der Opferschutz angesprochen werden. Die Schüler müssen wissen, dass jeder von ihnen jederzeit Opfer werden und wie man sich helfen lassen kann. Die Gefahren, die von unreflektierten und nicht aufgearbeiteten Vorfällen ausgehen können, sind zu verdeutlichen.	
	Verknüpfung mit Lernzielbeschreibung: 1.5	

Tab. 6.3-e: Lernzielbeschreibung 2.5 Dimension Risikobewertungskompetenz

2.6	**Die Schüler bestimmen und benennen die Gefahren, wenn Andere über eigene Tätigkeiten und Aufenthaltsorte informiert sind.**	**DSK11**
	Da es inzwischen sehr beliebt ist, die Öffentlichkeit über seine Handlungen (unreflektiert) zu informieren, muss eine Sensibilisierung dahingehend stattfinden. Über diese preisgegebene Information können Rückschlüsse gezogen werden, die wiederum unerwünschte Folgen auslösen (z. B. die Urlaubsposts, die Verbrecher zum Ausräumen der eigenen Wohnung „auffordern“). Die Gründe für die eigene Datenverbreitung sind das eigene Präsentieren. Findet die Datenverbreitung durch Dritte statt, dann liegt ein Datenmissbrauch vor. Diskussionswürdig ist das Risiko, welches durch die Standortermittlung von Smartphones ausgeht. Viele Apps erfragen oder fordern zwecks (komfortabler) Nutzung den Standort über GPS vom Besitzer, verschweigen aber damit, dass durch das Gerät zurückgelegte Wege gespeichert, ausgelesen und (z. B. für Werbezwecke) ausgewertet werden. Mit Hilfe solcher Informationen kann das Verhalten anderer vorausbestimmt werden, wenn sich Wege in bestimmter Regelmäßigkeit wiederholen (z. B. Schulwege). An dieser Stelle kann diskutiert werden, wann eine Standortermittlung Sinn macht (man möchte Hilfe an einen unbekannten Ort anfordern), für welche App eine solche Funktion interessant ist und wie die Funktion ausgeschaltet werden kann.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 1.6, 1.7, 2.1, 2.3, 4.2, 4.3 und 5.2	

Tab. 6.3-f: Lernzielbeschreibung 2.6 Dimension Risikobewertungskompetenz

2.7	**Die Schüler schätzen die Gefahren einer Malware-Infektion durch ungeschicktes und unvorsichtiges Handeln ab.**	**DSK12+ DSK13+ DSK14**
	Dieses Gebiet ist sehr groß und es können nicht alle Eventualitäten besprochen werden. Typische Fehler wie das Öffnen von E-Mail-Dateianhängen unbekannter Absender, der Aktivierung von Makros in Software, die zur Gruppe der Office-Programmen zählt, oder das Anklicken von Links in Chat-Nachrichten oder Pop-Up-Fenstern von Browsern müssen thematisiert werden. Hier können Verhaltensregeln abgeleitet und auf Plakaten, die im Klassenraum ausgehangen werden, festgehalten werden. Den Schülern ist zu verdeutlichen, mit welchen Lockmitteln Internetnutzer zum Anklicken fremder Links animiert werden. Nachdem die unterschiedlichen Formen von Malware, von denen die Schüler teilweise sicherlich auch schon gehört haben, genannt worden sind, müssen die Funktionen geklärt werden. Spannend wäre es für die Schüler, wenn es mindestens einen ausgewählten Rechner gibt, der in einem Sandbox-Modus läuft und in dem Malware-Programme gestartet werden können. Somit würden die Schüler in einem Art Simulationsmodus die Folgen unachtsamer Handlungen „live“ erleben. Abschließend ist die Frage zu klären, wie man sich vor Malware schützen kann. Diese Kompetenzförderung wird durch die Auswahl- und Nutzungskompetenz und Handlungskompetenz abgedeckt. Wichtig ist an dieser Stelle im Sinne eines Merksatzes festzuhalten, dass, wie häufig auch im realen Leben, gilt: Erst denken, dann handeln.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 4.4, 4.5, 5.1, 5.3, 5.5, 5.6 und 5.7	

Tab. 6.3-g: Lernzielbeschreibung 2.7 Dimension Risikobewertungskompetenz

Auswahl- und Nutzungskompetenz

In dieser Dimension schnitten die Schüler im Rahmen der Untersuchung mangelhaft ab. Daher müssen folgende Kompetenzen gefördert werden:

3.1	**Die Schüler kennen und nutzen technische Maßnahmen zur sicheren Internetgestaltung.**	**DSK5**
	Eine absolut sichere Internetgestaltung kann es nicht geben, da bei jeder Internetnutzung ein Restrisiko vorhanden ist. Ziel muss es aber sein, durch geschickte Maßnahmen dieses Restrisiko zu minimieren (s. auch Abschnitt 1.2). (Thielen 2018) zeigt in seiner Arbeit, wie durch die Methode des Stationenlernens dies umgesetzt werden kann, wenn die Ausstattung der Schule entsprechend ausgerichtet ist. Wichtig ist, dass die Schüler, nachdem sie die Arten von Malware kennen, erfahren, welche Mittel Ihnen zum Schutz zur Verfügung stehen. Das beginnt mit einer Anti-Viren-Software, geht über die Einstellung der Firewall über zu passenden Browsertools. Es geht jedoch nicht darum, die Konfiguration jeder nur denkbaren Einstellung (z. B. der Firewall) zu thematisieren, sondern von den Grundeinstellungen der Anbieter auszugehen und vor allem auf die Verwendung und das regelmäßige Aktualisieren der Software hinzuweisen oder gar zu fordern. Zudem sind Browsereinstellungen (z. B. die Deaktivierung von ActiveX-Elementen) zu besprechen. Ob die Verschlüsselung von E-Mails in diesem Alter von Bedeutung ist, bezweifelt der Autor, da die Schüler zur Kommunikation in der Regel Messenger-Dienste nutzen (vgl. Abschnitt 2.3.2). Die vorbereitenden Arbeiten für die Verschlüsselung (Generierung eines Schlüsselpaars, Einbindung in den E-Mail-Client, usw.) sind sehr aufwendig, sodass in diesem Alter darauf verzichtet werden kann. Dennoch muss den Schülern an dieser Stelle vermittelt werden, dass der Versand einer E-Mail dem Versand einer Postkarte in der realen Welt gleich kommt, da für jeden, der die E-Mail (berechtigt oder unberechtigt) zu lesen bekommt, der Inhalt dieser bekannt sein wird. Das klassische Postgeheimnis gibt es in der digitalen Welt nicht. Nicht unproblematisch ist auch die Tatsache, dass durch die Verwendung unterschiedlicher Betriebssysteme, unterschiedlicher Software und unterschiedlicher Browser nicht alle nur denkbaren Einstellungen diskutiert werden können. Einerseits sollte die Lehrkraft sich auf ein Betriebssystem (hier bietet sich *Windows* an, da es am verbreitetsten ist[192]) und einen Browser (hier ist *Mozilla Firefox* zu empfehlen, da er datenschutzfreundliche Einstellungen bietet und sehr beliebt ist[193]) konzentrieren. Andererseits wäre es eine Möglichkeit, die Eltern „mitzunehmen“ und diese für eine sichere Einstellung der privaten Rechner zu Hause zu gewinnen.[194] Es bietet sich z. B. an, an der Schule einen Projektsamstag für Eltern und Schülern (ggf. mit elterlicher Unterstützung) durchzuführen.	

[192] Siehe https://de.statista.com/statistik/daten/studie/158102/umfrage/marktanteile-von-betriebssystemen-in-deutschland-seit-2009/ (zuletzt geprüft am 05.01.20)

[193] Siehe https://de.statista.com/statistik/daten/studie/13007/umfrage/marktanteile-der-browser-bei-der-internetnutzung-in-deutschland-seit-2009/ (zuletzt geprüft am 05.01.20)

[194] Bei dem rheinland-pfälzischen Projekt *Medienkompetenz macht Schule* ist ein wichtiger Baustein des 10-Punkte-Programms die Einbindung von Eltern (vgl. https://medienkompetenz.bildung-rp.de/partner/eltern-weiter-intensiv-einbinden.html und https://eltern-medienkompetenz.bildung-rp.de/; zuletzt geprüft am 30.12.2019).

	… Eine Beobachtung, die der Autor immer häufiger macht, ist, dass durch die Installation von Add-Ons zum Internetschutz einige Webseiten nicht mehr korrekt oder gar nicht mehr angezeigt werden. Hier ist die Verlockung gerade für die Jugendlichen, die die Hilfe und Unterstützung beim sicheren Surfen benötigen, groß, die Sicherheitseinstellung zu umgehen, um an die gewünschte Information zu gelangen. Hier ist wichtig, sich der Seriosität der aufgerufenen Seite bewusst zu sein, wenn man die Sicherheitseinstellungen „lockert“.
	Verknüpfung mit Lernzielbeschreibung: 1.1, 1.8, 1.9, 4.4, 5.1, 5.2 und 5.6

Tab. 6.4-a: Lernzielbeschreibung 3.1 Dimension Auswahl- und Nutzungskompetenz

3.2	**Die Schüler kennen und nutzen kostenlose Alternativen für Musik oder Software im Netz.**	**DSK17**
	Mit dieser Kompetenz wird das Urheberrecht aufgegriffen, dessen Grundaussagen mit den Schülern zu erarbeiten sind. Neben den gesetzlichen Regeln ist eine Sensibilisierung für das Urheberrecht anzustreben. Zur Thematisierung eignet sich an diesem Punkt die bei den Schülern beliebte Weiterleitung und Veröffentlichung von Fotos, auf denen Freunde oder andere Personen abgebildet sind (vgl. Lernzielbeschreibung 1.5). Dies kann sehr gut mit der Urheberrechtsfrage verknüpft werden. Des Weiteren sind legale von illegalen Quellen (für Musik, Videos, Software) zu charakterisieren und aufzuzeigen. Gerade weil *YouTube* zum jetzigen Zeitpunkt als beliebtestes Soziales Netzwerk bei den Schülern gilt (vgl. Abschnitte 2.3.2 und 4.3.3.1), kann die Lehrkraft anhand dieses Beispiels die Nutzungs- und Datenschutzbestimmungen besprechen.	
	Verknüpfung mit Lernzielbeschreibung: 1.5, 5.3	

Tab. 6.4-b: Lernzielbeschreibung 3.2 Dimension Auswahl- und Nutzungskompetenz

Urteilskompetenz

In dieser Dimension schnitten die Schüler im Rahmen der Untersuchung ausreichend ab. Daher müssen folgende Kompetenzen gefördert werden:

4.1	**Die Schüler bewerten und beurteilen, welche Änderungen in den Privatsphäreeinstellungen Sozialer Netzwerke sinnvoll sind, und ziehen Rückschlüsse für ihr Handeln.**	**DSK7 + DSK8**
	Die Förderung dieser Kompetenz erfolgt am geschicktesten in Kombination mit der Lernzielbeschreibung 2.1, bei der die Sensibilität der unterschiedlichen Art von personenbezogenen Daten besprochen wird. Hierbei erfolgt gleichzeitig eine Bewertung und Beurteilung des jeweiligen Datums anhand vorher vereinbarter Sach- und Wertekriterien. Sinnvoll wäre es, dass die Schüler sich im Anschluss die Privatsphäre-Einstellung eines Sozialen Netzwerks anschauen, was jedoch wiederum die Mitgliedschaft in einem solchen voraussetzt, die nicht gezwungener Maßen gewährleistet ist. Denkbar wäre hier der Einsatz der Lernplattform *InstaHub*[195], welche jedoch zum jetzigen Zeitpunkt eine Funktion der Privatsphäre-Einstellung noch nicht implementiert hat. Da die Betreiber Sozialer Netzwerke ihre Einstellungsoptionen für die Nutzer-Profile in bestimmten Zeitabständen auch immer wieder ändern, macht es wenig Sinn, sich hier auf die Ebene einer Bedienerschulung einzulassen. Stattdessen muss auf die Möglichkeit der Änderung der persönlichen Einstellungen generell hingewiesen werden.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 2.1, 4.2, 4.3 und 5.2	

Tab. 6.5-a: Lernzielbeschreibung 4.1 Dimension Urteilskompetenz

[195] Zu *InstaHub* vergleiche Abschnitt 2.4.

4.2	**Die Schüler beurteilen die eigene Veröffentlichung von Daten im Internet und deren Folgen, sowie die Notwendigkeit, selber entscheiden zu können, wer etwas über die eigene Person erfährt, und nehmen dazu kritisch Stellung.**	**DSK7**
	Es ist davon auszugehen, dass in dem jungen Alter die Schüler kaum eigene Erfahrungen mit den Folgen veröffentlichter persönlicher Daten haben werden. Daher ist es besonders schwierig, hierfür ein Verständnis zu entwickeln. Denn wie auch eine (ältere) Schülerin in (Berendt et al. 2014) berichtet, möchte sie sich nicht bei jeder Gelegenheit über die Folgen veröffentlichter Daten und Likes Gedanken machen. In der Regel, so zeigen Untersuchungen (vgl. Abschnitt 2.3), nimmt die Sorgfalt in dem Moment zu, wenn man persönlich betroffen ist. Daher bleibt an dieser Stelle der Lehrkraft nur die Möglichkeit durch Erfahrungsberichte aus Unterrichtsmaterialien oder Presse die Lernenden auf die möglichen Konsequenzen (vor allem unbedachter) veröffentlichter personenbezogener Daten hinzuweisen. Denkbar ist, dass die Schüler zur Schulung der Beurteilung beispielhaft Fälle von zweckfremder Datennutzung vorgelegt bekommen, um daran kritisch Stellung zu nehmen und passende Verhaltensregeln zu formulieren, die auf Plakaten für das Klassenzimmer festgehalten werden können. Die Entscheidung darüber, wer welche Daten zu lesen oder zu sehen bekommt, wird in den meisten Fällen durch Einstellungen in den Sozialen Netzwerken und durch Posts in diesen oder in Messenger-Diensten geregelt. Dies knüpft an die Lernzielbeschreibung 4.1 an.	
	Verknüpfung mit Lernzielbeschreibung: 1.5, 1.6, 2.1, 2.3, 2.4, 2.6, 4.1 und 4.3	

Tab. 6.5-b: Lernzielbeschreibung 4.2 Dimension Urteilskompetenz

4.3	**Die Schüler bewerten, schätzen ab und nehmen erörternd Stellung, welche Informationen sie selbst über sich ins Internet stellen.**	**DSK16+ DSK11**[196]
	Diese Kompetenz knüpft an die vorangehende Lernzielbeschreibungen 4.2 an und sollte in diesem Zusammenhang mit gefördert werden.	
	Verknüpfung mit Lernzielbeschreibung: 2.1, 2.3, 2.4, 2.6, 4.1 und 4.2	

Tab. 6.5-c: Lernzielbeschreibung 4.3 Dimension Urteilskompetenz

4.4	**Die Schüler erläutern und beurteilen die Funktion der Deaktivierung aktiver Inhalte in einem Browser.**	**DSK5 + DSK13**
	Die potentiellen Gefahren, die von aktiven Elementen auf Webseiten ausgehen, können den Schülern anhand von Beispielfällen vorgestellt werden. Ähnlich wie im Fall der Lernzielbeschreibung 2.7 genannt, könnten solche Gefahren auch in einem Sandbox-Betrieb demonstriert werden, um das Verständnis dafür zu erhöhen. Abschließend ist den Lernenden die Deaktivierung aktiver Inhalte zu demonstrieren.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 2.7, 3.1 und 4.5	

Tab. 6.5-d: Lernzielbeschreibung 4.4 Dimension Urteilskompetenz

[196] Diese aus einem Item der Studie abgeleitete Kompetenz ist aufgrund der Entscheidung der Q-Sortierung eine Handlungskompetenz. Da der Autor diese jedoch mit den beiden vorangehenden Kompetenzen eher als eine Urteilskompetenz sieht, wurde sie auch an obiger Stelle innerhalb der Liste aufgenommen.

4.5	**Die Schüler beurteilen die Gefahr, reizvoll klingende Werbebanner anzuklicken, und schätzen dies ab.**	**DSK9 + DSK14**
	Im Gegensatz zu dem vorausgehenden Fall der Lernzielbeschreibungen 4.4 kennen die Schüler aus eigener Erfahrung die verlockenden Pop-Up-Fenster und Werbebanner. Vermutlich wird auch der Eine oder die Andere damit seine bzw. ihre Erfahrung gemacht haben, sodass hier auf Erfahrungsberichte aus der Lerngruppe zurückgegriffen werden kann. Die aus der Psychologie bekannten Verhaltensregeln, die von Webseitenbetreibern ausgenutzt werden, müssen den Schülern vermittelt werden (z. B. Reaktion auf Reiz, Gefahr sich ablenken zu lassen). Dass augenscheinlich zufälligerweise genau solche Dinge in Pop-Up-Fenstern und Werbebannern angeboten werden, die im Interessensbereich des Surfenden liegen, bietet die Möglichkeit diesen Aspekt mit dem Thema *Webtracking* zu verbinden (vgl. Lernzielbeschreibung 1.6). Die Folgen, die ein (unbedachter) Klick auf einen Werbebanner haben kann, können den Lernenden anhand von Pressemitteilungen aufgezeigt werden. Abschließend sollte die Lehrkraft zeigen, wie durch passende Browsereinstellungen das Auftreten solcher Werbebanner größtenteils unterbunden werden kann	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 1.6, 2.7 und 4.4	

Tab. 6.5-e: Lernzielbeschreibung 4.5 Dimension Urteilskompetenz

Handlungskompetenz

In dieser Dimension schnitten die Schüler im Rahmen der Untersuchung mangelhaft ab. Daher müssen folgende Kompetenzen gefördert werden:

5.1	**Die Schüler erklären die Nutzung sicherer Geräte mit persönlichem Passwort, die Verwendung verschiedener Passwörter und die Notwendigkeit von Passwortänderungen in regelmäßigen Abständen und wenden dies an.**	**DSK5 + DSK15**
	Da fast jeder Schüler der betrachtenden Altersgruppe ein eigenes Smartphone besitzt, auf dem persönliche Daten gespeichert sind, kann die Nutzung dieser Geräte als ein Ansatz gewählt werden, sich dem Thema *Passwörter und deren Verwendung* zu widmen. Erst durch einen entsprechend gesicherten Zugang zu den eigenen Daten kann ein Schutz dieser (bis auf ein Restrisiko) gewährleistet werden. Die Schüler können selbstständig die Frage nach der Minimierung des Restrisikos erarbeiten. Ziel muss einerseits sein, dass die Schüler die Regeln starker Passwörter beachten, ihre Passwörter regelmäßig ändern und für verschiedene Zugänge auch verschiedene Passwörter nutzen. Andererseits müssen diese Regeln auch angewendet werden, was durch die Lehrkraft jedoch nicht kontrolliert werden kann, sonst wäre die Funktion des Passworts ad absurdum geführt. Einzig eine regelmäßige Erinnerung zur Passwortänderung kann unterstützend wirken. Browser bieten die Möglichkeit an, Passwörter zu speichern und diesen Passwortspeicher durch ein einziges Masterpasswort zu schützen. Von dieser Funktion sollten die Schüler Gebrauch machen, aber bei jedem Passwort überlegen, wie sensibel es ist, um es abzuspeichern (so ist z. B. das Passwort für das Online-Banking so kritisch, dass es niemals abgespeichert werden sollte, während das Zugangsdatum zum Sozialen Netzwerk weniger kritisch ist); da Schüler in diesem Alter noch nicht geschäftsfähig sind und auch über keinen Online-Banking-Zugang verfügen, gibt es keine passenden Beispiele aus der Erfahrungswelt der Schüler. Des Weiteren bietet es sich an, Passworttresore vorzustellen, in denen alle Passwörter gespeichert sind. Die Stärke von Passwörtern kann im Zusammenhang mit kryptologischen Fragestellungen behandelt werden. Wenn die Lehrkraft bewusst schwache Passwörter wählt, könnte sie die Schüler in Form eines Art Wettkampfs gegeneinander als Codeknacker antreten lassen.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 2.2, 2.7 und 3.1	

Tab. 6.6-a: Lernzielbeschreibung 5.1 Dimension Handlungskompetenz

5.2	**Die Schüler erläutern die Notwendigkeit der Aktualisierung persönlicher Sicherheitseinstellungen in Sozialen Netzwerken und anderen Plattformen gegenüber den Grundeinstellungen der Anbieter und führen dies aus.**	**DSK5**
	Die Grundeinstellungen der Dienstanbieter sind in der Regel eher schwach oder juristischen Vorgaben entsprechend eingestellt und verlangen immer eine Nachjustierung vom Nutzer, sofern er seine Daten besser schützen möchte. Anhand beliebter Plattformen kann ein solches Vorgehen erarbeitet und demonstriert werden.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 2.6, 3.1 und 4.1	

Tab. 6.6-b: Lernzielbeschreibung 5.2 Dimension Handlungskompetenz

5.3	**Die Schüler nennen Webseiten, die bekanntermaßen sicher sind, und entscheiden sich für deren Nutzung.**	**DSK5**
	Die Seriosität von Webseiten zu beurteilen, ist nicht immer leicht. Daher müssen Regeln oder ein Kriterienkatalog erstellt werden, anhand dessen eine Beurteilung über eine Webseite erleichtert wird. Zu Beginn bieten sich Suchmaschinen an, da sie die erste Anlaufstelle bei einer Informationsrecherche im Netz sind. Da Google die bekannteste Maschine ist[197], kann die Lehrkraft mit dieser einsteigen, mit den Schülern den Aufbau der Suchergebnisseiten inspizieren und die Datenschutzfrage von Google, die immer wieder ein Stein des Anstoßes für Datenschützer ist, diskutieren. Zu diesem oder zu einem späteren Zeitpunkt könnte die Produktpalette der Firma *Google* und deren Tochterunternehmen ins Gespräch gebracht werden und die Verknüpfung der Daten aus den verschiedenen Unternehmensbereichen thematisiert werden. Aufgrund der Schwierigkeit dieses Teilthemas könnten die jüngeren Schüler damit überfordert sein, sodass die Lehrkraft hier einschätzen muss, inwieweit dieser Aspekt beleuchtet wird oder nicht. Die Gefahren, die durch die Datenverknüpfung solcher Unternehmen entstehen, müssen letztendlich aber klar und deutlich hervorgehoben und formuliert werden. Neben der Suchmaschine *Google* gibt es auch Produkte wie *Startpage*[198], die grundlegende Datenschutzrichtlinien einhalten. Es ist wichtig, hierbei mehrere Alternativen an Suchmaschinen den Lernenden vorzustellen. In dem vorliegenden Alter bieten sich auch noch spezielle Kinder-Suchmaschinen wie *Blinde Kuh*[199] an, die sich jedoch stärker an Kinder im Primarbereich richtet. Trotz aller Seriosität einiger Anbieter (wie z. B. im Bereich der Presse wie *FAZ*, *SZ* oder *Spiegel online* oder im Bereich Lernhilfen von Schulbuchverlagen) gibt es kaum noch einen Anbieter, der auf die Einbindung von Tracking-Software, Cookies, usw. verzichtet. Unter dem Deckmantel der verbesserten Funktionalität werden diese Tools in die Webseiten integriert, sodass der Nutzer sich unter der Nutzung entsprechender Add-Ons wie *Cookie AutoDelete*[200] oder *Privacy Badger*[201] bis zu einem gewissen Grad der Fremdkontrolle entziehen kann (Stichwort *Selbstdatenschutz*). Die Schüler können einerseits sinnvolle und datenschutzfreundliche Webseiten sammeln und die URL als Lesezeichen im Browser speichern und anderseits auch Kriterien für seriöse Webseiten je nach Themengebiet erstellen, sodass eine Einordnung der Qualität der jeweiligen Webseite erleichtert wird.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 1.2, 1.6, 1.8, 2.7 und 3.2	

Tab. 6.6-c: Lernzielbeschreibung 5.3 Dimension Handlungskompetenz

[197] Siehe https://seo-summary.de/suchmaschinen/ (zuletzt geprüft am 05.01.20)
[198] Siehe https://www.startpage.com/ (zuletzt geprüft am 05.01.20)
[199] Siehe https://www.blinde-kuh.de/index.html (zuletzt geprüft am 05.01.20)
[200] Siehe https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete/ (zuletzt geprüft am 05.01.20)
[201] Siehe https://addons.mozilla.org/en-US/firefox/addon/privacy-badger17/ (zuletzt geprüft am 05.01.20)

5.4	**Die Schüler erklären die Notwendigkeit regelmäßiger Virenscan der Festplatte und regelmäßiger Datenbackups auf externen Medien und wenden dies an.**	**DSK5**
	Die Erkenntnis einer Malware-Gefahr kann durch Lernzielbeschreibung 2.7 gefördert werden, sodass als logische Konsequenz ein Viren- bzw. Malwarescan folgt. Den Start eines solchen Scans ist leicht erklärt, jedoch müssen die Schüler auch etwaige Meldungen (z. B. *verdächtige Datei XY gefunden und in Quarantäne verschoben*) und deren Auswirkungen für die Arbeit mit dem Rechner verstehen. Hier bietet sich die Demonstration in einer Sandbox an, in die durch die Lehrkraft zuvor bewusst Malware eingeschleust wurde. Da durch ein Hardwaredefekt oder eine Malware ein Datenverlust entstehen kann, müssen Schüler Maßnahmen des einfachen Datenbackups kennen (Thema *Datensicherung*). Dazu sollten die Schüler lernen eine verschlüsselte Partition ihrer Festplatte anzulegen, in der alle persönlichen Daten gespeichert werden. Diese Partition kann schon mit einfachen Mitteln regelmäßig gesichert werden, ohne dafür eine spezielle Software zu bemühen.	
	Verknüpfung mit Lernzielbeschreibung: 1.1 und 5.6	

Tab. 6.6-d: Lernzielbeschreibung 5.4 Dimension Handlungskompetenz

5.5	**Die Schüler erläutern die Gefahr von Spam-Mails, schätzen den Verdacht solcher E-Mails anhand von Merkmalen ein und löschen diese sofort.**	**DSK5**
	Zu Beginn muss der Begriff *Spam-Mail* geklärt sein. Dies kann an beispielhaft ausgewählten unterschiedlichen E-Mail-Beispielen geschehen, an denen die Schüler selbst entscheiden, ob eine Spam-Mail vorliegt oder nicht. Die Merkmale, durch die Spam-Mails gekennzeichnet sind, können herausgearbeitet und in entsprechende Regeln gefasst werden, die im Klassenzimmer ausgehangen werden. Im nächsten Schritt müssen die Gefahren, die von Spam-Mails ausgehen können, betrachtet werden, wozu die Lehrkraft passende Beispiele vorstellt. Durch die Möglichkeit, dass ein Rechner durch Malware infiziert oder ein Rechner fremdgesteuert wird, können Schüler sensibilisiert werden, unerwartete E-Mails, deren Absender man nicht kennt, misstrauisch zu betrachten. Aber auch die Gefahr, dass einem der Absender bekannt ist, heißt nicht, dass diese E-Mail auch von diesem geschrieben und versandt worden ist. Im Zweifelsfall bietet es sich an, vorher rückzufragen. Eine Spam-Mail alleine richtet noch keinen Schaden an, erst durch das Öffnen von Dateianhängen oder dem Anklicken eines Links wird die Infizierung gestartet. Wenn auch die Nutzung von E-Mails unter den Jugendlichen inzwischen eher selten ist (vgl. Abschnitt 2.3.2), so müssen den Schülern die Verhaltensregeln im Umgang mit und das Erkennen von Spam-Mail bekannt sein.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 2.7	

Tab. 6.6-e: Lernzielbeschreibung 5.5 Dimension Handlungskompetenz

5.6	**Die Schüler erklären die Notwendigkeit der Aktualisierung von Software und führen Updates aus.**	**DSK15**
	Die Schüler müssen lernen, dass jede Software nie frei von Programmierfehlern ist, die entweder die ordnungsgemäße Lauffähigkeit nicht zulassen oder Verbrechern als Einfalltor in Informatiksysteme dienen, und dass Updates die Sicherheit und Lauffähigkeit der Software erhöhen. In vielen Fällen werden Updates von einem Programm automatisch im Hintergrund ausgeführt, sodass der Nutzer sich darum nicht weiter sorgen muss, sofern diese Funktion aktiviert ist. Daher sollte die Lehrkraft mit den Schülern gemeinsam Update-Einstellungen von Betriebssystem und Software wie *Browser*, *Anti-Viren-Software* und *Office-Produkten* prüfen und bei Bedarf ausführen. Für die Notwendigkeit der Updates sind die Schüler zu sensibilisieren.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 2.7, 3.1 und 5.4	

Tab. 6.6-f Lernzielbeschreibung 5.6 Dimension Handlungskompetenz

5.7	**Die Schüler überprüfen ihre Online-Zeit (unter anderem aufgrund hoher Sicherheitsrisiken) und handeln entsprechend.**	**DSK16**
	Die Zeit, die Kinder und Jugendliche mit digitalen Medien und insbesondere dem Smartphone verbringen, ist sehr hoch (vgl. Abschnitt 2.3.2).[202] Daher ist es nicht nur aufgrund von Sicherheitsrisiken und eventuell anfallenden Kosten sinnvoll, die Schüler zu einer achtsamen und kontrollierten Smartphonenutzung zu erziehen. Sie könnten z. B. ihre Smartphonenutzung tabellarisch protokollieren und damit die eigene online-Zeit berechnen. Auch auf dem Markt verfügbare Smartphone-Apps könnten dies leisten (z. B. *QualityTime*[203] für Android oder *Moment*[204] für iOS), jedoch wird hier jede Form der Nutzung minutengenau aufgezeichnet, d. h. der Nutzer steht unter Fremdbeobachtung. Und genau hier kann eine Diskussion über Datenschutz ansetzen. Auch die sehr beliebten Fitnessarmbänder, die sogar in der Lage sein sollen, die Schlafqualität zu analysieren, bieten einen guten Zugang zu dem Thema. Die Nutzungshäufigkeit (außerhalb des eigenen Unterrichts) kann und soll auch nicht durch die Lehrkraft kontrolliert werden, jedoch ist das Ziel erreicht, wenn der Smartphonegebrauch überdacht wird.	
	Verknüpfung mit Lernzielbeschreibung: 1.1, 2.7	

Tab. 6.6-g: Lernzielbeschreibung 5.7 Dimension Handlungskompetenz

Die folgende Abbildung stellt zusammenfassend dar, wie eine jeweilige einzelne Lernzielbeschreibung in Verbindung mit anderen Lernzielbeschreibungen steht. Jede Lernzielbeschreibung ist durch einen Knoten und die entsprechenden Verknüpfungen durch Kanten dargestellt, wobei die Kanten zur Lernzielbeschreibung 1.1, die sich über den gesamten Bereich erstreckt, nur angedeutet worden sind, um die Übersichtlichkeit des Graphen zu gewährleisten.

[202] Manfred Spitzer prägte vor einigen Jahren den Begriff der *digitalen Demenz*, um damit auf die Probleme des übermäßigen Konsums digitaler Medien bei Kindern und Jugendlichen hinzuweisen. (vgl. https://de.wikipedia.org/wiki/Digitale_Demenz und https://www.youtube.com/watch?v=MRrPbNLhEuQ; zuletzt geprüft am 31.12.19)

[203] Siehe https://www.qualitytimeapp.com/ (zuletzt geprüft am 05.01.20)

[204] Siehe https://www.chip.de/downloads/Moment-iPhone-_-iPad-App_81310672.html (zuletzt geprüft am 05.01.20)

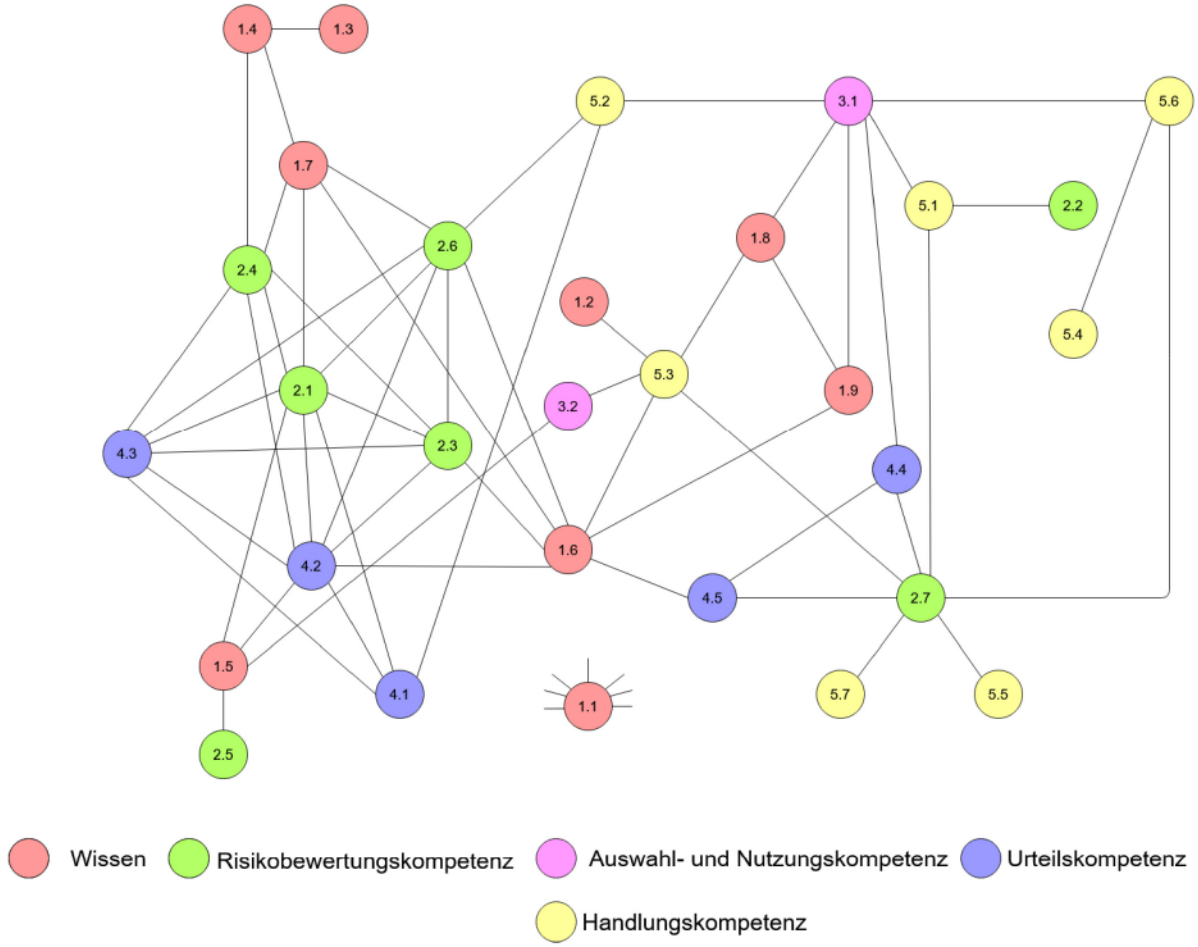


Abb. 6.1: Darstellung der Zusammenhänge zwischen den einzelnen Lernzielbeschreibungen

Man kann deutlich erkennen, wie die einzelnen Lernziele sich gegenseitig beeinflussen. Bei der Gestaltung eines Lehr-Lern-Settings kann dieses Bild insoweit eine Hilfe sein, um passende thematische Verknüpfungen bzw. Anknüpfungspunkte zu finden. So können z. B. mit Lernzielbeschreibung 1.6 (Tracking des Surfverhaltens) gleichzeitig die Lernzielbeschreibungen 1.7 (zweckfremde Nutzung persönlicher Daten), 1.9 (Maßnahmen zur Erschwernis der Nachverfolgung im Netz), 2.3 (Gefahrabschätzung zweckfremder Datennutzung), 2.6 (Information über Tätigkeit und/oder Aufenthaltsort), 4.2 (Beurteilung der Veröffentlichung von Daten und den Folgen), 4.5 (Gefahr von Werbebannern) und 5.3 (Kenntnis sicherer Webseiten) thematisiert werden, sodass anhand konkreter Vorfälle (die aus Presseberichten oder Materialien genommen werden können) Inhalte zur Kompetenzförderung verschiedener Dimensionen zur Verfügung stehen.

Im Rahmen der Studie war den Schülern die Möglichkeit gegeben worden, Themenwünsche zu äußern (vgl. Abschnitt 4.5). Folgende tabellarische Übersicht stellt die Themen den entsprechenden Lernzielbeschreibungen gegenüber:

Thema	Anteil[205]	Lernzielbeschreibungen
Gefahren beim Surfen	65 %	1.1, 1.2, 1.6, 1.7, 1.8, 2.3, 2.4, 2.6, 2.7, 4.5, 5.3, 5.5, 5.7
Schutz von Daten	65 %	1.1, 1.5, 1.6, 1.7, 1.8, 1.9, 2.1, 2.3, 2.4, 2.6, 4.1, 4.2, 4.3, 5.1, 5.2, 5.4, 5.6
Technische Möglichkeiten[206]	55 %	1.1, 1.6, 1.9, 2.6, 2.7, 3.1, 4.4, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7
Rechtliche Situation	46 %	1.1, 1.3, 1.4, 1.5, 1.6, 1.7, 2.3, 2.4, 2.5, 3.2

Tab. 6.7: Gegenüberstellung der Themen der Befragung und der Lernzielbeschreibungen

Man erkennt, dass sich die Interessen der Schüler deutlich mit den Lernzielbeschreibungen decken. Rückblickend kann der Autor zudem feststellen, dass bei allen Unterrichtsbesuchen, die im Rahmen der Projekte (vgl. Kapitel 5) stattgefunden haben und denen er beigewohnt hat, seitens der Schüler immer eine sehr starke Aufmerksamkeit für die Themen vorhanden war.

6.3. Unterrichtsprojekte im Kontext der Lernzielbeschreibungen

In Kapitel 5 werden zwei Projekte vorgestellt (vgl. Abschnitt 5.1.1 (Thielen 2018) und Abschnitt 5.1.2 (Savelsberg 2019)), die auf den Unterricht für die Orientierungsstufe abgestimmt sind. Beide Projekte zielen vor allem auf die Lernzielbeschreibungen 1.1, 1.2, 1.3, 1.5, 1.8, 1.9, 2.1, 2.3, 2.6, 3.1, 4.2, 4.3 und 5.1 ab. Ausgehend von diesem Punkt können diese Unterrichtseinheiten zur Stärkung weiterer Lernzielbeschreibungen auch weiter ausgebaut werden. Die in Abschnitt 5.1.6 beschriebene Arbeit (Böhm 2015) für die Sekundarstufe II bietet einen Fundus an Ideen zur Unterrichtsgestaltung, muss jedoch auf das entsprechend jüngere Alter der Jugendlichen angepasst werden. Somit können diese Konzepte als Ausgangspunkte für die weitere Arbeit zur Förderung der Datenschutzkompetenz dienen.

In dem Projekt von (Kramer und Spaeing 2014, S. 373), welches auf singuläre Besuche in einzelnen Klassen ausgelegt ist, wird ein Curriculum vorgestellt, das in dieser Form ebenfalls im Unterricht so umgesetzt werden kann. Die folgende Tabelle stellt das Curriculum und die Zuordnung zu den Lernzielbeschreibungen dar:

[205] Gerundeter prozentualer Anteil der Befürworter
[206] Hier werden alle Schutzmöglichkeiten zusammengefasst und nicht nur die, die technischer Art sind.

Phase	Inhalt	Lernzielbeschreibung
1	Der Einstieg erfolgt über den Begriff der sog. „Freunde“ in Sozialen Netzwerken; ein Filmbeitrag untermauert die Handlungsstrategien der Anbieter.	1.7
2	Dem folgt dem Alter entsprechend die Einführung des Begriffs *Datenschutz* ohne dabei Gesetze zu thematisieren.	1.3, 1.4
3	Im nächsten Schritt steht die Charakterisierung dessen, was personenbezogene Daten sind; dabei wird bei den Interessenten solcher Daten differenziert zwischen denen, die berechtigtes Interesse haben, und denen, die die Angaben freiwillig mitgeteilt bekommen, und denen, die sich mit betrügerischen Absichten Zugang dazu verschaffen.	1.7, 2.1, 2.3, 2.4
In dem Projekt folgt bei einem Schulbesuch an dieser Stelle eine Schwerpunktsetzung durch Auswahl einzelner Phasen, jedoch sind alle folgenden Punkte wichtig, um im Unterricht besprochen zu werden.		
4	Das Internet als „allumfassende Informationsquelle, die auch nichts vergisst“, steht als nächstes im Mittelpunkt der Betrachtungen; dass einmal veröffentlichte Daten so gut wie nicht mehr gelöscht werden können, muss den Schülern klar werden; über die IP-Adresse ist eine Identifizierung möglich.	2.3, 4.2, 4.3
5	Die Veröffentlichung persönlicher oder intimer Informationen im Web 2.0 oder in Sozialen Netzwerken kann verheerende Folgen haben, sodass über eine Veröffentlichung vorher genau nachgedacht werden muss; als negative Folge werden Probleme im Rahmen von Bewerbungsverfahren genannt; zudem wird eine Warnung vor Straftätern ausgesprochen, die sich unter falschen Daten in Sozialen Netzwerken anmelden, um nach Opfern zu suchen; trotz einer Altersbeschränkung Sozialer Netzwerke werden diese Plattformen von Kindern und Jugendlichen sehr gerne genutzt.	1.5, 1.7, 2.1, 2.3, 2.4, 2.6, 4.1, 4.2, 4.3, 5.2
6	Videochats können ein weiteres Problemfeld darstellen; die Zweckentfremdung der Webcam und die Gefahr von Webcam-Spannern werden thematisiert.	2.3, 2.4
7	Im Block *Handy und Smartphone* wird aufgezeigt, wie Daten geschützt werden können; in diesem Zusammenhang werden auch das „Recht am eigenen Bild“, die Handyortung, „Missbrauchsszenarien“ und das „Sexting und Treffen mit Cyberfreunden“ behandelt.	1.5, 1.7, 2.3, 2.4, 2.6
8	Anhand „Konsequenzen illegaler Downloads“ und „legale[n] Alternativen“, die vorgestellt werden, wird das Thema *Urheberrecht* in das Curriculum eingebracht.	3.2

Tab. 6.8a: Zuordnung der Lernzielbeschreibungen zum Curriculum von Kramer und Spaeing

Phase	Inhalt	Lernzielbeschreibung
9	Regeln für die Erstellung von sicheren Passwörtern und der Beachtung, für verschiedene Zugänge auch verschiedene Passwörter zu nutzen, wird der Aspekt der sicheren Passwörter beleuchtet.	5.1
10	Mit der Einheit *PC-Sicherheit* stehen „Schutzmechanismen wie Virenscanner, Firewalls, Updates, WLAN-Verschlüsselung und Datensicherung“ im Vordergrund; wegen der „Sterblichkeit“ der Hardware wird der Datensicherung eine besondere Aufmerksamkeit geschenkt.	2.7, 3.1, 4.4, 5.4, 5.6
11	Im Rahmen des Themas *Cyber-Mobbing* erfolgt eine Information über „die geltenden Gesetze“ und „technischen Möglichkeiten“, um „einen ‚Mobber‘ dingfest zu machen“; zudem ist es wichtig, dass Betroffene sich Vertrauenspersonen öffnen.	2.5
12	Abschließende Verhaltensregeln runden das Projekt ab.[207]	

Tab. 6.8b: Zuordnung der Lernzielbeschreibungen zum Curriculum von Kramer und Spaeing

Die Gegenüberstellung zeigt, dass insbesondere die Lernzielbeschreibungen 1.7, 2.3 und 2.4 innerhalb dieses Curriculums stark vertreten sind. Die Beschreibung 1.1 spielt prinzipiell in alle Bereiche des Curriculums rein. Weniger stark sind 1.3, 1.4, 1.5, 2.1, 2.6, 2.7, 3.1, 3.2, 4.1, 4.2, 4.3, 4.4, 5.1, 5.2, 5.4 und 5.6 vertreten.

In Abschnitt 2.4 wird der Vorschlag einer IniK[208]-Unterrichtsreihe von (Diethelm 2011) vorgestellt, bei der das Thema *Datenschutz* den ersten Teil darstellt. Methodisch orientiert sie sich am forschend-entdeckenden Lernen, da der Themenbereich „nicht eng abgesteckt und nicht mit einer klaren Aufgaben- und Zielvorstellung versehen ist“ (Diethelm 2011, S. 29). Auch wenn diese Reihe für einen Grundkurs der Jahrgangsstufe 11 als Einstieg in das Fach *Informatik* gestaltet ist, so kann sie auszugsweise deutlich didaktisch reduziert mit jüngeren Schülern behandelt werden. Da der Autor diesen Vorschlag der Unterrichtsreihe für gelungen hält, wird trotz der angedachten Altersgruppe an dieser Stelle auf ihn eingegangen. Die folgende Tabelle stellt knapp den Ablauf der Reihe und die Zuordnung zu den Lernzielbeschreibungen dar; Bemerkungen zur Übertragung der Unterrichtseinheit auf die Orientierungsstufe sind in kursiver Schrift gehalten:

[207] Diese sind: „Schütze Dich und Deine Daten. Sei misstrauisch, glaube nicht alles. Halte Dein Passwort geheim. Keine illegalen Downloads. Vorsicht bei Treffen mit Cyber-‚Freunden‘. Sei auch im Netz immer fair. Bist Du unsicher, frage nach“ (Kramer und Spaeing 2014, S. 374).

[208] IniK ist die Abkürzung für *Informatik im Kontext*; vgl. dazu Abschnitt 2.4.

Phase	Inhalt	Lernzielbeschreibung
1	Thema: *Kurszählung – Fragen zum Datenschutz* Einstieg über einen Befragungsbogen *Kurszählung*, der nach dem Ausfüllen zerrissen wird, um die Schüler emotional zu motivieren, da sie bereit waren, ihre Daten freiwillig preis zu geben; anschließend werden Fragen zum Zweck der Datenschutzgesetze, zur informationellen Selbstbestimmung oder zur Datenvermeidung gesammelt und schriftlich in Gruppenarbeit durch Internetrecherche beantwortet; Hausaufgabe ist die Befragung der Eltern nach dem Volkszählungsurteil 1983 und dem Zensus 2011. *Nach dem Einstieg durch einen für das Alter passend gestalteten Fragebogen müssen die Schüler an das Thema im Unterrichtsgespräch ohne juristischen Hintergrund herangeführt werden. Entsprechend altersgerecht aufgearbeitete Unterrichtsmaterialien können hier eingesetzt werden. Die Hausaufgabe einer Befragung der Eltern (oder Großeltern) könnte durch vertiefende Aufgaben ersetzt werden (z. B. konstruierte Fälle vorlegen und begründet entscheiden, ob eine Verletzung des Datenschutzes vorliegt oder nicht).*	1.3, 1.4, 1.5, 1.7, 2.1, 2.4
2	Thema: *Datenschutz als Grundrecht?* Zu Beginn werden die Hausaufgaben besprochen und herausgearbeitet, dass Datenschutz kein Grundrecht ist, aber aus dem Grundgesetz abgeleitet wird; „die Bedeutung des Datenschutzes auf sich selbst beziehen und entdeckend reflektieren“ bilden den Kern der zweiten Phase (Liste über Mitgliedschaften und den in Verein/Firmen gespeicherten Daten führen); Einverständniserklärung für die Eltern formulieren, dass die Jugendlichen ihre Daten weitergeben dürfen. Alternative für ältere Schüler: Firma anschreiben und um Auskunft der über sie gespeicherten Daten bitten. *Dieser Block ist für die Schüler der Orientierungsstufe noch nicht von Bedeutung, da der juristische Hintergrund für die Schüler zu abstrakt und unverständlich ist. Sie könnten aber z. B. auflisten, wer vermutlich welche persönlichen Daten über sie gespeichert hat. Hierdurch kann schon eine erste Sensibilisierung eingeleitet werden.*	

Tab. 6.9a: Zuordnung der Lernzielbeschreibungen zum Verlaufsplan von Diethelm

Phase	Inhalt	Lernzielbeschreibung
3	Thema: *Alltag Überwachung – Kameras und RFID* Die Leitfrage lautet, ob zur Sicherheit auf dem Schulgelände Kameras installiert werden sollten; Ziel ist zu erkennen, wie Beobachtung Verhalten beeinflusst und letztendlich der Demokratie schadet; ein Bezug zum Artikel 2 des Grundgesetzes herstellen; Unterstützung des Themas durch Filmbeiträge. *Der Inhalt dieser Einheit ist zu anspruchsvoll für die Lernenden. Der einzige anzusprechende Aspekt aus diesem Block wäre gegebenenfalls sich bewusst zu machen, dass eine zu starke Beobachtung zu konformen Verhalten der Beobachteten führen wird. Da aber noch kein Demokratieverständnis vorhanden ist, bleibt dieser Punkt singulär und bietet keine weitere Anknüpfung.*	2.3, 2.4, 2.6
4	Thema: *Die Macht einer Suchmaschine* Einstieg über einen Filmbeitrag zu Google, den die Autorin erst für Schüler ab 15 Jahren empfiehlt, da er beängstigend ist; Fragen über die eigene Weitergabe von Daten an Google und das Sammeln von Daten durch Google; Schutz der Privatsphäre; Datenschutzvorfälle recherchieren und diskutieren. *An dieser Stelle bietet sich die Vorstellung geeigneter Suchmaschinen als Alternative zu Google an, denn die Zusammenhänge der Google-Sammelwut und deren Folgen können von den Schülern noch nicht vollständig erfasst werden. Hier muss die Lehrkraft unterstützend wirken.*	1.3, 1.4, 1.6, 1.7, 1.8, 1.9, 2.3, 2.4, 2.6, 3.1, 4.2, 4.3, 5.3
5	Thema: *Wie funktioniert das Internet?*[209] Durch Filmbeiträge und Rollenspiel die Funktionsweise herausarbeiten und grundlegende Begriffe klären. *Dieses Thema sollte unabhängig vom Thema Datenschutz zu einem anderen Zeitpunkt behandelt werden, um den Fokus für die Lernenden ausschließlich auf den Datenschutz zu lenken.*	1.1, 1.2, 1.8, 1.9

Tab. 6.9b: Zuordnung der Lernzielbeschreibungen zum Verlaufsplan von Diethelm

[209] Diese Phase wird nicht ausführlicher beschrieben, da sie nur indirekt mit dem Thema *Datenschutz* zu tun hat.

Phase	Inhalt	Lernzielbeschreibung
6	Thema: *Vorratsdatenspeicherung* Anhand von Fernsehberichten werden die Informationen zur Verfügung gestellt; Gründe für die Vorratsdatenspeicherung erarbeiten und das Urteil des Bundesverfassungsgerichts nachvollziehen. *Dieses Thema übertrifft ebenfalls das Verständnis für die Schüler, da es zu abstrakt ist und insbesondere für sie kein Alltagsbezug besitzt.*	1.3, 1.7, 2.3
7	Thema: *Raubkopie – Was ist eigentlich erlaubt?* Klärung der Begriffsteile des Worts *Raubkopie* und Formulierung von Fragen in diesem Zusammenhang, die in Gruppenarbeit mithilfe von Material geklärt werden; das Thema *Tauschbörse* kann angesprochen werden. *Im Gegensatz zu den vorherigen Phasen ist dieses Thema für die Schüler von Bedeutung, da Daten untereinander gerne ausgetauscht werden und dabei möglicherweise Rechtsverletzungen begangen werden können. Ausgehend von Alltagsbeispielen (z. B. Streamen, Aufzeichnen und Weitergabe von Musik) können die Fragen um das Urheberrecht behandelt und richtiges Verhalten herausgestellt werden. Altersgerechte Materialien hierzu stehen in ausreichender Anzahl im Netz zur Verfügung.*	1.6, 1.8, 2.7, 3.2, 4.5, 5.3, 5.4
8	Thema: *Antworten zum Urheberrecht* Die Antworten zu den Fragen aus Phase 7 werden besprochen und eine Präsentation für die Schulgemeinschaft vorbereitet (Plakat, Rollenspiel). *Eine Präsentation in Form von Plakaten ist ebenfalls eine passende Methode für die jüngeren Schüler. Es wäre dann eine Zusammenfassung des Phase 7.*	
9	Thema: *Filesharing* Klärung der Fragen nach der Funktionsweise und Strafverfolgung beim Filesharing und nach dem Brennen von CD; Posterpräsentation der Ergebnisse. *Filesharing betrifft die Altersgruppe z. B. im Zusammenhang mit dem Tausch von Computerspielen. Dies kann in Phase 7 subsummiert werden.*	

Tab. 6.9c: Zuordnung der Lernzielbeschreibungen zum Verlaufsplan von Diethelm

Phase	Inhalt	Lernzielbeschreibung
10	Thema: *Tauschbörsen – Pro und Kontra* In Form eines Rollenspiels (mit den Rollen *Internetuser*, *Künstler*, *Tauschbörsenbetreiber*, *Produktionsfirma*) die Inhalte wiederholen. *Das Thema sollte mit den vorhergehenden Phasen ausreichend behandelt worden sein, sodass durch ein Rollenspiel kein Mehrgewinn zu erwarten ist.*	

Tab. 6.9d: Zuordnung der Lernzielbeschreibungen zum Verlaufsplan von Diethelm

Die Gegenüberstellung zeigt, dass insbesondere die Lernzielbeschreibungen 1.3, 1.7, 1.8, 2.3 und 2.4 innerhalb dieses Projekts stark und die Lernzielbeschreibungen 1.4, 1.6, 1.9 und 2.6 häufig vertreten sind. Eine geringe Rolle spielen die Lernzielbeschreibungen 1.1, 1.2, 1.5, 2.1, 2.7, 3.1, 3.2, 4.2, 4.3, 4.5, 5.3 und 5.4.

Die vorgestellten Unterrichtsprojekte decken alle einen großen Teil der Lernzielbeschreibungen ab, sodass sich anbietet – neben den Projekten aus Kapitel 5 – auch mit diesen Ideen und Ansätzen weiterzuarbeiten. Bei den zu verwendenden Materialien ist jedoch auf die Aktualität in Bezug auf die genutzten Beispiele (und auf die Rechtslage im Bereich *Datenschutz*) zu achten. In der Regel sind Unterlagen, die zeitlose Aspekte behandeln, von Vorteil. Da aber gerade das Gebiet des Datenschutzes stetiger Fortentwicklung unterworfen ist, wird es kaum solche Unterrichtsmaterialien geben können, die über einen langen Zeitraum in der jeweils ausgearbeiteten Form Gültigkeit haben werden. Auch die in Kapitel 5 vorgestellten neueren Unterrichtsbeiträge müssen in regelmäßigen Abständen genauso darauf hin überprüft werden, wie der Einsatz von Werkzeugen, die eine technische Maßnahme zum Selbstdatenschutz darstellen (z. B. einen Werbefilter wie *Adblock Plus*[210], eine Anti-Tracking-Software wie *Ghostery*[211] oder *Disconnect Mobile*[212] oder einen Passwortmanager wie *KeePassX*[213]).

Die in diesem Abschnitt formulierten Lernzielbeschreibungen können den Anfang einer solchen Liste darstellen. Sollten sich bei der Materialerstellung oder den Unterrichtsbeobachtungen weitere Lernziele entwickeln, dann böte es sich an, diese einer Dimension des Datenschutzkompetenzmodells zuzuordnen und mit den vorhandenen Lernzielbeschreibungen zu verknüpfen. Es ist jedoch darauf zu achten, dass die Liste wegen der Übersichtlichkeit nicht zu lang wird. Gegebenenfalls besteht die Möglichkeit, ähnliche Lernzielbeschreibungen zusammenzufassen.

[210] Siehe https://adblockplus.org/de/ (zuletzt geprüft am 05.01.20)
[211] Siehe https://www.ghostery.com/de/ (zuletzt geprüft am 05.01.20)
[212] Siehe https://disconnect.me/ (zuletzt geprüft am 05.01.20)
[213] Siehe https://www.keepassx.org/ (zuletzt geprüft am 05.01.20)

Des Weiteren ist die Entwicklung eines Curriculums im Sinne eines Spiralcurriculums zu bedenken, denn damit bietet sich die Gelegenheit, das Thema *Datenschutz* wiederkehrend in verschiedenen Klassenstufen aufzugreifen und den aktuellen Umständen anzupassen. Durch den wiederholenden Charakter wird ein höherer Lernerfolg garantiert. Da zudem die Erfahrung der Schüler im Rahmen der Internetnutzung mit dem Alter steigt, können die Lernenden verstärkt eigene Erfahrungen in den Unterricht einbringen.

6.4. Drittes Zwischenergebnis

Die dritte Forschungsfrage lautet:

> Wie könnte dem Mangel an Datenschutzkompetenz begegnet bzw. dieser behoben werden?

Hierzu sind ausgehend von den Ergebnissen der Untersuchung (vgl. Kapitel 4) Lernzielbeschreibungen abgeleitet worden, die in den Tabellen 6.2 bis 6.6 gelistet sind. Diese stehen in Zusammenhang mit den in Tabelle 3.8 formulierten Datenschutzkompetenzen. Somit schließt sich an dieser Stelle der Kreis der Betrachtungen und das Datenschutzkompetenzmodell, die Untersuchung und die Lernzielbeschreibungen bilden eine Einheit. Abschließend sind in Abschnitt 6.3 die Lernzielbeschreibungen schon vorhandenen Unterrichtsprojekten zugeordnet.

Die nächsten Schritte sind, aus den Lernzielbeschreibungen unter Verwendung vorhandener guter Materialien und Unterrichtsprojekten konkrete Unterrichtsreihen bzw. Curricula zu entwerfen, die im Feldversuch zu testen und zu evaluieren sind.

„Durch das Recht auf informationelle Selbstbestimmung ist der Mensch
kein aus einer Masse von Daten zusammengesetztes Wesen,
sondern ein Individuum in der Gesellschaft."
Zusammengefasst von (Noll 2019, S. 26)
nach (Egger und Schillinger 1996, S. 53)

7. Zusammenfassung der Ergebnisse und Ausblick

Kinder und Jugendliche kommen schon im Grundschulalter mit dem Computer (und anderen Erscheinungsformen wie Tablet-PC oder Smartphone) und dem Medium Internet in Berührung, sodass sie sich in einem Alter ab zehn Jahren, nicht selten ohne elterliche oder erzieherische Begleitung, in das weltweite Netz aufmachen. Daher müssen sie mit einem Rüstzeug an Grundlagen ausgestattet sein, um sich und andere vor Gefahren im Zusammenhang mit der Internetnutzung schützen und Risiken einschätzen zu können. Eine der Grundlagen ist ein datenschutzkompetentes Verhalten, dem sich die vorliegende Arbeit widmet.

Ausgangspunkt ist die Fragestellung nach der Datenschutzkompetenz bei Jugendlichen im Alter von zehn bis 13 Jahren. Speziell dazu gibt es keine Studie, die dies untersucht hat. Zugleich ist die Frage nach dem, was Datenschutzkompetenz ist und ausmacht, nicht ausreichend beantwortet. Der Begriff wird zwar häufig in der Literatur und Presse genutzt, aber ohne sauber definiert zu sein.

Unter diesem Blickwinkel standen folgende Forschungsfragen im Fokus der Betrachtungen:

1) Wie kann man Datenschutzkompetenz konzeptualisieren?

2) In welchen Dimensionen des in dieser Arbeit hergeleiteten Datenschutzkompetenzmodells weisen Schüler der Klassenstufe 5 bis 7 einen Mangel an Datenschutzkompetenz auf?

3) Wie könnte dem Mangel an Datenschutzkompetenz begegnet bzw. dieser behoben werden?

Zur Beantwortung der ersten Frage wurde ein Datenschutzkompetenzmodell (vgl. Abschnitt 3.4) entwickelt, welches aus einem Medienkompetenzmodell (vgl. Abschnitt 3.1) und einem Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse (vgl. Abschnitt 3.3) in Verbindung mit einem Vertrauensmodell (vgl. Abschnitt 3.2) entstand. Das Modell ist durch fünf Dimensionen charakterisiert:

1. Wissen
2. Risikobewertungskompetenz
3. Auswahl- und Nutzungskompetenz
4. Urteilskompetenz
5. Handlungskompetenz.

Datenschutzkompetenz kann als Zusammenschluss von Wissen, Risikobewertungskompetenz, Auswahl- und Nutzungskompetenz, Urteilskompetenz und Handlungskompetenz mit Bezug auf das schützenswerte Gut der persönlichen Daten definiert werden. Eine Person gilt als datenschutzkompetent, wenn sie in allen diesen Dimensionen ein ausreichendes Maß an Kompetenz besitzt. Für das ausreichende Maß wiederum werden 17 Datenschutzkompetenzen formuliert (vgl. Tabelle 3.8), die Basiskompetenzen und damit Mindestanforderungen darstellen und aus den Bildungsstandards für das Fach *Informatik* abgeleitet sind.

Zur Beantwortung der zweiten Frage wurde im Winter 2017/18 an allgemeinbildenden rheinland-pfälzischen Schulen in den Klassenstufen 5 bis 7 eine Studie durchgeführt. Die dafür verwendeten Items stammen aus unterschiedlichen vorangegangenen Studien, die in irgendeiner Art und Weise im Zusammenhang mit dem Thema *Datenschutz* stehen. Knapp 1000 brauchbare Datensätze konnten bei der Erhebung generiert werden, die für eine deskriptive Auswertung und eine bivariate Analyse zur Verfügung standen.

Die deskriptive Auswertung (vgl. Abschnitte 4.3.3.1 und 4.3.3.3) zeigte, dass die Befragten in allen Dimensionsbereichen sehr schlecht abschnitten. Während die Risikobewertungskompetenz und die Urteilskompetenz noch als ausreichend bezeichnet werden können, schneiden die Schüler in den anderen Dimensionsbereichen mangelhaft ab. Im Bereich *Wissen* sind Grundbegriffe wie *Firewall* oder *Cookie* nicht bekannt, genauso wenig wie ihre Rechte, die sich aus der DSGVO und Datenschutzerklärungen ergeben. Durch ein etwas größeres Wissen sind die älteren Schüler[214] den jüngeren geringfügig überlegen. Die Sensibilität unterschiedlicher persönlicher Daten (um sie in sozialen Netzwerken anzugeben) können die Jugendlichen einerseits ordentlich abschätzen und Risiken im Internet einschätzen, andererseits werden Anhänge von E-Mails oder zugesandte Download-Links unbedacht geöffnet. In der Risikobewertungskompetenz sind die jüngeren Befragten den älteren überlegen, weil sie sich vermutlich vorsichtiger im Internetumgang verhalten, während die älteren eine höhere Risikobereitschaft besitzen und mehr Erfahrung in der Internetnutzung haben. Die mangelhafte Auswahl- und Nutzungskompetenz ist alters- und geschlechtsunabhängig. Die Defizite sind bei den Mädchen größer als bei den eher technisch interessierten Jungen. Technische Maßnahmen für eine sichere Internetnutzung sind größtenteils nicht bekannt und werden, wo bekannt, noch weniger genutzt. Im Bereich der *Urteilskompetenz* sind die Ergebnisse der Mädchen besser, da insbesondere die älteren unter ihnen vorsichtiger und überlegter agieren. Die Mehrheit der Befragten ändert ihre persönlichen Einstellungen in Sozialen Netzwerken nicht, da sie den Anbietern dieser Plattformen vertraut. Aber die Jugendlichen denken darüber nach, welche Inhalte andere Personen z. B. bei einem Post später sehen können, und klicken reizvoll klingende Werbebanner nicht an. Eine deutliche Mehrheit achtet auf die Informationen, die sie ins Internet stellt. Passwortgeschützte Geräte und verschiedene Passwörter werden mehrheitlich genutzt, jedoch werden diese nicht regelmäßig geändert. Daten-Back-Ups oder ein

[214] Dies bezeichnet die Schülergruppe im Alter zwölf und 13 Jahre.

Viren-Scan der Festplatte werden nur selten ausgeführt und weniger als die Hälfte der Befragten hält ihre Software auf dem neuesten Stand. Das Alter und das Geschlecht haben keinen Einfluss auf die Handlungskompetenz.

Zusammenfassend kann man feststellen, dass die Chancen und Risiken der Internetnutzung wahrgenommen werden, aber dies führt nicht zu einer Verstärkung der Sicherheitsanforderungen. Es fehlt an einem fachlichen Hintergrund und Verständnis. Die Beweggründe könnten durch Interviews hinterfragt werden, was eine interessante Fortführung der Arbeit darstellen würde.

Um eine etwaige (Un-)Abhängigkeit der Dimensionen des Modells aufzuzeigen, wurden die Korrelationen zwischen den einzelnen Dimensionen berechnet (vgl. Abschnitt 4.3.3.2). Dabei zeigte sich mit Ausnahme des Paars *Wissen* und *Risikobewertungskompetenz* überall eine schwache bis mittlere Korrelation. Mit Ausnahme des Paars *Risikobewertungskompetenz* und *Auswahl- und Nutzungskompetenz* und des Paars *Auswahl- und Nutzungskompetenz* und *Urteilskompetenz* sind die Korrelationskoeffizienten positiv.[215] Daraus kann geschlossen werden, dass die Dimensionen miteinander zusammenhängen und dass das Wissen und die Dimensionskompetenzen nicht getrennt voneinander gefördert werden können, d. h. sie sind ganzheitlich zu betrachten.

Zur Beantwortung der dritten Frage wurden aus den Ergebnissen der Studie Handlungsempfehlungen abgeleitet. Dies geschah durch Formulierung von 30 Lernzielbeschreibungen, die in Beziehung mit den aus dem Modell abgeleiteten Datenschutzkompetenzen stehen.

Ein nächster Schritt könnte sein, aus den Handlungsempfehlungen bzw. Lernzielbeschreibungen ein Curriculum zu entwerfen, welches sich am Ende über die gesamte Sekundarstufe erstreckt und in Form eines Spiralcurriculums aufgebaut ist. Dabei könnten die in Kapitel 5 vorgestellten Unterrichtsreihen und -materialien einen Beitrag leisten, indem sie auf dieses Curriculum abgestimmt werden. Zudem bieten die Projekte von (Kramer und Spaeing 2014) und (Diethelm 2011) Ansätze, bei denen es sich lohnt, sie weiter zu verfolgen. Weitere Materialien, die in der Arbeit von (Makosch 2019) anhand eines Kriterienkatalogs auf ihre Qualität hin untersucht worden sind und zu denen keine dokumentierten Rückmeldungen aus der Praxis vorliegen, könnten hinzugezogen und deren Erfolg im unterrichtlichen Einsatz geprüft werden. Das so entwickelte Curriculum und die Materialien müssten in einem abschließenden Schritt evaluiert und gegebenenfalls angepasst werden.

Da Informatik in Rheinland-Pfalz (noch) kein Pflichtfach in der Sekundarstufe, insbesondere in der Sekundarstufe I, ist, muss gleichzeitig bedacht werden, in welchem Zusammenhang in anderen Pflichtfächern die Lernziel- und Kompetenzförderung zum Thema *Datenschutz* erreicht werden kann. Dazu sind die Lehrpläne infrage kommender Fächer zu studieren und Anknüpfungspunkte herauszuarbeiten.

[215] Dies bedeutet, dass in der Mehrheit der Fälle mit einer größeren Kompetenz der ersten Dimension auch die Kompetenz der zweiten größer ist (und umgekehrt). Die beiden Ausnahmefälle bedeuten, dass mit einer größeren Kompetenz der ersten Dimension die Kompetenz der zweiten geringer ist (und umgekehrt).

Mit den ab Klassenstufe 1 gültigen Richtlinien der Verbraucherbildung (vgl. Abschnitt 2.2.2.3), in denen das Thema *Datenschutz* explizit genannt und entsprechende Kompetenzen formuliert sind, wird seit 2010 der Versuch unternommen, dieses Thema in den Schulunterricht der Primar- und Sekundarschulen zu integrieren. Wenn auch an der Untersuchung zu der vorliegenden Arbeit nur Schüler bis Klassenstufe 7 beteiligt waren, so kann in diesen Fällen nicht von einem erfolgreichen Konzept der Implementierung gesprochen werden, denn sonst hätten die Schüler besser abschneiden müssen. Wenn an dem Vorhaben der Verbraucherbildung festgehalten werden soll, dann wäre es sinnvoll, die Themen der einzelnen Bereiche *Finanzkompetenz und Konsum*, *Gesundheit und Ernährung* und *Datenschutz* verbindlich auf Jahrgangsstufen und Fächer festzuschreiben. Aber der Autor sieht dahingehend immer noch ein Problem, dass eine klar aufgezeigte Integration des Themas *Datenschutz* in ausgewählten Fächern vermutlich auch nur einen mäßigen Erfolg zeigen würde. Für den Misserfolg eines solchen Unterfangens sprächen die fehlende Fachexpertise vieler Lehrkräfte zu diesem Thema und die schon mit Lernstoff sehr ausgefüllten Lehrpläne.

Unabhängig von einem Curriculum und Materialien müssen daher die Lehrkräfte entsprechend ausgebildet sein. Sowohl in der Lehrerausbildung als auch in Form von Fortbildungen müssen passende Angebote eingerichtet werden. Dabei sollen neben der inhaltlichen Komponente (Wissen) auch didaktische und methodische Fragestellungen eine Rolle spielen. Die zurzeit herrschenden Probleme der Lehrer könnten sein, dass ihnen eine passende Ausbildung und das notwendige Wissen fehlt, sie sich daher mit dem Thema unsicher fühlen, gegebenenfalls das Thema auch nicht für unterrichtsrelevant erachten, keine passende Unterrichtsmaterialien kennen oder ihnen der Aufwand für das Anpassen der Materialien an die Lerngruppe oder an die Aktualität zu aufwendig ist. Durch entsprechende Weiterbildungen und Unterstützungen könnte diesen Problemen aber begegnet werden, um die Lehrkräfte für das Thema *Datenschutz* zu sensibilisieren und geeignete Materialien zur Verfügung zu stellen.

Der beste Weg aus Sicht des Autors wäre aber, die Thematik *Datenschutz* einem Pflichtfach *Informatik* zuzuweisen, welches in der Mehrheit der Bundesländer ebenso wie in Rheinland-Pfalz noch einzuführen wäre. Mit dem Schuljahr 2020/21 werden in Rheinland-Pfalz die ersten 21 sogenannten Informatik-Profil-Schulen starten, an denen alle Schüler ab der Klassenstufe 5 an dem Pflichtfach *Informatik* teilnehmen werden. Somit ist hier ein erster Schritt in die Richtung Pflichtfach getan. Damit die landesweite Einführung jedoch erfolgreich verlaufen wird, müssen zuerst entsprechende Lehrkräfte für das Fach *Informatik* aus- und fortgebildet werden. Dieser Prozess wird aber noch sehr viele Jahre dauern, sodass zwischenzeitlich mit dem integrativen Unterrichtskonzept weitergearbeitet werden muss. Ein anderer Weg ist, auf das in Abschnitt 2.4 beschriebene Angebot der Workshops des LfDI Rheinland-Pfalz zurückzugreifen, um die Datenschutzkompetenz der Schüler auszubilden. Auch wenn es sich hierbei nur um ein singuläres Konzept anstelle eines Lehr-Lern-Settings für den Unterricht handelt, ist dieses besser als die Augen vor der Realität und den Gefahren zu verschließen und das Thema *Datenschutz* im Unterricht zu verschweigen oder gar zu verbannen.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Acquisti, Alessandro; Gross, Ralph (2006): Imagined Communities. Awareness, Information Sharing, and Privacy on the Facebook. In: George Danezis und Philippe Golle (Hg.): Privacy enhancing technologies. PET 2006, 6th international workshop on Privacy Enhancing Technologies. Cambridge, UK, 28.-30.06.2006. Berlin, Heidelberg: Springer Verlag (Lecture notes in computer science, 4258), S. 36–58.

Altman, Irwin (1975): The environment and social behavior. Privacy, personal space, territory, crowding. Monterey, California: Brooks/Cole Publications.

Baacke, Dieter (1996): Medienkompetenz - Begrifflichkeit und sozialer Wandel. In: Antje von Rein (Hg.): Medienkompetenz als Schlüsselbegriff. 1. Aufl. Bad Heilbrunn: Julius Klinkhardt Verlag (Theorie und Praxis der Erwachsenenbildung), S. 112–124.

Baacke, Dieter (1998): Medienkompetenz - Herkunft, Reichweite und strategische Bedeutung eines Begriffs. In: Herbert Kubicek, Hans-Joachim Braczyk, Dieter Klumpp, Günter Müller, Werner Neu, Eckart Raubold und Alexander Roßnagel (Hg.): Lernort Multimedia. 1. Aufl. Heidelberg: Decker's Verlag (Jahrbuch Telekommunikation und Gesellschaft, 6), S. 22–27.

Baacke, Dieter (2004): Medienkompetenz als zentrales Operationsfeld von Projekten. In: Susanne Bergmann, Jürgen Lauffer, Lothar Mikos, Günter A. Thiele und Dieter Wiedemann (Hg.): Medienkompetenz. Modelle. Projekte. Bonn: Bundeszentrale für politische Bildung, S. 31–35.

Baumann, Rüdeger (2008): Probleme der Aufgabenkonstruktion gemäß Bildungsstandards. Überlegungen zu Kompetenzstufen und Operatoren. In: *LOG IN* 28 (153), S. 54–59.

Berendt, Bettina; Dettmar, Gebhard; Demir, Cihan; Peetz, Thomas (2014): Kostenlos ist nicht kostenfrei. Eine Unterrichtsreihe zur Datenauswertung in sozialen Netzwerken und ihren Implikationen für Privatsphäre und Demokratie. In: *LOG IN* 34 (2), S. 41–56.

Berendt, Bettina; Dettmar, Gebhard; Esslinger, Bernhard; Gramm, Andreas; Grillenberger, Andreas; Hug, Alexander; Witten, Helmut (2015): Datenschutz im 21. Jahrhundert – Ist Schutz der Privatsphäre (noch) möglich? In: Jens Gallenbacher (Hg.): Informatik allgemeinbildend begreifen. INFOS 2015, 16. GI-Fachtagung Informatik und Schule. Darmstadt, 20.-23.10.2015. Gesellschaft für Informatik e. V. Berlin, Heidelberg: Springer Verlag (LNI, 249), S. 33–42.

Biehl, Christopher Julien (2019): Entwicklung einer Unterrichtsreihe zu dem Thema Datenschutz mit Fokus auf den mathematischen Relationen in Sozialen Netzwerken. Masterarbeit. Universität Koblenz-Landau, Koblenz. Online verfügbar unter https://kola.opus.hbz-nrw.de/frontdoor/index/index/start/0/rows/10/sortfield/score/sortorder/desc/searchtype/advanced/author/Biehl/authormodifier/contains_all/docId/1913, zuletzt geprüft am 21.08.2019.

BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Hg.) (2014): Jung und vernetzt. Kinder und Jugendliche in der digitalen Welt. Berlin. Online verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Jung-und-vernetzt-Kinder-und-Jugendliche-in-der-digitalen-Gesellschaft.html, zuletzt geprüft am 01.07.2018.

Bitterer, Maja; Zeidler, Matthias; Wirthwein, Ulrike (2014): Deutsch.kompetent. Gymnasium, Sekundarstufe I, allgemeine Ausgabe, 1. Auflage. Hg. v. Maximilian Nutz. Stuttgart, Leipzig: Ernst Klett Verlag.

Böhm, Marco (2015): Erstellung von Aufgaben zu Datenschutz und Datensicherheit von Smartphone-Applikationen für Informatik im Kontext. Bachelorarbeit. Universität Koblenz-Landau, Koblenz. Online verfügbar unter https://kola.opus.hbz-nrw.de/frontdoor/index/index/docId/1898, zuletzt geprüft am 04.12.2019.

Bonneau, Joseph; Preibusch, Sören (2009): The Privacy Jungle. On the Market for Data Protection in Social Networks. In: David Pym und M. Angela Sasse (Hg.): Proceedings of the 8th Annual Workshop on the Economics of Information Security. WEIS 2009, Workshop on the Economics of Information Security. University College London, England, UK, 24.-25.06.2009, S. 1–45. Online verfügbar unter citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.443.6607&rep=rep1&type=pdf, zuletzt geprüft am 22.08.2019.

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph (2011): Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte. 1. Aufl. Heidelberg, Dordrecht, London, New York: Springer-Verlag. Online verfügbar unter https://pfiffige-senioren.de/Studie_Identitaetsdiebstahl_090610(2).pdf, zuletzt geprüft am 25.09.19.

Bos, Wilfried; Eickelmann, Birgit; Gerick, Julia (2014): ICILS 2013 auf einen Blick. International Computer and Information Literacy Study. Presseinformationen zur Sudie und zu zentralen Ergebnissen. Münster. Online verfügbar unter http://www.ifs.tu-dortmund.de/cms/Medienpool/Projekte/ICILS-2013/ICILS_2013_Presseinformation.pdf, zuletzt geprüft am 01.08.2019.

Bosse, Johanna; Fleischhut, Jens (1986): Datenerhebung, Datenverarbeitung, Datenschutz. Unterrichtsmaterialien für die 10. Jahrgangsstufe. 1. Aufl. Berlin.

Bräunlich, Katharina; Dienlin, Tobias; Eichenhofer, Johannes; Helm, Paula; Trepte, Sabine; Grimm, Rüdiger (2019): Linking Loose Ends: An Interdisciplinary Privacy and Communication Model. In: *New Media & Society* (in print).

Breier, Norbert (2005): Informatik im Fächerkanon allgemeinbildender Schulen - Überlegungen zu einem informationsorientierten didaktischen Ansatz. In: Steffen Friedrich (Hg.): Unterrichtskonzepte für informatische Bildung. INFOS 2005, 11. GI-Fachtagung Informatik und Schule. Dresden, 28.-30.09.2005. Gesellschaft für Informatik e. V. Bonn: Köllen Druck + Verlag (LNI, P-60), S. 67–78.

Breier, Norbert; Hubwieser, Peter (2002): An Information-Oriented Approach to Informatical Education. In: *Informatics in Education* (1), S. 31–42. Online verfügbar unter www.academia.edu/download/46996878/An_information-oriented_approach_to_info20160704-28708-1trdlnr.pdf, zuletzt geprüft am 07.02.2018.

Brinda, Torsten; Brüggen, Niels; Diethelm, Ira; Knaus, Thomas; Kommer, Sven; Kopf, Christine et al. (2019): Frankfurt-Dreieck zur Bildung in der digital vernetzten Welt. Ein interdisziplinäres Modell. Hg. v. Initiative "Keine Bildung ohne Medien!". Aachen. Online verfügbar unter https://www.keine-bildung-ohne-medien.de/frankfurter-dreieck/, zuletzt geprüft am 07.08.2019.

Brinda, Torsten; Diethelm, Ira; Gemulla, Rainer; Romeike, Ralf; Schöning, Johannes; Schulte, Carsten (2016): Dagstuhl-Erklärung. Bildung in der digital vernetzten Welt. Hg. v. Gesellschaft für Informatik e. V. Bonn. Online verfügbar unter https://gi.de/fileadmin/GI/Hauptseite/Themen/Dagstuhl-Erkla__rung_2016-03-23.pdf, zuletzt geprüft am 22.02.2018.

Brüggen, Niels; Wagner, Ulrike (2017): Recht oder Verhandlungssache? In: Michael Friedewald, Jörn Lamla und Alexander Roßnagel (Hg.): Informationelle Selbstbestimmung im digitalen Wandel. Wiesbaden: Springer Vieweg Verlag (DuD-Fachbeiträge), S. 131–146.

Bund-Länder-Kommission für Bildungsplanung und Forschungsförderung (1987): Gesamtkonzept für die informationstechnische Bildung. Materialien für die Bildungsplanung. Hg. v. Bund-Länder-Kommission für Bildungsplanung und Forschungsförderung. Bonn (Heft 16). Online verfügbar unter www.blk-bonn.de/papers/heft16.pdf, zuletzt geprüft am 07.02.2018.

Burgoon, Judee K. (1982): Privacy and Communication. In: Michael Burgoon (Hg.): Communication Yearbook 6. Hoboken: Taylor and Francis Verlag, S. 206–249.

Carretero, Stephanie; Vuorikari, Riina; Punie, Yves (2017): DigComp 2.1. The Digital Competence Framework for Citizens. With eight proficiency levels and examples of use. European Union. Luxembourg (EUR, Scientific and technical research series). Online verfügbar unter publications.jrc.ec.europa.eu/repository/bitstream/JRC106281/web-digcomp2.1pdf_(online).pdf, zuletzt geprüft am 27.01.2018.

Caspar, Johannes (2013): Soziale Netzwerke - Endstation informationeller Selbstbestimmung. Ein Bericht aus der Behördenpraxis. In: *DuD* 37 (12), S. 767–771. Online verfügbar unter https://link.springer.com/content/pdf/10.1007/s11623-013-0323-7.pdf, zuletzt geprüft am 22.08.19.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (Hg.) (2015): DIVSI U9-Studie. Kinder in der digitalen Welt. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Hamburg. Online verfügbar unter www.divsi.de/wp-content/uploads/2015/06/U9-Studie-DIVSI-web.pdf, zuletzt geprüft am 08.06.2018.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (Hg.) (2018): DIVSI U25-Studie - Euphorie war gestern. Die "Generation Internet" zwischen Glück und Abhängigkeit. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Hamburg. Online verfügbar unter https://www.divsi.de/publikationen/studien/divsi-u25-studie-euphorie-war-gestern/, zuletzt geprüft am 01.08.2019.

Dey, Ratan; Ding, Yuan; Ross, Keith W. (2013): Profiling high-school students with facebook. How Online Privacy Laws Can Actually Increase Minors' Risk. In: Konstantina (Dina) Papagiannaki, Krishna Gummadi und Craig Partridge (Hg.): Proceedings of the 13th ACM Internet Measurement Conference. IMC 2013, ACM Internet Measurement Conference. Barcelona, Spain, 23.-25.10.2013. Association for Computing Machinery (ACM). New York, NY, Red Hook, NY: ACM; Curran, S. 405–416.

Dienlin, Tobias; Trepte, Sabine (2015): Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. In: *Eur. J. Soc. Psychol.* 45 (3), S. 285–297.

Diethelm, Ira (2011): Wie forschend-entdeckendes Lernen gelingen kann. Forschendes und entdeckendes Lernen in Kontexten zu Datenschutz, Internet und Urheberrecht. In: *LOG IN* 30 (168), S. 28–34.

Dietz, Alexander; Oppermann, Frank (Hg.) (2011): Planspiel "Datenschutz 2.0". Eine Unterrichtsreihe der Projekts "Informatik im Kontext" *LOG IN* 31 (171). Berlin: LOG IN-Verlag.

Dörge, Christina (2012): Informatische Schlüsselkompetenzen - Konzepte der Informationstechnologie im Sinne einer informatischen Allgemeinbildung. Dissertation. Carl von Ossietzky Universität, Oldenburg. Fakultät II - Informatik, Wirtschafts- und Rechtswissenschaften. Online verfügbar unter http://oops.uni-oldenburg.de/1426/, zuletzt geprüft am 05.02.2018.

Döring, Nicola; Bortz, Jürgen (2016): Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften. Unter Mitarbeit von Sandra Pöschl-Günther. 5. vollständig überarbeitete, aktualisierte und erweiterte Auflage. Berlin, Heidelberg: Springer (Springer-Lehrbuch).

Dorn, Julian (2017): friendzone. A Social Network is Rising. In: *LOG IN* 36 (187/188), S. 69–74.

Dorn, Julian (2019): InstaHub. Gründe dein eigenes soziales Netzwerk. In: *MNU-Journal* 72 (4), S. 289–295.

Dorn, Ralf; Gramm, Andreas; Wagner, Oliver (2005): Planspiel zum Datenschutz. Die gläsernen Schüler von Biesdorf - Ein Erfahrungsbericht. In: *LOG IN* 24 (136/137), S. 72–75.

Eckert, Claudia (2013): IT-Sicherheit. Konzepte - Verfahren - Protokolle. 8., aktualisierte und korrigierte Aufl. München: Oldenbourg-Verlag.

Egger, Edeltraud; Schillinger, Bernhard (1996): Datenschutz als Bürgerrecht. In: Peter Fleissner (Hg.): Datensicherheit und Datenschutz. Technische und rechtliche Perspektiven. 1. Aufl. Innsbruck: Studien-Verlag, S. 47–64.

Eickelmann, Birgit (2017): Kompetenzen in der digitalen Welt. Konzepte und Entwicklungsperspektiven. Berlin: Verlag Friedrich-Ebert-Stiftung Abteilung Studienförderung (Gute Gesellschaft - soziale Demokratie #2017plus).

Europäische Union (2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG. Datenschutz-Grundverordnung vom 27.04.2016. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE, zuletzt geprüft am 14.01.2020.

Feierabend, Sabine; Plankenhorn, Theresa; Rathgeb, Thomas (2015): JIM-Studie 2015. Jugend, Information, (Multi-)Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland. Hg. v. Medienpädagogischer Forschungsverbund Südwest. Stuttgart. Online verfügbar unter www.mpfs.de/fileadmin/files/Studien/JIM/2015/JIM_Studie_2015.pdf, zuletzt geprüft am 02.07.2018.

Feierabend, Sabine; Plankenhorn, Theresa; Rathgeb, Thomas (2017): KIM-Studie 2016. Kinder, Internet, Medien. Basisstudie zum Medienumgang 6- bis 13-Jähriger in Deutschland. Hg. v. Medienpädagogischer Forschungsverbund Südwest. Stuttgart. Online verfügbar unter https://www.mpfs.de/fileadmin/files/Studien/KIM/2016/KIM_2016_Web-PDF.pdf, zuletzt geprüft am 17.01.19.

Feierabend, Sabine; Rathgeb, Thomas; Reutter, Theresa (2018): JIM-Studie 2018. Jugend, Information, Medien. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland. Hg. v. Medienpädagogischer Forschungsverbund Südwest. Stuttgart. Online verfügbar unter https://www.mpfs.de/studien/jim-studie/2018/, zuletzt geprüft am 01.08.2019.

Feierabend, Sabine; Rathgeb, Thomas; Reutter, Theresa (2019): KIM-Studie 2018. Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger. Hg. v. Medienpädagogischer Forschungsverbund Südwest. Stuttgart. Online verfügbar unter https://www.mpfs.de/studien/kim-studie/2018/, zuletzt geprüft am 03.08.2019.

Ferrari, Anusca (2013): DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe. JRC Scientific and Policy Reports. Hg. v. Yves Punie und Barbara N. Brecko. European Commission. Seville. Online verfügbar unter http://ftp.jrc.es/EURdoc/JRC83167.pdf, zuletzt geprüft am 09.03.2017.

Florencio, Dinei; Herley, Cormac (2007): A large-scale study of web password habits. In: Carey Williamson (Hg.): Proceedings of the 16th international conference on World Wide Web. WWW 2007, the 16th international conference on World Wide Web. Banff, Alberta, Canada, 08.-12.05.2007. Association for Computing Machinery (ACM). New York, NY: ACM Press, S. 657–665. Online verfügbar unter www.ra.ethz.ch/CDStore/www2007/www2007.org/papers/paper620.pdf, zuletzt geprüft am 26.09.2019.

Freytag, Johann-Christoph (2014): Grundlagen und Visionen großer Forschungsfragen im Bereich Big Data. In: *Informatik Spektrum* 37 (2), S. 97–104.

Friedrich, Steffen (2003): Informatik und PISA - vom Wehe zum Wohl der Schulinformatik. In: Peter Hubwieser (Hg.): Informatische Fachkonzepte im Unterricht. INFOS 2003, 10. GI-Fachtagung Informatik und Schule. Garching bei München, 17.-19.09.2003. Gesellschaft für Informatik e. V. Bonn: Köllen Druck + Verlag (LNI, P-32), S. 123–134. Online verfügbar unter https://pdfs.semanticscholar.org/ce4a/902c746aa4fbc4fca693592ded1fd5249abe.pdf, zuletzt geprüft am 07.02.2018.

Fuchs, Karl; Landerer, Claudio (2005): Das mühsame Ringen um ein Komeptenzmodell. In: *CD Austria - Das multimedia Magazin für Österreichs Schulen* (12), S. 6–9.

Funder, David C.; Furr, R. Michael; Colvin, C. Randall (2000): The Riverside Behavioral Q-sort: A Tool for the Description of Social Behavior. In: *Journal of Personality* 68 (3), S. 451-489. Online verfügbar unter http://psych.wfu.edu/furr/reprints/rbq.pdf, zuletzt geprüft am 30.07.2018.

Gapski, Harald (2001): Medienkompetenz. Eine Bestandsaufnahme und Vorüberlegungen zu einem systemtheoretischen Rahmenkonzept. 1. Aufl. Wiesbaden: Westdeutscher Verlag.

Gapski, Harald (2006): Medienkompetenz messen? Eine Annäherung über verwandte Kompetenzfelder. In: Harald Gapski (Hg.): Medienkompetenz messen? Verfahren und Reflexion zur Erfassung von Schlüsselkompetenzen. München, Düsseldorf: kopaed verlagsGmbH (Schriftenreihe Medienkompetenz des Landes NRW, 3), S. 13–28.

Gesellschaft für Informatik e. V. (Hg.) (2000): Empfehlungen für ein Gesamtkonzept zur informatischen Bildung an allgemeinbildenden Schulen *LOG IN* 20 (2). Berlin: LOG IN-Verlag.

Gesellschaft für Informatik e. V. (Hg.) (2006): IT-Sicherheit in der Ausbildung. Empfehlungen zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung. Online verfügbar unter https://dl.gi.de/handle/20.500.12116/2343, zuletzt geprüft am 03.04.2018.

Gesellschaft für Informatik e. V. (Hg.) (2008): Grundsätze und Standards für die Informatik in der Schule. Bildungsstandards Informatik für die Sekundarstufe I. Beilage zu *LOG IN* 28 (150/151). Berlin: LOG IN-Verlag. Online verfügbar unter https://www.informatikstandards.de/docs/bildungsstandards_2008.pdf, zuletzt geprüft am 15.01.2020.

Gesellschaft für Informatik e. V. (Hg.) (2016): Bildungsstandards Informatik für die Sekundarstufe II. Beilage zu *LOG IN* 36 (183/184). Berlin: LOG IN-Verlag. Online verfügbar unter https://www.informatikstandards.de/docs/Bildungsstandards_SII.pdf, zuletzt geprüft am 15.01.2020.

Gesellschaft für Informatik e. V. (Hg.) (2019): Kompetenzen für informatische Bildung im Primarbereich. Empfehlungen der Gesellschaft für Informatik e.V. erarbeitet vom Arbeitskreis »Bildungsstandards Informatik im Primarbereich«. Beilage zu *LOG IN* 39 (189/190). Berlin: LOG IN-Verlag. Online verfügbar unter https://www.informatikstandards.de/docs/v142_empfehlungen_kompetenzen-primarbereich_2019-01-31.pdf, zuletzt geprüft am 19.09.19.

Gimmler, Roland (2012): Medienkompetenz und Datenschutzkompetenz in der Schule. In: *DuD* 36 (2), S. 110–116.

Gmeinwieser, Katharina (2017): Big Up 4 Big Data. Ein Stationsspiel zur Einführung in den Themenkomplex "Big Data". In: *LOG IN* 36 (187/188), S. 64–68.

Gönsch, Jochen; Klein, Robert; Steinhardt, Claudius (2009): Dynamic Pricing – State-of-The-Art. In: *Zeitschrift für Betriebswirtschaft* (3), S. 1–40. Online verfügbar unter https://ssrn.com/abstract=2179225, zuletzt geprüft am 19.09.19.

Gräsel, Cornelia (2010): Lehren und Lernen mit Schulbüchern. Beispiele aus der Unterrichtsforschung. In: Eckhardt Fuchs, Joachim Kahlert und Uwe Sandfuchs (Hg.): Schulbuch konkret. Kontexte - Produktion - Unterricht. Bad Heilbrunn: Julius Klinkhardt Verlag, S. 137–148.

Greving, Bert (2009): Messen und Skalieren von Sachverhalten. In: Sönke Albers, Daniel Klapper, Udo Konradt, Achim Walter und Joachim Wolf (Hg.): Methodik der empirischen Forschung. 3., überarbeitete und erweiterte Auflage. Wiesbaden: Gabler Verlag, S. 65–78.

Grillenberger, Andreas; Romeike, Ralf (2015): Big Data im Informatikunterricht: Motivation und Umsetzung. In: Jens Gallenbacher (Hg.): Informatik allgemeinbildend begreifen. INFOS 2015, 16. GI-Fachtagung Informatik und Schule. Darmstadt, 20.-23.10.2015. Gesellschaft für Informatik e. V. Berlin, Heidelberg: Springer Verlag (LNI, 249), S. 125–134.

Grillenberger, Andreas; Romeike, Ralf (2017): Datenmanagement als Thema für den Informatikunterricht. Ein Überblick über die Grundlagen des Fachgebiets aus informatikdidaktischer Sicht. In: *LOG IN* 36 (187/188), S. 44–52.

Grimm, Rüdiger (2008): IT-Sicherheitsmodelle. Hg. v. Fachbereich Informatik Universität Koblenz-Landau. Koblenz. Online verfügbar unter www.uni-koblenz.de/~fb4reports/2008/2008_03_Arbeitsberichte.pdf, zuletzt geprüft am 06.02.2018.

Grimm, Rüdiger (2015): Big Data aus Informatiksicht und die Wirkung von Verschlüsselung. In: Philipp Richter (Hg.): Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data. 1. Auflage. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG (Der Elektronische Rechtsverkehr, 32), S. 127–150.

Grimm, Rüdiger; Bräunlich, Katharina (2015): Vertrauen und Privatheit. Anwendung des Referenzmodells für Vertrauen auf die Prinzipien des Datenschutzes. In: *DuD* 39 (5), S. 289–294.

Grimm, Rüdiger; Maier, Michaela; Rothmund, Tobias (2015): Vertrauen. Ein interdisziplinäres Referenzmodell. In: *DuD* (5), S. 283–294.

Grimm, Rüdiger; Simić-Draws, Daniela; Bräunlich, Katharina; Kasten, Andreas; Meletiadou, Anastasia (2016): Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse. In: *Informatik Spektrum* 39 (1), S. 2–20.

Gross, Ralph; Acquisti, Alessandro (2005): Information Revelation and Privacy in Online Social Networks. In: Vijay Atluri, Sabrina de Di Capitani Vimercati und Roger Dingledine (Hg.): Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society. co-located with 12th ACM Computer and Communications Security Conference (CCS 2005). WPES 2005, ACM Workshop on Privacy in the Electronic Society. Alexandria, Virginia, USA, 07.11.2005. Association for Computing Machinery (ACM). New York, NY: ACM Press, S. 71–80. Online verfügbar unter https://dataprivacylab.org/projects/facebook/facebook1.pdf, zuletzt geprüft am 22.08.19.

Hansen, Marit (2015a): Herausforderung Verbraucherdatenschutz in der digitalen Welt. 1. Aufl. Hg. v. Abteilung Wirtschafts- und Sozialpolitik. Friedrich-Ebert-Stiftung. Bonn. Online verfügbar unter library.fes.de/pdf-files/wiso/12017-20151029.pdf, zuletzt geprüft am 15.09.19.

Hansen, Marit (2015b): Zukunft von Datenschutz und Privatsphäre in einer mobilen Welt. In: *DuD* 39 (7), S. 435–439. Online verfügbar unter https://link.springer.com/content/pdf/10.1007%2Fs11623-015-0445-1.pdf, zuletzt geprüft am 18.01.18.

Hill, Hermann (2014): Neubestimmung der Privatheit – auf dem Weg zu »Neuer Sozialität«. In: Hermann Hill und Utz Schliesky (Hg.): Die Neubestimmung der Privatheit. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG (Verwaltungsressourcen und Verwaltungsstrukturen), S. 249–267.

Homburg, Christian; Krohmer, Harley (2008): Der Prozess der Marktforschung: Festlegung der Datenerhebungsmethode, Stichprobenbildung und Fragebogengestaltung. In: Andreas Herrmann, Christian Homburg und Martin Klarmann (Hg.): Handbuch Marktforschung. Methoden, Anwendungen, Praxisbeispiele. 3., vollst. überarb. und erw. Aufl. Wiesbaden: Gabler Verlag, S. 21–51.

Hoofnagle, Chris Jay; King, Jennifer; Li, Su; Turow, Joseph (2010): How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? In: *SSRN Journal*. Online verfügbar unter papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864, zuletzt geprüft am 01.07.2018.

Hubwieser, Peter (2007): Didaktik der Informatik. Grundlagen, Konzepte, Beispiele. 3. Aufl. Berlin, Heidelberg: Springer-Verlag (eXamen.press).

Hubwieser, Peter; Broy, Manfred (1997): Ein neuer Ansatz für den Informatikunterricht am Gymnasium. In: *LOG IN* 17 (3/4), S. 42–47.

Hug, Alexander (2018): "I've got nothing to hide!" Survey on a Data Privacy Competence with German Schoolchildren. In: Andreas Mühling und Quintin Cutts (Hg.): Proceedings of the 13th Workshop in Primary and Secondary Computing Education. WiPSCE 2018, the 13th Workshop in Primary and Secondary Computing Education. Potsdam, Germany, 04.-06.10.2018. New York, USA: ACM Press, S. 159–160.

Hug, Alexander; Grimm, Rüdiger (2016a): Extension of a didactic media competence model by privacy risk. Arbeitsbericht. Universität Koblenz-Landau, Koblenz. Online verfügbar unter https://www.uni-koblenz-landau.de/de/koblenz/fb4/publikationen/reports, zuletzt geprüft am 19.12.19.

Hug, Alexander; Grimm, Rüdiger (2016b): Extension of a Didactic Media Competence Model by Privacy Risk. In: Jan Varenhold und Erik Barendsen (Hg.): Proceedings of the 11th Workshop in Primary and Secondary Computing Education. WiPSCE 2016, the 11th Workshop in Primary and Secondary Computing Education. Münster, Germany, 13.-15.10.2016. New York, USA: ACM Press, S. 104–105.

Hug, Alexander; Grimm, Rüdiger (2017): Entwicklung eines Datenschutzkompetenzmodells. In: Ira Diethelm (Hg.): Informatische Bildung zum Verstehen und Gestalten der digitalen Welt. INFOS 2017, 17. GI-Fachtagung Informatik und Schule. Oldenburg, 13.-15.09.2017. Gesellschaft für Informatik e. V. Berlin, Heidelberg: Springer Verlag (LNI, 274), S. 167–170.

Humbert, Ludger (2006): Didaktik der Informatik. Mit praxiserprobtem Unterrichtsmaterial. 2., überarb. und erw. Aufl. Wiesbaden: B.G. Teubner Verlag | GWV Fachverlage GmbH Wiesbaden (Leitfäden der Informatik).

Jank, Werner; Meyer, Hilbert (1991): Didaktische Modelle. 5. Aufl. Berlin: Cornelsen Verlag Sciptor.

Jenny, Mirjam (2017): Risikokompetenz als Voraussetzung guter und selbstbestimmter Entscheidungen. In: *DMV Mitteilungen* 25 (4), S. 225–229.

Jörges, Hans-Ulrich (2017): Lernen in Zeiten der Lüge. Medienkunde für Schüler. In: *Profil. Das Magazin für Gymnasium und Gesellschaft* (11), S. 41.

Kehr, Flavius; Rothmund, Tobias; Gollwitzer, Mario; Füllgraf, Wendy: Prädiktoren sicherheitsrelevanten Verhaltens bei jugendlichen Computernutzern. Computersicherheit und Medienkompetenz. Fragebogen der Studie. Landau.

Kehr, Flavius; Rothmund, Tobias; Gollwitzer, Mario; Füllgraf, Wendy (2015): Prädiktoren sicherheitsrelevanten Verhaltens bei jugendlichen Computernutzern. In: *DuD* 39 (5), S. 303–307.

Klieme, Eckhard (2004): Was sind Kompetenzen und wie lassen sie sich messen? In: *Pädagogik* 56 (6), S. 10–13.

Kohl, Lutz (2009): Kompetenzorientierter Informatikunterricht in der Sekundarstufe I unter Verwendung der visuellen Programmiersprache Puck. Dissertation. Friedrich-Schiller-Universität, Jena. Online verfügbar unter https://ddi-wiki.gi.de/dissertation/kompetenzorientierter_informatikunterricht_in_der_sekundarstufe_i_unter_verwendung_der_visuellen_programmiersprache_puck, zuletzt geprüft am 15.08.19.

Kosinski, Michal; Stillwell, David; Graepel, Thore (2013): Private traits and attributes are predictable from digital records of human behavior. In: *Proceedings of the National Academy of Sciences of the United States of America* 110 (15), S. 5802–5805. Online verfügbar unter https://www.pnas.org/content/pnas/110/15/5802.full.pdf?3=, zuletzt geprüft am 19.09.19.

Koubek, Jochen (o. J.): Informatik im Kontext. Unter Mitarbeit von Helmut Witten. Online verfügbar unter www.informatik-im-kontext.de, zuletzt geprüft am 01.10.2015.

Koubek, Jochen (2005a): E-Mail-Kompetenzen. Ein Beispiel zu Standards für die informatische Bildung. In: *LOG IN* 24 (135), S. 61–65.

Koubek, Jochen (2005b): Informatische Allgemeinbildung. In: Steffen Friedrich (Hg.): Unterrichtskonzepte für informatische Bildung. INFOS 2005, 11. GI-Fachtagung Informatik und Schule. Dresden, 28.-30.09.2005. Gesellschaft für Informatik e. V. Bonn: Köllen Druck + Verlag (LNI, P-60), S. 57–66. Online verfügbar unter waste.informatik.hu-berlin.de/~koubek/forschung/informatischeallgemeinbildung.pdf, zuletzt geprüft am 08.02.2018.

Koubek, Jochen (2008): Der andere Schulhof. Die dunkle Seite von SchülerVZ. In: *LOG IN* 28 (153), S. 38–41.

Koubek, Jochen; Kurz, Constanze (2007): Informatik - Mensch - Gesellschaft im Schulunterricht. In: Sigrid Schubert (Hg.): Didaktik der Informatik in Theorie und Praxis. INFOS 2007, 12. GI-Fachtagung Informatik und Schule. Siegen, 19.-21.09.2007. Gesellschaft für Informatik e. V. Bonn: Köllen Druck + Verlag (LNI, P-112), S. 125–133. Online verfügbar unter dokumentix.ub.uni-siegen.de/opus/volltexte/2009/384/pdf/didaktik_der_informatik_2007.pdf.

Kramer, Rudi; Spaeing, Frank (2014): „Datenschutz geht zur Schule“ — was Hänschen nicht lernt… In: *DuD* 38 (6), S. 370–374.

Kuß, Alfred; Wildner, Raimund; Kreis, Henning (2018): Marktforschung. Datenerhebung und Datenanalyse. 6., überarbeitete und erweiterte Auflage. Wiesbaden: Springer Gabler Verlag. Online verfügbar unter http://dx.doi.org/10.1007/978-3-658-20566-9.

Länderkonferenz MedienBildung (Hg.) (2015): Kompetenzorientiertes Konzept für die schulische Medienbildung. LKM-Positionspapier vom 29.01.2015. Kronshagen. Online verfügbar unter https://lkm.lernnetz.de/files/Dateien_lkm/Dokumente/LKM-Positionspapier_2015.pdf, zuletzt geprüft am 10.08.19.

Langer, Thomas (2017): Bildung im digitalen Zeitalter. 10. Tagung des wissenschaftlichen Beirats des Deutschen Philologenverbands. In: *Profil. Das Magazin für Gymnasium und Gesellschaft* (11), S. 12–15.

Liu, Yabing; Gummadi, Krishna P.; Krishnamurthy, Balachander; Mislove, Alan (2011): Analyzing Facebook Privacy Settings. User Expectations vs. Reality. In: Patrick Thiran (Hg.): Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. IMC 2011, Internet Measurement Conference. Berlin, 02.-04.11.2011. Association for Computing Machinery (ACM). New York, NY: ACM Press, S. 61–70. Online verfügbar unter https://conferences.sigcomm.org/imc/2011/docs/p61.pdf, zuletzt geprüft am 22.08.19.

Livingstone, Sonia (2008): Taking risky opportunities in youthful content creation. Teenagers' use of social networking sites for intimacy, privacy and self-expression. In: *New Media & Society* 10 (3), S. 393–411.

Makosch, Yeliz (2019): Entwicklung eines Kriterienkatalogs zur Qualität von Unterrichtsmaterialien und Anwendung dessen durch Analyse von Materialien zum Thema Datenschutz. Masterarbeit. Universität Koblenz-Landau, Koblenz. Verfügbar über das Prüfungsamt der Universität Koblenz-Landau, Koblenz.

Masur, Philipp K. (2014): Gefällt mir (nicht). Das Social Web als Spannungsfeld zwischen Selbstoffenbarung und Datenschutz. ver.di, 2014. Online verfügbar unter edufant.net/pluginfile.php/1294/course/section/649/Masur_Vortrag_ver.di_2014.pdf, zuletzt geprüft am 22.08.19.

Masur, Philipp K.; Reinecke, Leonard; Ziegele, Marc; Quiring, Oliver (2014): The interplay of intrinsic need satisfaction and Facebook specific motives in explaining addictive behavior on Facebook. In: *Computers in Human Behavior* 39, S. 376–386.

Masur, Philipp K.; Teutsch, Doris; Trepte, Sabine (2017): Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). In: *Diagnostica* 63 (4), S. 256–268.

Mayer, R. C.; Davis, J. H.; Schoorman, F. D. (1995): An Integrative Model of Organizational Trust. In: *Academy of Management Review* 20 (3), S. 709–734.

Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) (2008a): Lehrplan Informatik. Wahlfach und Wahlpflichtfach an Gymnasien und Integrierten Gesamtschulen (Sekundarstufe I). Hg. v. Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP. Mainz. Online verfügbar unter https://informatik.bildung-rp.de/lehrplaene.html, zuletzt geprüft am 15.01.2018.

Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) (2008b): Lehrplan Informatik. Grund- und Leistungsfach, Einführungsphase und Qualifikationsphase der gymnasialen Oberstufe (Mainzer Studienstufe). Hg. v. Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP. Mainz. Online verfügbar unter http://informatik.bildung-rp.de/lehrplaene.html, zuletzt geprüft am 25.05.2015.

Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP (Hg.) (2010): Richtlinie Verbraucherbildung. Hg. v. Ministerium für Bildung, Wissenschaft, Jugend und Kultur RLP. Mainz. Online verfügbar unter http://verbraucherbildung.bildung-rp.de/fileadmin/user_upload/verbraucherbildung.bildung-rp.de/Materialien/Richtlinie_VB.pdf, zuletzt geprüft am 27.01.2016.

Müsgens, Martin (2015): Datenschutz im (mobilen) Internet. 4. Aufl. Hg. v. klicksafe und Internet-ABC. Düsseldorf. Online verfügbar unter http://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Eltern_Allgemein/Datenschutz_im__mobilen__Internet_Brosch%C3%BCre.pdf, zuletzt geprüft am 19.09.19.

Neumann-Braun, Klaus (2000): Medienkompetenz und Informationsgesellschaft. Hg. v. Johann Wolfgang Goethe Universität. Fachbereich 03/Gesellschaftswissenschaften/Institut III. Frankfurt (Paper 30 des Forschungsschwerpunkts "Familien-, Jugend- und Kommunikationssoziologie"). Online verfügbar unter http://publikationen.ub.uni-frankfurt.de/files/3394/B.pdf, zuletzt geprüft am 25.01.2017.

Noll, Christoph (2019): Weiterentwicklung der Unterrichtsreihe Planspiel 2.0: „Wer weiß was über mich im Internet?“ des Projekts Informatik im Kontext und Durchführung dieser in einem Grundkurs Informatik. Masterarbeit. Universität Koblenz-Landau, Koblenz. Online verfügbar unter https://kola.opus.hbz-nrw.de/frontdoor/index/index/start/0/rows/10/sortfield/score/sortorder/desc/searchtype/simple/query/Noll/docId/1902, zuletzt geprüft am 19.08.2019.

Norberg, Patricia A.; Horne, Daniel R.; Horne, David A. (2007): The Privacy Paradox. Personal Information Disclosure Intentions versus Behaviors. In: *Journal of Consumer Affairs* 41 (1), S. 100–126.

Oberle, Daniel; Berendt, Bettina; Hotho, Andreas; Gonzalez, Jorge (2003): Conceptual User Tracking. In: Ernestina Menasalvas, Javier Segovia und Piotr S. Szczepaniak (Hg.): Advances in Web Intelligence. AWIC 2003, First International Atlantic Web Intelligence Conference. Madrid, 05.-06.05.2003. Berlin, Heidelberg: Springer Verlag, S. 155–164. Online verfügbar unter citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.269.6791&rep=rep1&type=pdf, zuletzt geprüft am 19.09.19.

Pariser, Eli (2011): The Filter Bubble. What the Internet Is Hiding from You. New York: Penguin Press.

Peters, Ingo-Rüdiger (2008): Soziale Netze im Mittelalter und heute. In: *LOG IN* 28 (153), S. 42–45.

Petko, Dominik; Heimgartner, Daniela; Schmuki, Robert; Weber, Yves (2017): Virtual:Stories. Den Umgang mit Gefahren im Internet durch Fallgeschichten lernen. In: *LOG IN* 36 (187/188), S. 53–57.

Pfitzmann, Andreas; Schill, Alexander; Westfeld, Andreas; Wolf, Gritta (2000): Mehrseitige Sicherheit in offenen Netzen. Grundlagen, praktische Umsetzung und in Java implementierte Demonstrations-Software. Unter Mitarbeit von Guntram Wicke und Jan Zöllner. Braunschweig: Vieweg-Verlag (DuD-Fachbeiträge).

Rein, Antje von (Hg.) (1996): Medienkompetenz als Schlüsselbegriff. 1. Aufl. Bad Heilbrunn: Julius Klinkhardt Verlag (Theorie und Praxis der Erwachsenenbildung).

Rieger, Frank (2013): Von Daten und Macht. Essay. In: *Aus Politik und Zeitgeschichte* 63 (15-16), S. 3–7. Online verfügbar unter http://www.bpb.de/apuz/157538/von-daten-und-machtessay?p=1, zuletzt geprüft am 19.09.19.

Roßnagel, Alexander; Banzhaf, Jürgen; Grimm, Rüdiger (2003): Datenschutz im electronic commerce. Technik, Recht, Praxis. 1. Aufl. Heidelberg: Verlag Recht und Wirtschaft (Schriftenreihe Kommunikation & Recht, 18).

Roßnagel, Alexander (Hg.) (2003): Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung. 1. Aufl. München: Beck Verlag.

Saint-Mont, Uwe (2013): Die Macht der Daten. Wie Information unser Leben bestimmt. 1. Aufl. Berlin, Heidelberg: Springer Verlag.

Savelsberg, Jan (2019): Weiterentwicklung und Implementierung des Projekts "InstaHub" für die Sekundarstufe I mit dem Themenschwerpunkt Datenschutz. Masterarbeit. Universität Koblenz-Landau, Koblenz. Online verfügbar unter https://kola.opus.hbz-nrw.de/frontdoor/index/index/start/0/rows/10/sortfield/score/sortorder/desc/searchtype/authorsearch/author/Savelsberg/authormodifier/contains_all/docId/1892, zuletzt geprüft am 15.06.2019.

Schecker, Horst; Parchmann, Ilka (2006): Modellierung naturwissenschaftlicher Kompetenz. In: *Zeitschrift für Didaktik der Naturwissenschaften* 12, S. 45–66.

Scheibler, Petra (o. J.): Qualitative versus quantitative Forschung. Online verfügbar unter studi-lektor.de/tipps/qualitative-forschung/qualitative-quantitative-forschung.html, zuletzt geprüft am 06.07.2018.

Schenk, Michael; Niemann, Julia; Reinmann, Gabi; Roßnagel, Alexander (2012a): Digitale Privatsphäre. Heranwachsende und Datenschutz auf sozialen Netzwerkplattformen. Anhangband. Unter Mitarbeit von Silke Jandt und Jan-Mathis Schnurr. Landesanstalt für Medien Nordrhein-Westfalen (Schriftenreihe Medienforschung der Landesanstalt für Medien Nordrhein-Westfalen). Online verfügbar unter www.lfm-nrw.de/foerderung/forschung/abgeschlossene-projekte/schriftenreihe-medienforschung/digitale-privatsphaere.html, zuletzt geprüft am 01.07.2018.

Schenk, Michael; Niemann, Julia; Reinmann, Gabi; Schnurr, Jan-Mathis; Jandt, Silke; Roßnagel, Alexander (2012b): Gläserne Freunde? Kompaktversion zur LfM-Studie „Digitale Privatsphäre. Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen“. Manuskriptfassung. Hg. v. Landesanstalt für Medien Nordrhein-Westfalen (LfM). Düsseldorf. Online verfügbar unter https://www.lfm-nrw.de/fileadmin/lfm-nrw/Forschung/Kompaktstudie-Glaeserne-Freunde.pdf, zuletzt geprüft am 26.07.2015.

Schorb, Bernd (1998): Stichwort Medienpädagogik. In: *Zeitschrift für Erziehungswissenschaften* (1), S. 7.

Schubert, Sigrid; Schwill, Andreas (2011): Didaktik der Informatik. 2. Aufl. Heidelberg: Spektrum Akademischer Verlag.

Schubert, Sigrid; Stechert, Peer; Freischlad, Stefan (2005): Die Phisher im Internet. Ein Beitrag zu Standards der informatischen Bildung über die Sicherheit im Netz. In: *LOG IN* 24 (135), S. 66–68.

Schulte, Carsten; Brinda, Torsten (2005): Beiträge der Objektorientierung zu einem Kompetenzmodell des informatischen Modellierens. In: Steffen Friedrich (Hg.): Unterrichtskonzepte für informatische Bildung. INFOS 2005, 11. GI-Fachtagung Informatik und Schule. Dresden, 28.-30.09.2005. Gesellschaft für Informatik e. V. Bonn: Köllen Druck + Verlag (LNI, P-60), S. 137–148.

Schulz, Andreas D. (2012): Nutzung und Datenschutzpraxis im studiVZ. Eine Untersuchung zum Selbstdatenschutz. In: *DuD* 36 (4), S. 262–269. Online verfügbar unter https://link.springer.com/content/pdf/10.1007/s11623-012-0096-4.pdf, zuletzt geprüft am 22.08.2019.

Sedlmeier, Peter; Renkewitz, Frank (2013): Forschungsmethoden und Statistik für Psychologen und Sozialwissenschaftler. 2., aktualisierte und erweiterte Auflage. München, Harlow, Amsterdam, Madrid, Boston, San Francisco, Don Mills, Mexico City, Sydney: Pearson Verlag (Always learning).

Seifert, Oliver; Sauck, Tony; Schwarzbach, Maximilian; Lerch, Christopher; Weinert, Martin; Knobelsdorf, Maria (2013): „Ich glaube, Google ist so was wie eine Vorhalle des Internets“ – Erste Ergebnisse einer qualitativen Untersuchung von Schülervorstellungen von der Suchmaschine Google. In: Norbert Breier, Peer Stechert und Thomas Wilke (Hg.): Informatik erweitert Horizonte. INFOS 2013, 15. GI-Fachtagung Informatik und Schule. Kiel, 26.-28.09.2013. Gesellschaft für Informatik e. V. Bonn: Köllen Druck + Verlag (LNI, P-219), S. 45–56.

Sekretariat der Kultusministerkonferenz (Hg.) (2016): Strategie der Kultusministerkonferenz "Bildung in der digitalen Welt". Hg. v. Sekretariat der Kultusministerkonferenz. Berlin. Online verfügbar unter www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2016/Bildung_digitale_Welt_Webversion.pdf, zuletzt geprüft am 29.01.2018.

Six, Ulrike; Gimmler, Roland (2013): Medienkompetenz im schulischen Kontext. In: Ines Vogel (Hg.): Kommunikation in der Schule. 1., neue Ausg. Stuttgart: UTB (UTB, 3649 : Schulpädagogik), S. 96–117.

Six, Ulrike; Gleich, Uli; Gimmler, Roland (Hg.) (2007): Kommunikationspsychologie -- Medienpsychologie. Lehrbuch. 1. Aufl. Weinheim: BeltzPVU Verlag.

Söllner, Matthias; Hoffmann, Axel; Hoffmann, Holger; Wacker, Arno; Leimeister, Jan Marco (2012): Understanding the Formation of Trust in IT Artifacts. In: F. George Joey (Hg.): Proceedings of the International Conference on Information Systems. ICIS 2012, 33rd International Conference on Information Systems. Orlando, FL, 16.-19.12.2012. Red Hook, NY 12571 USA: Curran Associates, Inc., S. 1–18.

Srivastava, Agrima; Geethakumari, G. (2013): Measuring privacy leaks in Online Social Networks. In: B. G. Sangameshwara, Sabu M. Thampi und V. N. Manjunath Aradhya (Hg.): Proceedings of the 2013 International Conference on Advances in Computing, Communications and Informatics. ICACCI 2013, the International Conference on Advances in Computing, Communications and Informatics. Mysore, India, 22.-25.8.2013. IEEE Communications Society. Piscataway, NJ: IEEE, S. 2095–2100. Online verfügbar unter https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6637504, zuletzt geprüft am 22.08.2019.

Stechert, Peer (2009): Fachdidaktische Diskussion von Informatiksystemen und der Kompetenzentwicklung im Informatikunterricht. Dissertation. Universität Siegen, Siegen. Fachbereich Elektrotechnik und Informatik. Online verfügbar unter http://dokumentix.ub.uni-siegen.de/opus/volltexte/2009/385/pdf/stechert.pdf, zuletzt geprüft am 05.02.2018.

Steil, Daniel (2019): Weiterentwicklung des Newsfeeds von InstaHub und Entwicklung einer Unterrichtsreihe zum Thema „Algorithmen in sozialen Netzwerken“ für die Sekundarstufe II. Masterarbeit. Universität Koblenz-Landau, Koblenz. Online verfügbar unter https://kola.opus.hbz-nrw.de/frontdoor/index/index/start/0/rows/10/sortfield/score/sortorder/desc/searchtype/simple/query/Steil/yearfq/2019/docId/2013, zuletzt geprüft am 19.12.2019.

Thielen, Johannes (2018): Entwicklung einer Unterrichtsreihe mit dem Thema Datenschutz zur Verbesserung der Datenschutzkompetenz von Schülerinnen und Schülern der Klassenstufe 6 an einem Gymnasium. Masterarbeit. Universität Koblenz-Landau, Koblenz. Online verfügbar unter https://kola.opus.hbz-nrw.de/frontdoor/index/index/start/0/rows/10/sortfield/score/sortorder/desc/searchtype/authorsearch/author/Thielen/authormodifier/contains_all/docId/1831, zuletzt geprüft am 15.06.2019.

Trepte, Sabine; Dienlin, Tobias; Reinecke, Leonard (2014a): Risky behaviors. How online experiences influence privacy behaviors. In: Birgit Stark, Oliver Quiring und Nikolaus Jackob (Hg.): Von der Gutenberg-Galaxis zur Google-Galaxis. Alte und neue Grenzvermessungen nach 50 Jahren DGPuK. 1. Aufl. Wiesbaden: UVK Verlagsgesellschaft (Schriftenreihe der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft, 50), S. 225–244.

Trepte, Sabine; Masur, Philipp K. (2015a): Privatheit im Wandel. Eine repräsentative Umfrage zur Wahrnehmung und Beurteilung von Privatheit. Hg. v. Universität Hohenheim. Lehrstuhl für Medienpsychologie. Stuttgart. Online verfügbar unter https://www.uni-hohenheim.de/fileadmin/einrichtungen/psych/Team_MP/Berichte/Bericht_-_Privatheit_im_Wandel_2014-06-18.pdf, zuletzt geprüft am 30.08.2019.

Trepte, Sabine; Masur, Philipp K. (2015b): Online-Privatheitskompetenz in Deutschland. Ergebnisse von zwei repräsentativen Studien. Hg. v. Universität Hohenheim. Lehrstuhl für Medienpsychologie. Stuttgart. Online verfügbar unter https://www.uni-hohenheim.de/fileadmin/einrichtungen/psych/Team_MP/Berichte/Privatheitskompetenz_2015-11-04.pdf, zuletzt geprüft am 30.08.2019.

Trepte, Sabine; Masur, Philipp K.; Pape, Thilo von (2014b): Privatheit im Wandel? Eine repräsentative Umfrage und eine Inhaltsanalyse zur Wahrung von Privatheit und Datenschutz. Forum Privatheit, 17.10.2014. Online verfügbar unter www.forum-privatheit.de/forum-privatheit-de/aktuelles/veranstaltungen/veranstaltungsdokumente/2014-10-20-symposium-forum-privatheit/Forumsbeitraege/Trepte_Privatheit-aus-psycholog.-Perspektive_Kick-Off-Forpri_2014-10-17.pdf, zuletzt geprüft am 22.08.2019.

Trepte, Sabine; Masur, Philipp K.; Scharkow, Michael; Dienlin, Tobias (2015a): Privatheitsbedürfnisse verschiedener Kommunikationstypen on- und offline. Ergebnisse einer repräsentativen Studie zum Umgang mit persönlichen Inhalten. In: *Media Perspektiven* (5), S. 250–257. Online verfügbar unter https://medienpsychologie.uni-hohenheim.de/fileadmin/einrichtungen/psych/Dateien/Publikationen/Trepte_Masur_Scharkow_Dienlin_2015_Privatheitsbeduerfnisse_verschiedener_Kommunikationstypen_on-_und_offline.pdf, zuletzt geprüft am 30.08.2019.

Trepte, Sabine; Teutsch, Doris (2016): Privacy Paradox. In: Nicole Krämer, Stephan Schwan, Dagmar Unz und Monika Suckfüll (Hg.): Medienpsychologie. Schlüsselbegriffe und Konzepte. Stuttgart: Kohlhammer Verlag, S. 372–377.

Trepte, Sabine; Teutsch, Doris; Masur, Philipp K.; Eicher, Carolin; Fischer, Mona; Hennhöfer, Alisa; Lind, Fabienne (2015b): Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In: Serge Gutwirth, Ronald Leenes und Paul de Hert (Hg.): Reforming European Data Protection Law. Dordrecht: Springer Verlag Netherlands (20), S. 333–365. Online verfügbar unter https://link.springer.com/chapter/10.1007/978-94-017-9385-8_14, zuletzt geprüft am 13.12.2017.

Vollbrecht, Ralf; Mägdefrau, Jutta (1999): Medienkompetenz als Ziel schulischer Medienpädagogik. In: *medien praktisch - Zeitschrift für Medienpädagogik* 23 (1), S. 54–57.

Wagner, Edgar (2010): Datenschutz als Bildungsaufgabe. In: *DuD* 34 (8), S. 557–561.

Wagner, Edgar (2012): Datenschutz als Bildungsauftrag. In: *DuD* 36 (2), S. 83–87.

Wagner, Kai (2013): Selbstdatenschutz durch präventive Verarbeitungskontrolle. Dissertation. Universität Hamburg, Hamburg. Fachbereich Informatik. Online verfügbar unter http://ediss.sub.unihamburg.de/volltexte/2013/6013/pdf/Dissertation.pdf, zuletzt geprüft am 22.09.2019.

Wagner, Ulrike; Brüggen, Niels; Gebel, Christa (2010): Persönliche Informationen in aller Öffentlichkeit? Ergebniszusammenfassung der Teilstudie „Persönliche Informationen in aller Öffentlichkeit? Jugendliche und ihre Perspektive auf Datenschutz und Persönlichkeitsrechte in Sozialen Netzwerkdiensten" im Rahmen der Untersuchung „Das Internet als Rezeptions- und Präsentationsplattform für Jugendliche" im Auftrag der Bayerischen Landeszentrale für neue Medien (BLM). Hg. v. Bayerische Landeszentrale für neuen Medien (BLM). München. Online verfügbar unter http://www.jff.de/jff/publikationen/weitere-veroeffentlichungen/artikel/art/persoenliche-informationen-in-aller-oeffentlichkeit-jugendliche-und-ihre-perspektive-auf-datenschutz/, zuletzt geprüft am 26.07.2015.

Wagner, Wolf-Rüdiger (2001): Datenschutz, Selbstschutz, Medienkompetenz. Wieviel informationstechnische Grundbildung braucht der kompetente Mediennutzer? In: *MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung* 4 (1), S. 1–16.

Wambach, Tim (2018): Retrospektive Analyse der Ausbreitung und dynamische Erkennung von Web-Tracking durch Sandboxing. Dissertation. Universität Koblenz-Landau, Koblenz. Institut für Wirtschafts- und Verwaltungsinformatik. Online verfügbar unter https://kola.opus.hbz-nrw.de/frontdoor/index/index/docId/1749, zuletzt geprüft am 01.11.2019.

Weichert, Thilo (2012): Datenschutzverstoß als Geschäftsmodell - der Fall Facebook. In: *DuD* 36 (10), S. 716–721.

Weichert, Thilo (2014): Technik, Terror, Transparenz. Stimmen Orwells Visionen? In: *LOG IN* 33 (178/179), S. 10–20.

Weinert, Franz E. (2001): Concept of competence – A conceptual Clarification. In: Dominique Simone Rychen und Laura Hersh Salganik (Hg.): Defining and Selecting Key Competencies. Göttingen: Hogrefe & Huber Verlag, S. 45–65.

Weinert, Franz E. (Hg.) (2002): Leistungsmessungen in Schulen. 2., unveränd. Aufl., Dr. nach Typoskript. Weinheim [u.a.]: Beltz-Verl. (Beltz Verlag Pädagogik).

Wirtz, Markus Antonius; Nachtigall, Christof (2012): Deskriptive Statistik. 6., überarbeitete Auflage. Weinheim: Beltz Juventa Verlag (Statistische Methoden für Psychologen, Teil 1).

Wolf, Thomas (2011): In den Fängen der Datendiebe. Daten bedeuten Macht - und Geld. In: *FOCUS MONEY ONLINE*. Online verfügbar unter https://link.springer.com/content/pdf/10.1007/978-3-642-35117-4.pdf, zuletzt geprüft am 19.09.19.

Wolf, Willi (1995): Qualitative versus quantitative Forschung. In: Eckard König und Peter Zedler (Hg.): Bilanz qualitativer Forschung. Bd. 1: Grundlagen qualitativer Forschung. 1. Aufl. Weinheim: Deutscher Studien Verlag, S. 309–329.

Wübbenhorst, Klaus (2018): Reaktive Messverfahren. Ausführliche Definition. Gabler Wirtschaftslexikon. Online verfügbar unter https://wirtschaftslexikon.gabler.de/definition/reaktive-messverfahren-43565/version-266894, zuletzt geprüft am 01.02.2019.

Youn, Seounmi (2008): Parental Influence and Teens' Attitude toward Online Privacy Protection. In: *The Journal of Consumer Affairs* 42 (3), S. 362–388, zuletzt geprüft am 22.08.19.

Zacharias, Wolfgang (2004): Neue Medien und kulturelle Bildung. Eine kultur- und medienpädagogische Herausforderung. In: Susanne Bergmann, Jürgen Lauffer, Lothar Mikos, Günter A. Thiele und Dieter Wiedemann (Hg.): Medienkompetenz. Modelle. Projekte. Bonn: Bundeszentrale für politische Bildung, S. 48–55.

Zeidler, Simon Alexander; Brüggemann, Sebastian (2014): Die Zukunft personalisierter Werbung im Internet. In: *Computer und Recht* 30 (4), S. 248–257.

Zorn, Isabel (2010): Konstruktionstätigkeit mit Digitalen Medien — Eine qualitative Studie als Beitrag zur Medienbildung. Dissertation. Universität Bremen, Bremen. Online verfügbar unter http://nbn-resolving.de/urn:nbn:de:gbv:46-diss000117767, zuletzt geprüft am 25.11.2017.

ANHANG

Inhaltsverzeichnis Anhang

ANHANG 2.1

Auswertung frei verfügbarer Unterrichtsmaterialien

Die folgenden Seiten umfassen eine Auflistung frei verfügbarer Unterrichtsmaterialien mit einer Einschätzung ihrer Qualität und ist aus (Makosch 2019) zusammengestellt (vgl. Abschnitt 2.4).

Nr.	Titel	Autor / Herausgeber / Verlag	Jahr	URL	Note
01	Knowhow für junge User. Mehr Sicherheit im Umgang mit dem World Wide Web. Materialien für den Unterricht. Baustein 8 | Was wir immer tun sollten: Mindestschutz!	Marco Fileccia; Birgit Kimmel; Stefanie Rack; Isabell Tatsch; Friederike Groschup / klicksafe	2016	https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Lehrerhandbuch/LH_Baustein_8.pdf	3
02	Datensatz - Datenschatz? Warum Datenschutz und Datensicherheit wichtig sind.	Steffen Haschler / klicksafe (Aus der Reihe klicksafe to go)	2017	https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks_to_go_Datensatz_-_Datenschatz.pdf	2
03	Ich bin öffentlich ganz privat. Datenschutz und Persönlichkeitsrechte im Web. Materialien für den Unterricht.	Stefanie Rack; Marco Fileccia; AK „Datenschutz und Bildung“ der Datenschutzbeauftragten des Bundes und der Länder / klicksafe	2015	https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatzmodule/LH_Zusatzmodul_Datenschutz_klicksafe.pdf	2
04	„Ethik macht klick". Werte-Navi fürs digitale Leben. Arbeitsmaterialien für Schule und Jugendarbeit. Baustein 1 Privatsphäre und Big Data	Petra Grimm; Karla Neef; Michael Waltinger; Birgit Kimmel; Stefanie Rack / klicksafe	2018	https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_LH_Zusatz_Ethik/LH_Zusatzmodul_medienethik_klicksafe_gesamt.pdf	4
05	Ich im Netz I. Inhalte in Sozialen Netzwerken reflektieren und bewerten.	Marco Fileccia / Stiftung Medienpädagogik Bayern	2017	https://www.medienfuehrerschein.bayern/Angebot/Weiterfuehrende_Schulen/6_und_7_Jahrgangsstufe/mediabase/pdf/Unterrichtseinheit_419.pdf	2
06	Ich im Netz III. Rechtliche Grundlagen kennen und reflektieren.	Kristina Hopf / Stiftung Medienpädagogik Bayern	2017	https://www.medienfuehrerschein.bayern/Angebot/Weiterfuehrende_Schulen/8_und_9_Jahrgangsstufe/mediabase/pdf/Unterrichtseinheit_216.pdf	2

Nr.	Titel	Autor / Herausgeber / Verlag	Jahr	URL	Note
07	Datenschutz und Soziale Netzwerke - „Selbst & Bewusst".	Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit in Kooperation mit Ingo Kriebisch, Volker Wegner / Landesinstitut für Lehrerbildung und Schulentwicklung	--	https://li.hamburg.de/contentblob/4392476/2a7f5dd417731006157a6f19bfd02414/data/pdf-unterricht-datenschutz-netzwerk.pdf	3
08	Schutz der Privatsphäre im Internet. Mit Übungen für den Unterricht.	Barbara Amann-Hechenberger; Barbara Buchegger; Sonja Schwarz; Piotr Luckos; Katharina Maimer; Sonja Schwarz / Österreichische Datenschutzkommission und Österreichisches Institut für angewandte Telekommunikation	2011	https://www.saferinternet.at/fileadmin/categorized/Materialien/Schulmaterial_Schutz_der_Privatsphaere_im_Internet.pdf	3
09	Leben im Netz - die digitale Gesellschaft. Baustein B: Nackt im Netz - Datenschutz und Privatsphäre	Holger Meeh / Landeszentrale für politische Bildung Baden-Württemberg	2010	http://www.politikundunterricht.de/2_3_10/internet.pdf	4
10	Datenschutz - das bleibt privat!	Internet-ABC e.V. (Hrsg.)	2017	https://www.internet abc.de/index.php?eID=ajaxRequest&action=downloadFile&src=fileadmin/user_upload/for_teachers/lernmodule/lernmodul-datenschutz.pdf&fileUid=53958	2
11	Risiken im Internet	Schuldnerhilfe Oberösterreich	2017	https://bmsk2.cms.apa.at/cms/konsumentenfragen/epaper.html?channel=CH3119&doc=CMS1424080633671&section=WEITERFUEHRENDES&index=2&i=0	4

Nr.	Titel	Autor / Herausgeber / Verlag	Jahr	URL	Note
12	Facebook – mit Chancen und Risiken bewusst umgehen	Sebastian Marcks / Bundeszentrale für politische Bildung	2012	https://www.bpb.de/lernen/digitale-bildung/unterricht-am-whiteboard/135488/facebook	1
13	Datenschutz und Privatheit im Netz	Daniel Schäfer / Hessischer Bildungsserver/Jugendmedien-schutz	--	https://jugendmedienschutz.bildung.hessen.de/lehrer/Unterrichtsmaterialien_Downloads/Unterrichsteinheiten/5.6_-_Datenschutz_Privatheit_Komplett.pdf	3
14	Big Up 4 Big Data	Medienfachberatung Schwaben (Bezirk Schwaben / Bezirksjugendring Schwaben)	2017	https://medienfachberatung.de/wp-content/uploads/2017/03/Spielanleitung-Big-Up-4-Big-Data_MFB-Schwaben.pdf	5
15	Persönliche Daten im Internet – so viel wie nötig, so wenig wie möglich	Ralf Willius, Kathrin Beckhuis / Niedersächsische Landesmedienanstalt	--	https://www.nlm.de/fileadmin/dateien/medienkompetenz/u_materialien_pdf/daten/Unterrichtseinheit_persoenliche_Daten.pdf	4
16	Unterrichtsidee: Datenschutz geht alle an	Bundesagentur für Arbeit; planet-berufe.de	--	http://planet-beruf.de/fileadmin/assets/PDF/Unterrichtsideen/pb_UI_Datenschutz_geht_alle_an.doc	5
17	Schutz der Privatsphäre im Internet. Arbeitsmaterialien für den Unterricht. Aus der Reihe: IT-Sicherheit macht Schule in Nordrhein-Westfalen	Wolfgang Dax-Romswinkel; Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen / Agentur >>secure-it.nrw<<	2008	https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Internet/Inhalt/Schutz_der_Privatsphaere_im_Internet/Schutz_der_Privatsphaere_im_Internet.pdf	3

Nr.	Titel	Autor / Herausgeber / Verlag	Jahr	URL	Note
18	Website: Youngdata	Unabhängige Datenschutzbehörden des Bundes und der Länder und des Kantons Zürich; Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI RLP)	--	https://www.youngdata.de/	2
19	Website: watch your web	IJAB - Fachstelle für Internationale Jugendarbeit der Bundesrepublik Deutschland e.V.	--	http://www.watchyourweb.de	4
20	Website: www.data-kids.de	Maja Smoltczyk (Berliner Beauftragte für Datenschutz und Informationsfreiheit)	--	https://data-kids.de/	3
21	Kommunikation in Sozialen Netzwerken	Christina Fanselow; Erika Patzer; Damir Skako/ Christina Fanselow; Cornelsen Verlag	2013	--	4
22	Warum ist Datenschutz wichtig? Das PRISM-Rollenspiel zum Thema Datenschutz	Der Lehrerfreund	2013	https://www.lehrerfreund.de/schule/1s/datenschutz-prism-spiel/4407	3

ANHANG 4.1

Im Rahmen der Gesamtstudie verwendete Items

Die folgenden Seiten umfassen die Auflistung aller Items, deren Zuordnung zu den ursprünglichen Studien und die Auswahl für die finale Erhebung (blau unterlegte Fragen).

Code[1]	Frage[2]	Quelle[3]
A1(a)	Wie häufig hast du in den letzten sechs Monaten ... [... dich auf einer Website oder bei einem Online-Dienst nicht angemeldet (registriert), weil man dort seine persönlichen Daten angeben musste?]	OPLIS
A1(b)	Wie häufig hast du in den letzten sechs Monaten ... [... bei der Anmeldung nicht Deine offizielle E-Mailadresse angegeben, um Deine Identität zu verschleiern?]	OPLIS
A1(c)	Wie häufig hast du in den letzten sechs Monaten ... [... in Deinem Internetbrowser die Cookies oder den Cache gelöscht?]	OPLIS
A1(d)	Wie häufig hast du in den letzten sechs Monaten ... [... Online-Dienstanbieter gebeten, Deine persönlichen Daten aus ihrer Datenbank zu löschen?]	OPLIS
A2(a)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Informationen im Internet recherchieren können]	DIVSI U9
A2(b)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Sich mit anderen im Internet vernetzen können]	DIVSI U9
A2(c)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Die eigene Person im Internet angemessen darstellen können]	DIVSI U9
A2(d)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Die eigene Privatsphäre im Internet gut schützen können]	DIVSI U9
A2(e)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Gewalttätigen, rassistischen und pornografischen Inhalten ausweichen können]	DIVSI U9
A2(f)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Konsequenzen des eigenen Hochladens von Textbeiträgen, Fotos und ähnlichem im digitalen Raum abschätzen können]	DIVSI U9
A2(g)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Zwischen privaten und öffentlichen Räumen im Internet unterscheiden können]	DIVSI U9
A2(h)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Vertrauenswürdigkeit von Informationsquellen im Internet einschätzen können]	DIVSI U9
A2(i)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Das Internet und digitale Medien zu kreativen Betätigungen und der Gestaltung eigener Inhalte nutzen können]	DIVSI U9
A3(a)	Schätze Dich selbst bei folgenden Fragen ein: [Ich kann gut einschätzen, was Online-Unternehmen mit meinen Daten und Informationen machen.]	OPLIS

[1] Der Code ist die Durchnummerierung des LimeSurvey-Fragebogens (vgl. Anhang A4.2); der Kleinbuchstabe gibt die evtl. Teilfrage an.
[2] Die Fragen, die hellblau unterlegt sind, sind die Fragen, die letztendlich in die finale Version aufgenommen worden sind (vgl. Anhang A4.7).
[3] Abkürzungen der verwendeten Studien, deren Quellen am Ende der Tabelle stehen.

Code	Frage	Quelle
A3(b)	Schätze Dich selbst bei folgenden Fragen ein: [Ich kenne Hard- und Softwareanwendungen, mit deren Hilfe man die eigenen Daten schützen kann.]	OPLIS
A3(c)	Schätze Dich selbst bei folgenden Fragen ein: [Über meine Rechte als Nutzer von Online-Angeboten weiß ich gut Bescheid.]	OPLIS
A4(a)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich suche immer erst nach Möglichkeiten, Musik im Internet kostenlos zu bekommen, bevor ich daran denke, sie zu kaufen.]	CM
A4(b)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich weiß genau, was ich tun muss, um den Kopierschutz einer Software oder eines Spiels zu umgehen (sogenanntes „cracken“).]	CM
A4(c)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.]	CM
A4(d)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich verwende gerne Freeware- oder Open-Source-Alternativen zu kostspieligen Software-Programmen.]	CM
A4(e)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich sichere in regelmäßigen Abständen die wichtigsten Daten auf einem CD/DVD-Rohling oder einer externen Festplatte.]	CM
A4(f)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.]	CM
A4(g)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Wenn ich mir die Originalversion einer Software nicht leisten kann, suche ich nach kostenlosen und legalen Freeware-Alternativen.]	CM
A4(h)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich denke nicht lange darüber nach, einen E-Mail-Anhang zu öffnen – ich tue es einfach.]	CM
A4(i)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Wenn ich per E-Mail oder im Chat einen Link zugesendet bekomme, klicke ich ihn meistens an, auch wenn ich mir nicht sicher bin, auf welcher Seite ich lande.]	CM
A4(j)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich achte nicht darauf, von welchen Seiten die Dateien stammen, die ich herunterlade.]	CM
A4(k)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich freue mich, wenn mich fremde Leute im Chat ansprechen und antworte ihnen gerne.]	CM
A4(l)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Filme, Musik, Spiele oder andere Software lade ich manchmal auch von etwas zwielichtigen Seiten.]	CM
A4(m)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Wenn ich von Fremden E-Mails erhalte, bin ich oft neugierig und öffne sie.]	CM
A4(n)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich lege Wert darauf, Originalversionen meiner Software zu besitzen.]	CM
A4(o)	Wie sehr treffen die folgenden Aussagen auf dich zu? [E-Mails, bei denen ich die Vermutung habe, dass es sich um unerwünschte Nachrichten (Spam) handelt, lösche ich sofort.]	CM
A4(p)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich vermeide es, auf Internetseiten zu surfen, die mir verdächtig oder zwielichtig erscheinen.]	CM

Code	Frage	Quelle
A4(q)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Dateianhänge bei E-Mails lasse ich immer erst von meinem Virenprogramm prüfen, bevor ich sie öffne.]	CM
A4(r)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich ändere in regelmäßigen Abständen alle meine Passwörter.]	CM
A4(s)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich benutze Passwörter, die ich mir möglichst leicht merken kann.]	CM
A4(t)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.]	CM
A4(u)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Aufgrund des hohen Sicherheitsrisikos im Internet schränke ich meine Online-Zeit ein.]	CM
A4(v)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich achte darauf, welche Informationen ich selbst über mich ins Internet stelle.]	CM
A4(w)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich achte darauf, welche Informationen über mich im Internet sichtbar sind.]	CM
A5(a)	Ich denke, ich bin in der Lage... [private Informationen über mich zu schützen.]	DP
A5(b)	Ich denke, ich bin in der Lage... [private Informationen geheim zu halten.]	DP
A5(c)	Ich denke, ich bin in der Lage... [Datenschutz zu verstehen.]	DP
B1(a)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze verschiedene Passwörter.]	DIVSI U25
B1(b)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze sichere Geräte mit persönlichem Passwort.]	DIVSI U25
B1(c)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... aktualisiere persönliche Sicherheitseinstellungen in Sozialen Netzwerken gegenüber Grundeinstellungen.]	DIVSI U25
B1(d)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze nur Seiten, bei denen ich weiß, dass sie sicher sind.]	DIVSI U25
B1(e)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... gebe keine persönlichen Daten in Sozialen Netzwerken preis.]	DIVSI U25
B1(f)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... gebe keine persönlichen Daten beim Mailen preis.]	DIVSI U25
B1(g)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... gebe keine persönlichen Daten beim Online-Shopping preis.]	DIVSI U25
B1(h)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... gebe keine persönlichen Daten beim Chatten preis.]	DIVSI U25
B1(i)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... mache bewusst falsche/irreführende persönliche Angaben.]	DIVSI U25
B1(j)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... lade keine Dateien hoch.]	DIVSI U25
B1(k)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... lade keine Dateien herunter.]	DIVSI U25
B1(l)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... lese die Datenschutzerklärungen auf Webseiten.]	DIVSI U25

Code	Frage	Quelle
B2(a)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze Pop-Up-Blocker oder Adblocker.]	DIVSI U25
B2(b)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze eine Firewall.]	DIVSI U25
B2(c)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze eine Verschlüsselungssoftware.]	DIVSI U25
B2(d)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [...aktualisiere regelmäßig meine Anti-Viren-Software.]	DIVSI U25
B2(e)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze Anti-Malware-Programme .]	OPLIS
B2(f)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze Anonymisierungstools.]	OPLIS
B2(g)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze Anti-Tracking-Software.]	OPLIS
B3(a)	Hast Du schon einmal folgende Strategien genutzt? [Aufgehört bestimmte Webseiten zu besuchen]	OPLIS
B3(b)	Hast Du schon einmal folgende Strategien genutzt? [Aus Sicherheitsbedenken einen Online-Einkauf unterlassen]	OPLIS
B3(c)	Hast Du schon einmal folgende Strategien genutzt? [Einen Online-Dienst nicht genutzt, um eigene Daten nicht für kommerzielle Zwecke herzugeben]	OPLIS
B3(d)	Hast Du schon einmal folgende Strategien genutzt? [Ein Pseudonym bei der Anmeldung benutzt]	OPLIS
B3(e)	Hast Du schon einmal folgende Strategien genutzt? [Anbieter gebeten, persönliche Daten nicht weiterzugeben]	OPLIS
B5(a)	Wie wichtig ist Dir jeweils einer der untenstehenden Aspekte bei der Nutzung eines Messengers? [Nutzerzahlen und Verbreitungsraum]	JIM
B5(b)	Wie wichtig ist Dir jeweils einer der untenstehenden Aspekte bei der Nutzung eines Messengers? [Zusatz wie Sticker, Sprachnachrichten, Telefonieren, Videoanrufe, ...]	JIM
B5(c)	Wie wichtig ist Dir jeweils einer der untenstehenden Aspekte bei der Nutzung eines Messengers? [Anzahl der Dateiformate, die weitergeleitet werden können]	JIM
B5(d)	Wie wichtig ist Dir jeweils einer der untenstehenden Aspekte bei der Nutzung eines Messengers? [Schnelligkeit der Übermittlung]	JIM
B5(e)	Wie wichtig ist Dir jeweils einer der untenstehenden Aspekte bei der Nutzung eines Messengers? [Verschlüsselung bei der Übermittlung]	JIM
B5(f)	Wie wichtig ist Dir jeweils einer der untenstehenden Aspekte bei der Nutzung eines Messengers? [Verschlüsselte Mitteilungen vom Provider (Anbieter) lesbar]	JIM
B5(g)	Wie wichtig ist Dir jeweils einer der untenstehenden Aspekte bei der Nutzung eines Messengers? [Sicherheit der Nachrichten bei Diebstahl des Schlüssels]	JIM
B5(h)	Wie wichtig ist Dir jeweils einer der untenstehenden Aspekte bei der Nutzung eines Messengers? [Identifikationsmöglichkeit des Gesprächspartners (Wissen, wer sein Gegenüber ist)]	JIM
C2	Was verbirgt sich hinter dem Begriff "Browserverlauf"? Im Browserverlauf werden ... [... die Adressen der besuchten Websites gespeichert.][4]	OPLIS

[4] Bei den Wissensfragen sind aus Platzgründen in dieser Tabelle die alternativen Antwortmöglichkeiten ausgelassen.

Code	Frage	Quelle
C3	Was ist ein "Cookie"? Ein Cookie ist … [… eine Datei, die es Internetseiten ermöglicht, den Nutzer beim erneuten Besuch wiederzuerkennen.]4	OPLIS
C4	Was versteht man unter dem Begriff "Cache"? [Einen Puffer-Speicher, der das Surfen im Internet beschleunigt.]4	OPLIS
C5	Was versteht man unter einem "Trojaner"? Ein Trojaner ist ein Computerprogramm, das … [… als nützliche Anwendung getarnt ist, im Hintergrund aber eine andere Funktion erfüllt.]4	OPLIS
C6	Was ist ein Bot-Netz? [Ein Netzwerk von Computern, die über eine Schadsoftware miteinander verbunden sind und von einem zentralen Computer im Internet (Server) aus ferngesteuert werden können.]4	CM
C7	Was ist eine "Firewall"? Eine Firewall ist … [… ein Sicherungssystem, das den Computer vor unerwünschten Netzangriffen schützen soll.][4]	OPLIS
C8	Welche Aufgabe hat eine Firewall? [Sie überwacht den eingehenden und ausgehenden Datenverkehr im Internet und kann so die Verbreitung von Viren und anderen Schadprogrammen eindämmen.][4]	CM
D1	Welche der folgenden Abkürzungen steht für eine Art der Verschlüsselung in drahtlosen Netzwerken (WLANs)? [WEP]4	CM
D2	Welches der folgenden Dinge kann nicht passieren, wenn man einen Virus auf dem Computer hat? [Über das Stromnetz können auch andere Haushaltsgeräte angegriffen und mit dem Virus infiziert werden.]4	CM
D3	Welche Arten von Daten können von einem Virus abgegriffen und an Fremde verschickt werden? [Prinzipiell alle Daten, die auf dem Computer gespeichert sind oder eingegeben werden, inklusive Passwörtern und Zugangsdaten (z.B. zum Online-Banking, Kreditkartennummern etc.).]4	CM
D4	Welche der folgenden URLs garantiert einen mit hoher Wahrscheinlichkeit datenabhörsicheren Zugriff auf die Webseite? [https://www.sparkasse.de][4]	CM
D5(a)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [Im Betriebssystem integrierte Firewall (z.B. Windows Firewall, Apple Firewall)]	CM
D5(b)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [Aktive Inhalte im Browser (z.B. JavaScript, ActiveX)]	CM
D5(c)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [Add-Ons im Browser (z.B. Browser Helper Objects)]	CM
D5(d)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [automatische Update-Services (z.B. Windows Update)]	CM
D5(e)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [Benutzerkontensteuerung, wie hier zu sehen: {Hier erscheint ein Bild zur Benutzerkontensteuerung}]	CM
D6	Sortiere die folgenden Dateianhänge je nach der Gefahr, einen Virus damit zu erhalten. Beim ersten Element ist die Gefahr am größten:	CM
E1(a)	Sind folgende Aussagen wahr oder falsch? [Die Weiterleitung anonymisierter Nutzerdaten zu Marktforschungszwecken ist in der EU gesetzlich erlaubt.]	OPLIS

Code	Frage	Quelle
E1(b)	Sind folgende Aussagen wahr oder falsch? [Für alle Sozialen Netzwerkseiten gelten in Deutschland die gleichen Standard-AGBs. Abweichungen müssen von den Betreibern kenntlich gemacht werden.]	OPLIS
E1(c)	Sind folgende Aussagen wahr oder falsch? [Laut dem deutschen Gesetz haben Nutzer von Online-Anwendungen, die personenbezogene Daten erheben und verarbeiten, einen Anspruch darauf, die über sie gespeicherten Daten einzusehen.]	OPLIS
E1(d)	Sind folgende Aussagen wahr oder falsch? [Man muss Deine Erlaubnis einholen, wenn man ein Foto oder Video von dir hochlädt, auf dem Du klar zu erkennen bist.]	OPLIS
E1(e)	Sind folgende Aussagen wahr oder falsch? [Wenn eine Firma dein Internetverhalten über mehrere Seiten verfolgen möchte, muss sie zuerst dein Einverständnis einholen.]	OPLIS
E1(f)	Sind folgende Aussagen wahr oder falsch? [Wenn du ein Zeitschriftenabonnement per Mail oder telefonisch bestellst, dann ist es dem Verlag nicht erlaubt, deine Adresse und Telefonnummer an andere Firmen ohne deine Genehmigung zu verkaufen.]	OPLIS
E2(a)	Wenn eine Website eine Datenschutzerklärung veröffentlicht, bedeutet das, [dass die Website keine Informationen über dich mit anderen Firmen teilen darf, bis du deine Genehmigung gegeben hast.]	Hoof
E2(b)	Wenn eine Website eine Datenschutzerklärung veröffentlicht, bedeutet das, [dass die Website deine Adresse und dein Kaufverhalten nicht der Regierung mitteilen darf.]	Hoof
E2(c)	Wenn eine Website eine Datenschutzerklärung veröffentlicht, bedeutet das, [dass die Website Informationen über dich löschen muss (wie Name und Adresse), wenn du sie aufforderst dies zu tun.]	Hoof
E3	Informationelle Selbstbestimmung ist...	OPLIS
F1	Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken (nicht) zu veröffentlichen? [Vorname]	DP
G1	Hast du die Privatsphärenoptionen in Facebook angepasst? [Ja]	DP
G2	Was hast du geändert? [Sichtbarkeit des Profils]	BIT
G3(a)	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Ich überlege mir sehr genau, welche Informationen ich auf Facebook über mich preisgebe und welche nicht.]	DP
G3(b)	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Wenn ich auf Facebook etwas veröffentliche, denke ich nicht darüber nach, wer es später sehen kann.]	DP
G3(c)	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Ich mache mir keine Sorgen um meine Daten im Internet, weil ich weiß, wie ich sie schützen kann.]	DP
G3(d)	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Es ist mir wichtig, selbst bestimmen zu können, wer im Internet etwas über mich erfährt und wer nicht.]	DP
G4(a)	Sind folgende Aussagen wahr oder falsch? [Die National Security Agency (NSA) greift nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.]	OPLIS

Code	Frage	Quelle
G4(b)	Sind folgende Aussagen wahr oder falsch? [Betreiber Sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar nicht nutzen.]	OPLIS
G4(c)	Sind folgende Aussagen wahr oder falsch? [Daten, die Betreiber Sozialer Netzwerke (z. B. Facebook) über die Nutzer sammeln, werden nach 5 Jahren gelöscht.]	OPLIS
G4(d)	Sind folgende Aussagen wahr oder falsch? [Unternehmen kombinieren Daten, die auf verschiedenen Websites im Internet hinterlassen werden und stellen daraus Nutzerprofile zusammen.]	OPLIS
G4(e)	Sind folgende Aussagen wahr oder falsch? [E-Mails werden häufig über mehrere Rechner weitergeleitet, bevor sie bei ihrem eigentlichen Empfänger ankommen.]	OPLIS
G4(f)	Sind folgende Aussagen wahr oder falsch? [Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.]	OPLIS
G4(g)	Sind folgende Aussagen wahr oder falsch? [Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.]	OPLIS
G4(h)	Sind folgende Aussagen wahr oder falsch? [Durch das Surfen im „Private Browsing"-Modus kann die Rekonstruktion des eigenen Surfverhaltens erschwert werden, da keine Browserinformationen gespeichert werden.]	OPLIS
G4(i)	Sind folgende Aussagen wahr oder falsch? [Durch die Nutzung von falschen Namen oder Pseudonymen kann die Identifikation der eigenen Person im Internet zumindest erschwert werden.]	OPLIS
G4(j)	Sind folgende Aussagen wahr oder falsch? [Auch wenn selbst schwere Passwörter von IT-Profis geknackt werden können, ist es sinnvoll Passwörter zu verwenden, die aus einer Kombination aus Buchstaben, Zahlen und Sonderzeichen bestehen und keine Wörter, Namen oder einfache Zahlenkombinationen enthalten.]	OPLIS
G4(k)	Sind folgende Aussagen wahr oder falsch? [Um den Zugang zu eigenen Daten zu erschweren, sollte man verschiedene Passwörter und Benutzernamen für unterschiedliche Anwendungen nutzen und diese häufig ändern.]	OPLIS
G4(l)	Sind folgende Aussagen wahr oder falsch? [Um sich vor Hackerangriffen zu schützen ist es sinnvoll, das eigene WLAN auszuschalten, wenn dieses nicht gebraucht wird.]	OPLIS
G4(m)	Sind folgende Aussagen wahr oder falsch? [Die Nutzung von Anonymisierungsprogrammen kann vor der Sammlung und Auswertung der eigenen Daten durch Geheimdienste und andere Institutionen schützen.]	OPLIS
G4(n)	Sind folgende Aussagen wahr oder falsch? [Online-Shops (z.B. Amazon) werten das Nutzungsverhalten von Kunden aus und erstellen auf dieser Basis Kaufempfehlungen oder entsprechend zugeschnittene Werbung.]	OPLIS
G4(o)	Sind folgende Aussagen wahr oder falsch? [Unternehmen sind in der Lage, Nutzern Online-Werbung anzuzeigen, die auf ihrem Surf-Verhalten basiert.]	OPLIS
G4(p)	Sind folgende Aussagen wahr oder falsch? [Alle Browser bieten die Möglichkeit, das Speichern von Drittanbieter-Cookies zu unterbinden.]	OPLIS
G4(q)	Sind folgende Aussagen wahr oder falsch? [Alle Browser unterstützen automatisch das aktuelle Transport Layer Security Verfahren (TLS 1.2.), welches vor allem mit HTTPS eingesetzt wird.]	OPLIS

Code	Frage	Quelle
H1(a)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Soziale Netzwerke.]	MP
H1(b)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Betriebssysteme.]	MP
H1(c)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Anti-Viren-Systeme.]	MP
H1(d)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Online-Händler.]	MP
H1(e)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Online-Spiele.]	MP
H1(f)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in App-Stores bzw. die Apps-/Softwareentwickler.]	MP
H1(g)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Website-Anbieter, dass sie vertrauensvoll mit meinen persönlichen Daten umgehen.]	MP
H2	Was sind für dich Risiken im Internet? [Infizierung des Computers mit Schadprogrammen]	DIVSI U 25
H3	Jetzt geht es um deine Einschätzungen zu Risiken im Umgang mit Computern und Internet. Wie hoch ist deiner Ansicht nach das Risiko, … [… dass beim Onlineshopping die Kontodaten ausgespäht werden?][5]	CM
H4	Bei welcher der folgenden E-Mails könnte es sich um einen typischen Betrugsversuch (Phishing) handeln?[6]	CM

[5] In dieser Frage gab es verschiedene Situationen, in denen das Risiko eingeschätzt werden sollte.
[6] Hier waren beispielhafte Screenshots eingefügt.

Quellen

BIT — BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Hg.) (2014): Jung und vernetzt. Kinder und Jugendliche in der digitalen Welt. Berlin. Online verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Jung-und-vernetzt-Kinder-und-Jugendliche-in-der-digitalen-Gesellschaft.html, zuletzt geprüft am 01.07.2018.

CM / MP — Kehr, Flavius; Rothmund, Tobias; Gollwitzer, Mario; Füllgraf, Wendy: Prädiktoren sicherheitsrelevanten Verhaltens bei jugendlichen Computernutzern. Computersicherheit und Medienkompetenz. Fragebogen der Studie. Landau.

DIVSI U9 — Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (Hg.) (2015): DIVSI U9-Studie. Kinder in der digitalen Welt. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Hamburg. Online verfügbar unter www.divsi.de/wp-content/uploads/2015/06/U9-Studie-DIVSI-web.pdf, zuletzt geprüft am 08.06.2018.

DIVSI U25 — Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (Hg.) (2014): DIVSI U25-Studie. Kinder, Jugendliche und junge Erwachsene in der digitalen Welt. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Hamburg. Online verfügbar unter www.divsi.de/wp-content/uploads/2014/02/DIVSI-U25-Studie.pdf, zuletzt geprüft am 01.07.2018.

DP — Schenk, Michael; Niemann, Julia; Reinmann, Gabi; Roßnagel, Alexander (2012): Digitale Privatsphäre. Heranwachsende und Datenschutz auf sozialen Netzwerkplattformen. Anhangband. Unter Mitarbeit von Silke Jandt und Jan-Mathis Schnurr. Landesanstalt für Medien Nordrhein-Westfalen (Schriftenreihe Medienforschung der Landesanstalt für Medien Nordrhein-Westfalen). Online verfügbar unter www.lfm-nrw.de/foerderung/forschung/abgeschlossene-projekte/schriftenreihe-medienforschung/digitale-privatsphaere.html, zuletzt geprüft am 01.07.2018.

Hoof — Hoofnagle, Chris Jay; King, Jennifer; Li, Su; Turow, Joseph (2010): How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? In: *SSRN Journal.* Online verfügbar unter papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864 zuletzt geprüft am 01.07.2018

JIM — Feierabend, Sabine; Plankenhorn, Theresa; Rathgeb, Thomas (2015): JIM-Studie 2015. Jugend, Information, (Multi-)Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland. Hg. v. Medienpädagogischer Forschungsverbund Südwest. Stuttgart. Online verfügbar unter www.mpfs.de/fileadmin/files/Studien/JIM/2015/JIM_Studie_2015.pdf, zuletzt geprüft am 02.07.2018.

OPLIS — Masur, Philipp K.; Teutsch, Doris; Trepte, Sabine (2017): Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). PREPRINT. Hohenheim. Online verfügbar unter www.oplis.de/docs/OPLIS_pre-print.pdf, zuletzt geprüft am 01.07.2018.

ANHANG 4.2

Fragebogen der Q-Sortierung

Die folgenden Seiten umfassen den aus LimeSurvey exportierten Fragebogen, der den Q-Sortierern vorgelegt worden ist; die zusätzlichen Nummerierungen in Kleinbuchstaben am rechten Rand neben den Skalen dienen der Zuordnung im Rückmeldebogen (vgl. Anhang A4.3).

Herzlich Willkommen zur Umfrage zum Thema Datenschutzkompetenz von Schülerinnen und Schülern.

In dieser Umfrage soll überprüft werden, wie gut und verständlich die Fragen sind, daher sind die Daten erstmal irrelevant. Ich bitte trotzdem um gewissenhaftes Ausfüllen, da diese Prä-Pilotierung die Umfrage verbessern soll.

Generell solltest du die Aufgaben aufmerksam, genau und komplett lesen und deine Antworten frei und ehrlich geben. Da die Umfrage anonym ist, können deine Antworten auch nicht auf deine Person zurückverfolgt werden.

Teil A: Persönliche Einschätzungen

Du findest auf dieser Seite eine Reihe von Aussagen und Fragen. Antworte bitte möglichst spontan und ehrlich, d.h. ohne über die Antwort lange nachzudenken. Bei diesen Fragen gibt es keine richtigen oder falschen Antworten – es zählt alleine Deine Meinung und wie du empfindest!

[Kommentar für die Q-Sortierer: Dies sind die Fragen aus Block A] **Zusätzliche Erläuterung für die Q-Sortierer, die nur in der Papierversion existiert.**

A1. Wie häufig hast du in den letzten sechs Monaten ...

Code zur internen *ZUS3*

	nie				sehr häufig	
... dich auf einer Website oder bei einem Online-Dienst nicht angemeldet (registriert), weil man dort seine persönlichen Daten angeben musste?	☐	☐	☐	☐	☐	a)
... bei der Anmeldung nicht Deine offizielle E-Mailadresse angegeben, um Deine Identität zu verschleiern?	☐	☐	☐	☐	☐	b)
... in Deinem Internetbrowser die Cookies oder den Cache gelöscht?	☐	☐	☐	☐	☐	c)
... Online-Dienstanbieter gebeten, Deine persönlichen Daten aus ihrer Datenbank zu löschen?	☐	☐	☐	☐	☐	d)

A2. Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten?

I11b

	sehr			gar nicht	kann ich nicht einschätzen	
Informationen im Internet recherchieren können	☐	☐	☐	☐	☐	a)
Sich mit anderen im Internet vernetzen können	☐	☐	☐	☐	☐	b)
Die eigene Person im Internet angemessen darstellen können	☐	☐	☐	☐	☐	c)

	sehr			gar nicht	kann ich nicht einschätzen	
Die eigene Privatsphäre im Internet gut schützen können	☐	☐	☐	☐	☐	d)
Gewalttätigen, rassistischen und pornografischen Inhalten ausweichen können	☐	☐	☐	☐	☐	e)
Konsequenzen des eigenen Hochladens von Textbeiträgen, Fotos und ähnlichem im digitalen Raum abschätzen können	☐	☐	☐	☐	☐	f)
Zwischen privaten und öffentlichen Räumen im Internet unterscheiden können	☐	☐	☐	☐	☐	g)
Vertrauenswürdigkeit von Informationsquellen im Internet einschätzen können	☐	☐	☐	☐	☐	h)
Das Internet und digitale Medien zu kreativen Betätigungen und der Gestaltung eigener Inhalte nutzen können	☐	☐	☐	☐	☐	i)

A3. Schätze Dich selbst bei folgenden Fragen ein:

ZUS2

	stimme gar nicht zu			stimme voll und ganz zu	kann ich nicht einschätzen	
Ich kann gut einschätzen, was Online-Unternehmen mit meinen Daten und Informationen machen.	☐	☐	☐	☐	☐	a)
Ich kenne Hard- und Softwareanwendungen, mit deren Hilfe man die eigenen Daten schützen kann.	☐	☐	☐	☐	☐	b)
Über meine Rechte als Nutzer von Online-Angeboten weiß ich gut Bescheid.	☐	☐	☐	☐	☐	c)

A4. Wie sehr treffen die folgenden Aussagen auf dich zu?

CM46

	trifft überhaupt nicht zu			trifft voll und ganz zu	weiß nicht	
Ich suche immer erst nach Möglichkeiten, Musik im Internet kostenlos zu bekommen, bevor ich daran denke, sie zu kaufen.	☐	☐	☐	☐	☐	a)
Ich weiß genau, was ich tun muss, um den Kopierschutz einer Software oder eines Spiels zu umgehen (sogenanntes „cracken“).	☐	☐	☐	☐	☐	b)
Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.	☐	☐	☐	☐	☐	c)
Ich verwende gerne Freeware- oder Open-Source-Alternativen zu kostspieligen Software-Programmen.	☐	☐	☐	☐	☐	d)
Ich sichere in regelmäßigen Abständen die wichtigsten Daten auf einem CD/DVD-Rohling oder einer externen Festplatte.	☐	☐	☐	☐	☐	e)
Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.	☐	☐	☐	☐	☐	f)
Wenn ich mir die Originalversion einer Software nicht leisten kann, suche ich nach kostenlosen und legalen Freeware-Alternativen.	☐	☐	☐	☐	☐	g)
Ich denke nicht lange darüber nach, einen E-Mail-Anhang zu öffnen – ich tue es einfach.	☐	☐	☐	☐	☐	h)
Wenn ich per E-Mail oder im Chat einen Link zugesendet bekomme, klicke ich ihn meistens an, auch wenn ich mir nicht sicher bin, auf welcher Seite ich lande.	☐	☐	☐	☐	☐	i)
Ich achte nicht darauf, von welchen Seiten die Dateien stammen, die ich herunterlade.	☐	☐	☐	☐	☐	j)

	trifft überhaupt nicht zu			trifft voll und ganz zu	weiß nicht	
Ich freue mich, wenn mich fremde Leute im Chat ansprechen und antworte ihnen gerne.	☐	☐	☐	☐	☐	k)
Filme, Musik, Spiele oder andere Software lade ich manchmal auch von etwas zwielichtigen Seiten.	☐	☐	☐	☐	☐	l)
Wenn ich von Fremden E-Mails erhalte, bin ich oft neugierig und öffne sie.	☐	☐	☐	☐	☐	m)
Ich lege Wert darauf, Originalversionen meiner Software zu besitzen.	☐	☐	☐	☐	☐	n)
E-Mails, bei denen ich die Vermutung habe, dass es sich um unerwünschte Nachrichten (Spam) handelt, lösche ich sofort.	☐	☐	☐	☐	☐	o)
Ich vermeide es, auf Internetseiten zu surfen, die mir verdächtig oder zwielichtig erscheinen.	☐	☐	☐	☐	☐	p)
Dateianhänge bei E-Mails lasse ich immer erst von meinem Virenprogramm prüfen, bevor ich sie öffne.	☐	☐	☐	☐	☐	q)
Ich ändere in regelmäßigen Abständen alle meine Passwörter.	☐	☐	☐	☐	☐	r)
Ich benutze Passwörter, die ich mir möglichst leicht merken kann.	☐	☐	☐	☐	☐	s)
Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.	☐	☐	☐	☐	☐	t)
Aufgrund des hohen Sicherheitsrisikos im Internet schränke ich meine Online-Zeit ein.	☐	☐	☐	☐	☐	u)
Ich achte darauf, welche Informationen ich selbst über mich ins Internet stelle.	☐	☐	☐	☐	☐	v)
Ich achte darauf, welche Informationen über mich im Internet sichtbar sind.	☐	☐	☐	☐	☐	w)

A5. Ich denke, ich bin in der Lage...

	sehr sicher			unsicher	weiß nicht	
private Informationen über mich zu schützen.	☐	☐	☐	☐	☐	a)
private Informationen geheim zu halten.	☐	☐	☐	☐	☐	b)
Datenschutz zu verstehen.	☐	☐	☐	☐	☐	c)

Teil B: Internetnutzung

[Kommentar für die Q-Sortierer: Die Unterteilungen in Teil A/B/... werden die Schüler später nicht sehen, es dient nur unserer Orientierung]

B1. Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten?

Ich...

I24

	Ja	Nein	weiß nicht	
... nutze verschiedene Passwörter.	☐	☐	☐	a)

	Ja	Nein	weiß nicht	
... nutze sichere Geräte mit persönlichem Passwort.	☐	☐	☐	b)
... aktualisiere persönliche Sicherheitseinstellungen in sozialen Netzwerken gegenüber Grundeinstellungen.	☐	☐	☐	c)
... nutze nur Seiten, bei denen ich weiß, dass sie sicher sind.	☐	☐	☐	d)
... gebe keine persönlichen Daten in sozialen Netzwerken preis.	☐	☐	☐	e)
... gebe keine persönlichen Daten beim Mailen preis.	☐	☐	☐	f)
... gebe keine persönlichen Daten beim Online-Shopping preis.	☐	☐	☐	g)
... gebe keine persönlichen Daten beim Chatten preis.	☐	☐	☐	h)
... mache bewusst falsche/irreführende persönliche Angaben.	☐	☐	☐	i)
... lade keine Dateien hoch.	☐	☐	☐	j)
... lade keine Dateien herunter.	☐	☐	☐	k)
... lese die Datenschutzerklärungen auf Webseiten.	☐	☐	☐	l)

B2. Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich...

	Ja	Nein	Weiß nicht	
... nutze Pop-Up- Blocker oder Adblocker.	☐	☐	☐	a)
... nutze eine Firewall.	☐	☐	☐	b)
... nutze eine Verschlüsselungssoftware.	☐	☐	☐	c)
... aktualisiere regelmäßig meine Anti-Viren-Software.	☐	☐	☐	d)
... nutze Anti-Malware-Programme .	☐	☐	☐	e)
... nutze Anonymisierungstools.	☐	☐	☐	f)
... Anti-Tracking-Software.	☐	☐	☐	g)

B3. Hast Du schon einmal folgende Strategien genutzt?

I25

	Ja	Nein	Weiß nicht	
Aufgehört bestimmte Webseiten zu besuchen	☐	☐	☐	a)
Aus Sicherheitsbedenken einen Online-Einkauf unterlassen	☐	☐	☐	b)

	Ja	Nein	Weiß nicht	
Einen Online-Dienst nicht genutzt, um eigene Daten nicht für kommerzielle Zwecke herzugeben	☐	☐	☐	c)
Ein Pseudonym bei der Anmeldung benutzt	☐	☐	☐	d)
Anbieter gebeten, persönliche Daten nicht weiterzugeben	☐	☐	☐	e)

B4. Nutzt Du einen Messenger wie z.B. WhatsApp?

☐ Ja

☐ Nein

B5. Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers?

I13

	sehr wichtig			unwichtig	
Nutzerzahlen und Verbreitungsraum	☐	☐	☐	☐	a)
Zusatz wie Sticker, Sprachnachrichten, Telefonieren, Videoanrufe, ...	☐	☐	☐	☐	b)
Anzahl der Dateiformate, die weitergeleitet werden können	☐	☐	☐	☐	c)
Schnelligkeit der Übermittlung	☐	☐	☐	☐	d)
Verschlüsselung bei der Übermittlung	☐	☐	☐	☐	e)
Verschlüsselte Mitteilungen vom Provider (Anbieter) lesbar	☐	☐	☐	☐	f)
Sicherheit der Nachrichten bei Diebstahl des Schlüssels	☐	☐	☐	☐	g)
Identifikationsmöglichkeit des Gesprächspartners (Wissen, wer sein Gegenüber ist)	☐	☐	☐	☐	h)

Teil C: Technisches

[Kommentar für die Q-Sortierer: Die Antwortmöglichkeiten in Frage C2 bis C9 werden randomisiert.]

C1. Welche Browsertools nutzt du?

I09

☐ Ghostery

☐ Adblock Plus

☐ Bug me not

☐ Firebug

☐ Flagfox

☐ Self-Destructing-Cookies

☐ Keine

Sonstiges ☐

Sonstiges

C2. Was verbirgt sicht hinter dem Begriff "Browserverlauf"?

Im Browserverlauf werden ...

TEC01

... die Adressen der besuchten Websites gespeichert. ☐

... Cookies von besuchten Websites abgelegt. ☐

... potenziell infizierte Websites separat abgelegt. ☐

... je nach Browsertyp unterschiedliche Informationen über den Nutzer gespeichert. ☐

Weiß ich nicht. ☐

C3. Was ist ein "Cookie"?

TEC02

Ein Computer-Virus, den man sich beim Besuch einer Website einfangen kann. ☐

Ein Browser-Plugin, das sicheres Surfen gewährleistet. ☐

Ein Programm, mit dem man die Datenspeicherung von Web-Anbietern unterbinden kann. ☐

Eine Text-Datei, die es Websites ermöglicht, den Nutzer beim erneuten Besuch wiederzuerkennen. ☐

Weiß ich nicht. ☐

C4. Was versteht man unter dem Begriff "Cache"?

TEC03

Einen Puffer-Speicher, der das Surfen im Internet beschleunigt. ☐

Ein Browser-Plug-In, welches den Datentransfer beim Surfen verschlüsselt. ☐

Ein Programm, welches Daten über den Internetnutzer gezielt ausspioniert und an Dritte weiterleitet. ☐

Ein Programm, welches Daten auf eine externe Festplatte kopiert, um diese vor Datenklau zu schützen. ☐

Weiß ich nicht. ☐

C5. Was versteht man unter einem "Trojaner"?

Ein Trojaner ist ein Computerprogramm, dass ...

TEC04

... als nützliche Anwendung getarnt ist, im Hintergrund aber eine andere Funktion erfüllt. ☐

... den Rechner vor Viren und anderen Schadprogrammen schützt. ☐

... nur zum Spaß entwickelt wurde und keine spezifische Funktion hat. ☐

... als Computervirus in den 90ern Schaden anrichtete, heute aber nicht mehr existiert. ☐

Weiß ich nicht. ☐

C6. Was ist ein Bot-Netz?

CM53

Ein Netzwerk von Computern, die über eine Schadsoftware miteinander verbunden sind und von einem zentralen Computer im Internet (Server) aus ferngesteuert werden können. ☐

Ein Netzwerk von Hilfsprogrammen, die standardmäßig in jede Anti-Viren-Software eingebaut sind und sich gegenseitig über Virenfunde benachrichtigen. ☐

Ein Bereich im Internet, in dem sich besonders viele Hacker und Kriminelle treffen. ☐

Weiß nicht ☐

C7. Was ist eine "Firewall"?

TEC05

Ein Sicherungssystem, das den Computer vor unerwünschten Netzangriffen schützen soll. ☐

Ein veraltetes Schutzprogramm gegen Computer-Viren. ☐

Ein Browser-Plugin, das sicheres Surfen ermöglicht. ☐

Eine neue technische Entwicklung, die verhindert, dass Daten bei einem Kurzschluss verloren gehen. ☐

Weiß ich nicht. ☐

C8. Welche Aufgabe hat eine Firewall?

CM51

Sie schützt den Rechner vor Überhitzung und den daraus entstehenden Schwelbränden, die ohne Firewall auf der Hauptplatine auftreten können. ☐

Sie überwacht den eingehenden und ausgehenden Datenverkehr im Internet und kann so die Verbreitung von Phishing-Mails eindämmen. ☐

Sie überwacht den eingehenden und ausgehenden Datenverkehr im Internet und kann so die Verbreitung von Viren und anderen Schadprogrammen eindämmen. ☐

Sie überwacht den eingehenden Datenverkehr und kann so bei Ermittlungen gegen Benutzer illegaler Download-Börsen helfen. ☐

Weiß nicht ☐

Teil D: Technisches Teil2

D1. Welche der folgenden Abkürzungen steht für eine Art der Verschlüsselung in drahtlosen Netzwerken (WLANs)?

CM52

EWP ☐

WEP ☐

PWE ☐

Weiß nicht ☐

D2. Welches der folgenden Dinge kann nicht passieren, wenn man einen Virus auf dem Computer hat?

CM57

Vom eigenen Computer aus werden unerwünschte E-Mail-Nachrichten (Spam) versandt. ☐

Über das Stromnetz können auch andere Haushaltsgeräte angegriffen und mit dem Virus infiziert werden. ☐

Die Festplatte kann gelöscht oder gar zerstört werden. ☐

Andere Computer im Internet können angegriffen und mit dem Virus infiziert werden. ☐

Weiß nicht ☐

D3. Welche Arten von Daten können von einem Virus abgegriffen und an Fremde verschickt werden?

CM59

Prinzipiell alle Daten, die auf dem Computer gespeichert sind oder eingegeben werden, inklusive Passwörtern und Zugangsdaten (z.B. zum Online-Banking, Kreditkartennummern etc.). ☐

Prinzipiell alle Daten, die auf dem Computer gespeichert sind oder eingegeben werden. Passwörter und Zugangsdaten können allerdings nicht gespeichert werden, da diese in Windows besonders gut gesichert sind. ☐

Vor allem illegal heruntergeladene MP3- und Videodateien, da bekanntermaßen Viren dafür spezialisiert sind. ☐

Weiß nicht ☐

D4. Welche der folgenden URLs garantiert einen mit hoher Wahrscheinlichkeit datenabhörsicheren Zugriff auf die Webseite?

CM58

http://www.sparkasse.de ☐

https://www.sparkasse.de ☐

http://www.sicher.sparkasse.de ☐

http://banking.sparkasse.de ☐

Weiß nicht ☐

D5. Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht.

CM210

	Aktiviert	Nicht aktiviert	Weiß nicht	
Im Betriebssystem integrierte Firewall (z.B. Windows Firewall, Apple Firewall)	☐	☐	☐	a)
Aktive Inhalte im Browser (z.B. Javascript, ActiveX)	☐	☐	☐	b)
Add-Ons im Browser (z.B. Browser Helper Objects)	☐	☐	☐	c)
automatische Update-Services (z.B. Windows Update)	☐	☐	☐	d)
Benutzerkontensteuerung, wie hier zu sehen:[Q-Sortierer: Hier erscheint das Bild zur Benutzerkontensteuerung]	☐	☐	☐	e)

D6. Sortiere die folgenden Dateianhänge je nach der Gefahr, einen Virus damit zu erhalten. Beim ersten Element ist die Gefahr am größten:

CM55

[Q-Sortierer: In der Online-Variante ist das Sortieren durch Drag and Drop möglich und ersichtlich.]

.exe / .ini	☐
.pdf	☐
.docx / .xlsx / .pptx	☐
.odt / .ods / .odp	☐
.java / .class	☐
.vbs	☐

Teil E: Rechtliches

E1. Sind folgende Aussagen wahr oder falsch?

GES01,GES03,GES04

	wahr	falsch	weiß nicht	
Die Weiterleitung anonymisierter Nutzerdaten zu Marktforschungszwecken ist in der EU gesetzlich erlaubt.	☐	☐	☐	a)
Für alle sozialen Netzwerkseiten gelten in Deutschland die gleichen Standard-AGBs. Abweichungen müssen von den Betreibern kenntlich gemacht werden.	☐	☐	☐	b)
Laut dem deutschen Gesetz haben Nutzer von Online-Anwendungen, die personenbezogene Daten erheben und verarbeiten, einen Anspruch darauf, die über sie gespeicherten Daten einzusehen.	☐	☐	☐	c)
Man muss Deine Erlaubnis einholen, wenn man ein Foto oder Video von dir hochlädt, auf dem Du klar zu erkennen bist.	☐	☐	☐	d)
Wenn eine Firma dein Internetverhalten über mehrere Seiten verfolgen möchte, muss sie zuerst dein Einverständnis einholen.	☐	☐	☐	e)
Wenn du ein Zeitschriftenabonnement per Mail oder telefonisch bestellst, dann ist es dem Verlag nicht erlaubt, deine Adresse und Telefonnummer an andere Firmen ohne deine Genehmigung zu verkaufen.	☐	☐	☐	f)

E2. Wenn eine Website eine Datenschutzerklärung veröffentlicht, bedeutet das,

	Ja	Nein	Weiß nicht	
dass die Website keine Informationen über dich mit anderen Firmen teilen darf, bis du deine Genehmigung gegeben hast.	☐	☐	☐	a)
dass die Website deine Adresse und dein Kaufverhalten nicht der Regierung mitteilen darf.	☐	☐	☐	b)
dass die Website Informationen über dich löschen muss (wie Name und Adresse), wenn du sie aufforderst dies zu tun.	☐	☐	☐	c)

E3. Informationelle Selbstbestimmung ist...

GES05

... ein philosophischer Begriff. ☐

... die zentrale Aufgabe des Bundesdatenschutzbeauftragten. ☐

... ein Grundrecht deutscher Bürger. ☐

... die zentrale Forderung datenverarbeitender Stellen. ☐

Weiß ich nicht. ☐

Teil F: Datenschutz

F1. Wie sensibel sind folgende Daten, um sie in sozialen Netzwerken (nicht) zu veröffentlichen?

	Sehr sensibel, sollten nicht veröffentlicht werden			Unsensibel, kann man bedenkenlos veröffentlichen	Weiß nicht
Vorname	☐	☐	☐	☐	☐
Nachname	☐	☐	☐	☐	☐
Nickname / Spitzname	☐	☐	☐	☐	☐
Geburtsdatum	☐	☐	☐	☐	☐
Alter	☐	☐	☐	☐	☐
Wohnort	☐	☐	☐	☐	☐
Straße + Hausnummer	☐	☐	☐	☐	☐
Telefon- / Handynummer	☐	☐	☐	☐	☐
Messengername / -nummer	☐	☐	☐	☐	☐
E-Mailadresse	☐	☐	☐	☐	☐
Webseite (sofern vorhanden)	☐	☐	☐	☐	☐
Fotos	☐	☐	☐	☐	☐
Kontakte	☐	☐	☐	☐	☐
Beziehungsstatus	☐	☐	☐	☐	☐
Ausbildung / Beruf	☐	☐	☐	☐	☐
Lieblingsfilme / -musik / -bücher / -serien	☐	☐	☐	☐	☐

	Sehr sensibel, sollten nicht veröffentlicht werden			Unsensibel, kann man bedenkenlos veröffentlichen	Weiß nicht
Interessen / Hobbies	☐	☐	☐	☐	☐
Lieblingsorte	☐	☐	☐	☐	☐
Politische Einstellung	☐	☐	☐	☐	☐
Sexuelle Orientierung	☐	☐	☐	☐	☐
Eigene Erlebnisse	☐	☐	☐	☐	☐
Eigene Gedanken	☐	☐	☐	☐	☐
Eigene Gefühle	☐	☐	☐	☐	☐
Eigene Sorgen/Ängste	☐	☐	☐	☐	☐
Religion	☐	☐	☐	☐	☐

F2. Welches Soziale Netzwerk nutzt Du am meisten?

- ☐ Facebook
- ☐ Google+
- ☐ Twitter
- ☐ Youtube
- ☐ Tumblr
- ☐ Instagram
- ☐ MySpace
- ☐ LinkedIn
- ☐ Pinterest
- ☐ Ich nutze kein soziales Netzwerk
- ☐ Sonstiges

Sonstiges

Teil G: Datenschutz 2

G1. Hast du die Privatsphärenoptionen in {INSERTANS:165449X24038X334477} angepasst?

[Q-Sortierer: {INSERTANS:165449X24038X334477} wird ersetzt durch das Soziale Netzwerk, welches in der vorhergehenden Frage ausgewählt wird.]

- ☐ Ja
- ☐ Nein
- ☐ Teilweise

G2. Was hast du geändert?

I17b

- ☐ Sichtbarkeit des Profils
- ☐ Sichtbarkeit der Posts
- ☐ Wer auf meinen Seiten posten darf
- ☐ Wer mich kontaktieren darf
- ☐ Für wen ich zu finden bin
- ☐ Sonstiges

Sonstiges

G3. Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu?

	trifft voll und ganz zu			trifft überhaupt nicht zu	
Ich überlege mir sehr genau, welche Informationen ich auf {INSERTANS:165449X24038X334477other} über mich preisgebe und welche nicht.	☐	☐	☐	☐	a)
Wenn ich auf {INSERTANS:165449X24038X334477other} etwas veröffentliche, denke ich nicht darüber nach, wer es später sehen kann.	☐	☐	☐	☐	b)
Ich mache mir keine Sorgen um meine Daten im Internet, weil ich weiß, wie ich sie schützen kann.	☐	☐	☐	☐	c)
Es ist mir wichtig, selbst bestimmen zu können, wer im Internet etwas über mich erfährt und wer nicht.	☐	☐	☐	☐	d)

G4. Sind folgende Aussagen wahr oder falsch?

PRA01-05

	wahr	falsch	weiß nicht	
Die National Security Agency (NSA) greift nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.	☐	☐	☐	a)
Betreiber sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar nicht nutzen.	☐	☐	☐	b)

	wahr	falsch	weiß nicht	
Daten, die Betreiber sozialer Netzwerke (z. B. Facebook) über die Nutzer sammeln, werden nach 5 Jahren gelöscht.	☐	☐	☐	c)
Unternehmen kombinieren Daten, die auf verschiedenen Websites im Internet hinterlassen werden und stellen daraus Nutzerprofile zusammen.	☐	☐	☐	d)
E-Mails werden häufig über mehrere Rechner weitergeleitet, bevor sie bei ihrem eigentlichen Empfänger ankommen.	☐	☐	☐	e)
Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.	☐	☐	☐	f)
Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.	☐	☐	☐	g)
Durch das Surfen im „Private Browsing"-Modus kann die Rekonstruktion des eigenen Surfverhaltens erschwert werden, da keine Browserinformationen gespeichert werden.	☐	☐	☐	h)
Durch die Nutzung von falschen Namen oder Pseudonymen kann die Identifikation der eigenen Person im Internet zumindest erschwert werden.	☐	☐	☐	i)
Auch wenn selbst schwere Passwörter von IT-Profis geknackt werden können, ist es sinnvoll Passwörter zu verwenden, die aus einer Kombination aus Buchstaben, Zahlen und Sonderzeichen bestehen und keine Wörter, Namen oder einfache Zahlenkombinationen enthalten.	☐	☐	☐	j)
Um den Zugang zu eigenen Daten zu erschweren, sollte man verschiedene Passwörter und Benutzernamen für unterschiedliche Anwendungen nutzen und diese häufig ändern.	☐	☐	☐	k)
Um sich vor Hackerangriffen zu schützen ist es sinnvoll, das eigene WLAN auszuschalten, wenn dieses nicht gebraucht wird.	☐	☐	☐	l)
Die Nutzung von Anonymisierungsprogrammen kann vor der Sammlung und Auswertung der eigenen Daten durch Geheimdienste und andere Institutionen schützen.	☐	☐	☐	m)
Online-Shops (z.B. Amazon) werten das Nutzungsverhalten von Kunden aus und erstellen auf dieser Basis Kaufempfehlungen oder entsprechend zugeschnittene Werbung.	☐	☐	☐	n)
Unternehmen sind in der Lage Nutzern Online-Werbung anzuzeigen, die auf ihrem Surf-Verhalten basiert.	☐	☐	☐	o)
Alle Browser bieten die Möglichkeit, das Speichern von Drittanbieter-Cookies zu unterbinden.	☐	☐	☐	p)
Alle Browser unterstützen automatisch das aktuelle Transport Layer Security Verfahren (TLS 1.2.), welches vor allem mit HTTPS eingesetzt wird.	☐	☐	☐	q)

Teil H: Risiko vs. Vertrauen

H1. Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu?

MP35

	stimme überhaupt nicht zu				stimme voll und ganz zu	
Ich habe Vertrauen in soziale Netzwerke.	☐	☐	☐	☐	☐	a)
Ich habe Vertrauen in Betriebssysteme.	☐	☐	☐	☐	☐	b)

	stimme überhaupt nicht zu				stimme voll und ganz zu	
Ich habe Vertrauen in Anti-Viren-Systeme.	☐	☐	☐	☐	☐	c)
Ich habe Vertrauen in Online-Händler.	☐	☐	☐	☐	☐	d)
Ich habe Vertrauen in Online-Spiele.	☐	☐	☐	☐	☐	e)
Ich habe Vertrauen in App-Stores bzw. die Apps-/Softwareentwickler.	☐	☐	☐	☐	☐	f)
Ich habe Vertrauen in Website-Anbieter, dass sie vertrauensvoll mit meinen persönlichen Daten umgehen.	☐	☐	☐	☐	☐	g)

H2. Was sind für dich Risiken im Internet?

I22

	Ja	Nein	Unsicher
Infizierung des Computers mit Schadprogrammen	☐	☐	☐
Unerwünschte Weitergabe von persönlichen Daten an Dritte	☐	☐	☐
Ausspionieren meiner persönlichen Daten	☐	☐	☐
Belästigung durch Spam-Mails	☐	☐	☐
Betrug beim Online-Einkauf	☐	☐	☐
Nutzung meiner Daten für Werbezwecke	☐	☐	☐
Beleidigung oder Belästigung im Internet	☐	☐	☐
Versendung unerwünschter E-Mails in meinem Namen	☐	☐	☐
Mobbing/Stalking	☐	☐	☐
Andere wissen, was ich mache, oder kennen meinen Aufenthaltsort	☐	☐	☐
Fake-Profile	☐	☐	☐
Verlust oder Löschung persönlicher Daten	☐	☐	☐
Veröffentlichung peinlicher/intimer Chats/Fotos/…	☐	☐	☐

H3. Jetzt geht es um deine Einschätzungen zu Risiken im Umgang mit Computern und Internet.

Wie hoch ist deiner Ansicht nach das Risiko, …

CM47

	sehr geringes Risiko			sehr hohes Risiko
… dass beim Onlineshopping die Kontodaten ausgespäht werden?	☐	☐	☐	☐

	sehr geringes Risiko			sehr hohes Risiko
… dass ausgespähte Kontodaten dazu genutzt werden können, Geld von Deinem Konto abzuheben?	☐	☐	☐	☐
… dass der Computer durch das Öffnen von Mailanhängen mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐
… dass beim Onlinebanking die Kontodaten ausgespäht werden?	☐	☐	☐	☐
… dass man es nicht merkt, wenn der Rechner mit einem Computervirus infiziert ist?	☐	☐	☐	☐
… dass ein Computervirus von der Antivirensoftware nicht erkannt wird?	☐	☐	☐	☐
… dass der Computer durch den Download von Dateien über Tauschbörsen (z.B. eMule, BitTorrent) mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐
… dass der Computer beim Surfen im Internet (ohne Dateien herunterzuladen) mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐

H4. Bei welcher der folgenden E-Mails könnte es sich um einen typischen Betrugsversuch (Phishing) handeln?

CM56

Die Bilder befinden sich auf A.4.2 /

[Q-Sortierer: Hier erscheinen die Bilder sparkasse1 und sparkasse 2]

	Phishing-Versuch	kein Phishing-Versuch
	☐	☐
	☐	☐

Teil I: Sonstiges

I1. Wie alt bist du?

☐☐☐☐☐☐☐☐

I2. Bist du männlich oder weiblich?

weiblich ☐

männlich ☐

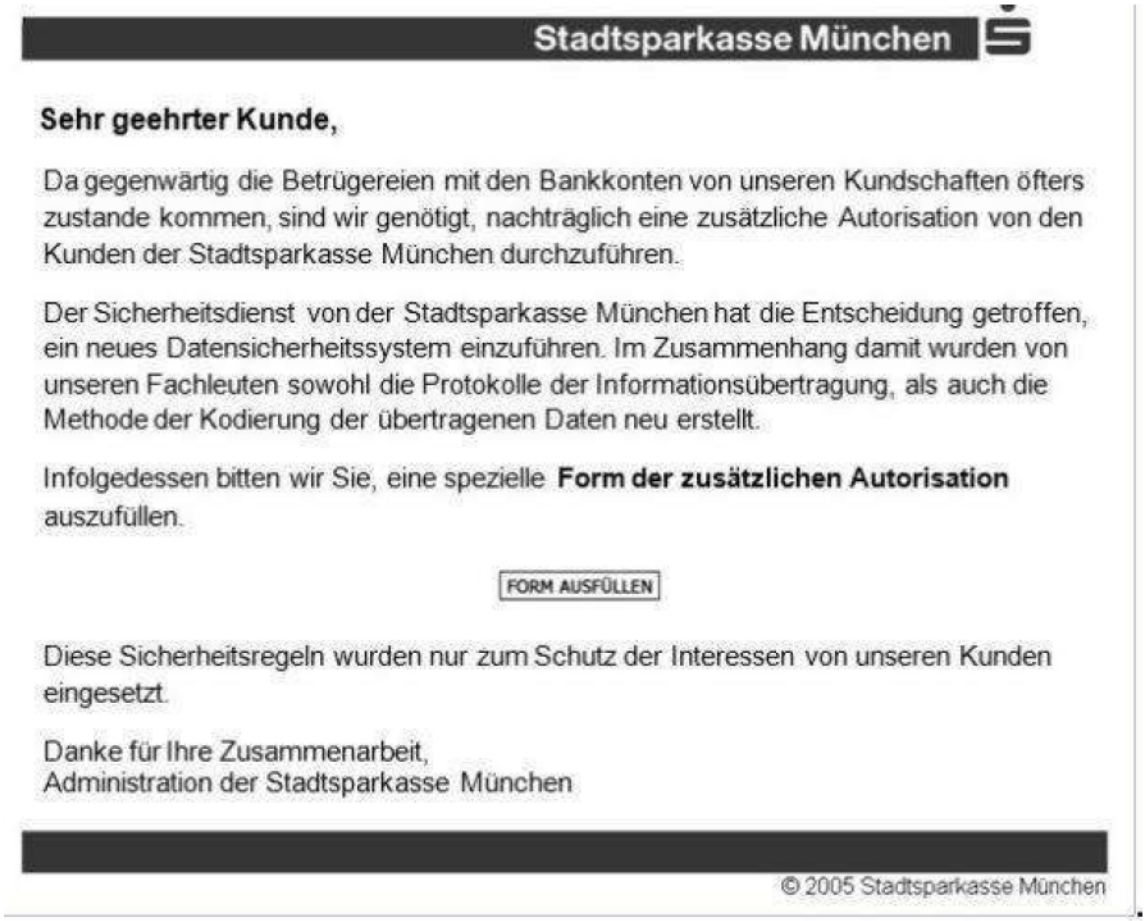
I3. Worüber hättest Du gerne mehr Informationen?

I28

	Ja	Unsicher	Nein
… zum Schutz meiner Daten im Internet	☐	☐	☐
… zur rechtlichen Situation in Bezug auf Datenschutz	☐	☐	☐
… zu technischen Möglichkeiten	☐	☐	☐
… zu den Gefahren beim Surfen im Internet	☐	☐	☐

Vielen Dank für die Teilnahme an der Umfrage. Mit den Ergebnissen können wir ein erstes Bild einholen und mit deiner Rückmeldung den Test verbessern, vereinfachen, kürzen oder auch vertiefen.

Sparkasse 1:



Stadtsparkasse München

Sehr geehrter Kunde,

Da gegenwärtig die Betrügereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind wir genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der Stadtsparkasse München durchzuführen.

Der Sicherheitsdienst von der Stadtsparkasse München hat die Entscheidung getroffen, ein neues Datensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die Protokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu erstellt.

Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

FORM AUSFÜLLEN

Diese Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.

Danke für Ihre Zusammenarbeit,
Administration der Stadtsparkasse München

© 2005 Stadtsparkasse München

Sparkasse 2:

Stadtsparkasse München

Sehr geehrter Herr Müller,

ich wünsche Ihnen im Namen der Stadtsparkasse München alles Gute zum Geburtstag, Glück, Gesundheit und viel Erfolg im neuen Lebensjahr.

Gerne möchte ich Ihnen bei der Planung Ihres finanziellen Erfolgs hilfreich zur Seite stehen. Zu diesem Zweck habe ich Ihnen einen persönlichen Finanzplan zusammengestellt, mit dem ihre Anlagen ideal an die Herausforderungen des kommenden Jahres angepasst sind.

Sie finden den Finanzplan auf dieser **speziellen Internetseite:**

FINANZPLAN ABRUFEN

Bitte setzen Sie sich möglichst bald mit mir in Verbindung, falls Sie Interesse an einer Finanzberatung haben.

Mit freundlichen Grüßen,

Jürgen W. Hartmann
Ihr Finanzberater

© 2005 Stadtsparkasse München

ANHANG 4.3

Erhebungsbogen zu den Fragen für die Q-Sortierung

Die folgenden Seiten umfassen den Erhebungsbogen für die Q-Sortierer, anhand dessen den Items die Dimensionen des Datenschutzkompetenzmodells zugeordnet worden sind.

Name: _____

Item	Erstauswahl OW	HW	RK	ANK	UK	HK	ggf. weitere Kompetenz (Abk. benutzen)	kein Konstrukt	Kommentar zum Item
A1(a)									
A1(b)									
A1(c)									
A1(d)									
A2(a)									
A2(b)									
A2(c)									
A2(d)									
A2(e)									
A2(f)									
A2(g)									
A2(h)									
A2(i)									
A3(a)									
A3(b)									
A3(c)									
A4(a)									
A4(b)									
A4(c)									
A4(d)									
A4(e)									
A4(f)									
A4(g)									
A4(h)									
A4(i)									
A4(j)									
A4(k)									
A4(l)									
A4(m)									
A4(n)									
A4(o)									
A4(p)									
A4(q)									
A4(r)									
A4(s)									
A4(t)									
A4(u)									
A4(u)									
A4(v)									
A4(w)									
A5(a)									
A5(b)									
A5(c)									
B1(a)									
B1(b)									
B1(c)									
B1(d)									
B1(e)									
B1(f)									
B1(g)									
B1(h)									
B1(i)									
B1(j)									
B1(k)									
B1(l)									
B2(a)									
B2(b)									
B2(c)									
B2(d)									
B2(e)									
B2(f)									
B2(g)									
B3(a)									
B3(b)									
B3(c)									
B3(d)									
B3(e)									
B5(a)									
B5(b)									
B5(c)									
B5(d)									
B5(e)									
B5(f)									
B5(g)									
B5(h)									

Item	Erstauswahl OW	HW	RK	ANK	UK	HK	ggf. weitere Kompetenz (Abk. benutzen)	kein Konstrukt	Kommentar zum Item
C2									
C3									
C4									
C5									
C6									
C7									
C8									
D1									
D2									
D3									
D4									
D5(a)									
D5(b)									
D5(c)									
D5(d)									
D5(e)									
D6									
E1(a)									
E1(b)									
E1(c)									
E1(d)									
E1(e)									
E1(f)									
E2(a)									
E2(b)									
E2(c)									
E3									
F1									
G1									
G2									
G3(a)									
G3(b)									
G3(c)									
G3(d)									
G4(a)									
G4(b)									
G4(c)									
G4(d)									
G4(e)									
G4(f)									
G4(g)									
G4(h)									
G4(i)									
G4(j)									
G4(k)									
G4(l)									
G4(m)									
G4(n)									
G4(o)									
G4(p)									
G4(q)									
H1(a)									
H1(b)									
H1(c)									
H1(d)									
H1(e)									
H1(f)									
H1(g)									
H2									
H3									
H4									

Abschließender Kommentar

ANHANG 4.4

Auswertung der Q-Sortierung

Die folgenden Seiten umfassen die Auswertung der Q-Sortierung und die Auswahl der Items für die Pilotierung und finale Erhebung (blau unterlegten Tabellenzeilen).

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W[1]	RK	ANK	UK	HK		
A1(a)	Wie häufig hast du in den letzten sechs Monaten ... [... dich auf einer Website oder bei einem Online-Dienst nicht angemeldet (registriert), weil man dort seine persönlichen Daten angeben musste?]	1	0	1	5	6	7	11	2	
A1(b)	Wie häufig hast du in den letzten sechs Monaten ... [... bei der Anmeldung nicht Deine offizielle E-Mailadresse angegeben, um Deine Identität zu verschleiern?]	1	0	1	7	3	2	19	0	
A1(c)	Wie häufig hast du in den letzten sechs Monaten ... [... in Deinem Internetbrowser die Cookies oder den Cache gelöscht?]	2	10	12	6	1	1	12	0	
A1(d)	Wie häufig hast du in den letzten sechs Monaten ... [... Online-Dienstanbieter gebeten, Deine persönlichen Daten aus ihrer Datenbank zu löschen?]	1	4	5	4	3	3	15	2	
A2(a)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Informationen im Internet recherchieren können]	15	0	15	0	13	2	0	2	
A2(b)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Sich mit anderen im Internet vernetzen können]	13	1	14	1	13	2	0	2	
A2(c)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Die eigene Person im Internet angemessen darstellen können]	5	2	7	3	5	8	5	4	
A2(d)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Die eigene Privatsphäre im Internet gut schützen können]	0	5	5	7	6	5	8	1	
A2(e)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Gewalttätigen, rassistischen und pornografischen Inhalten ausweichen können]	3	3	6	4	14	3	4	1	

[1] Während der Q-Sortierung wurde noch unterschieden zwischen *Hintergrundwissen* und *Orientierungswissen*; im Verlauf dieser Auswertung wurde jedoch klar, dass sich die beiden Dimensionen nicht trennscharf unterscheiden und wurden daher in *Wissen* zusammengefasst.

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
A2(f)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Konsequenzen des eigenen Hochladens von Textbeiträgen, Fotos und ähnlichem im digitalen Raum abschätzen können]	1	10	11	11	2	7	0	1	
A2(g)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Zwischen privaten und öffentlichen Räumen im Internet unterscheiden können]	7	8	15	6	6	4	0	1	
A2(h)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Vertrauenswürdigkeit von Informationsquellen im Internet einschätzen können]	3	3	6	13	3	9	0	1	
A2(i)	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich bei den folgenden Punkten? [Das Internet und digitale Medien zu kreativen Betätigungen und der Gestaltung eigener Inhalte nutzen können]	6	1	7	0	16	3	2	4	
A3(a)	Schätze Dich selbst bei folgenden Fragen ein: [Ich kann gut einschätzen, was Online-Unternehmen mit meinen Daten und Informationen machen.]	1	12	13	14	0	4	0	1	
A3(b)	Schätze Dich selbst bei folgenden Fragen ein: [Ich kenne Hard- und Softwareanwendungen, mit deren Hilfe man die eigenen Daten schützen kann.]	13	8	21	0	8	1	1	1	
A3(c)	Schätze Dich selbst bei folgenden Fragen ein: [Über meine Rechte als Nutzer von Online-Angeboten weiß ich gut Bescheid.]	5	23	28	1	0	2	0	1	
A4(a)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich suche immer erst nach Möglichkeiten, Musik im Internet kostenlos zu bekommen, bevor ich daran denke, sie zu kaufen.]	7	1	8	2	12	1	5	4	ANK
A4(b)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich weiß genau, was ich tun muss, um den Kopierschutz einer Software oder eines Spiels zu umgehen (sogenanntes „cracken“).]	12	8	20	2	4	0	4	2	

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
A4(c)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.]	3	6	9	3	5	0	14	1	HK
A4(d)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich verwende gerne Freeware- oder Open-Source-Alternativen zu kostspieligen Software-Programmen.]	5	1	6	1	13	2	5	5	
A4(e)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich sichere in regelmäßigen Abständen die wichtigsten Daten auf einem CD/DVD-Rohling oder einer externen Festplatte.]	2	5	7	6	3	0	14	2	HK
A4(f)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.]	2	0	2	5	7	9	6	3	UK
A4(g)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Wenn ich mir die Originalversion einer Software nicht leisten kann, suche ich nach kostenlosen und legalen Freeware-Alternativen.]	9	1	10	0	12	1	5	4	ANK
A4(h)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich denke nicht lange darüber nach, einen E-Mail-Anhang zu öffnen – ich tue es einfach.]	0	0	0	13	2	8	8	1	RK
A4(i)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Wenn ich per E-Mail oder im Chat einen Link zugesendet bekomme, klicke ich ihn meistens an, auch wenn ich mir nicht sicher bin, auf welcher Seite ich lande.]	0	0	0	13	2	8	8	1	RK
A4(j)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich achte nicht darauf, von welchen Seiten die Dateien stammen, die ich herunterlade.]	0	0	0	14	4	6	6	2	RK
A4(k)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich freue mich, wenn mich fremde Leute im Chat ansprechen und antworte ihnen gerne.]	1	2	3	11	2	8	6	2	
A4(l)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Filme, Musik, Spiele oder andere Software lade ich manchmal auch von etwas zwielichtigen Seiten.]	1	0	1	15	5	6	5	0	
A4(m)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Wenn ich von Fremden E-Mails erhalte, bin ich oft neugierig und öffne sie.]	0	1	1	15	3	5	7	1	

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
A4(n)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich lege Wert darauf, Originalversionen meiner Software zu besitzen.]	4	3	7	1	8	5	5	6	
A4(o)	Wie sehr treffen die folgenden Aussagen auf dich zu? [E-Mails, bei denen ich die Vermutung habe, dass es sich um unerwünschte Nachrichten (Spam) handelt, lösche ich sofort.]	0	2	2	7	3	6	13	1	HK
A4(p)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich vermeide es, auf Internetseiten zu surfen, die mir verdächtig oder zwielichtig erscheinen.]	0	0	0	10	10	3	9	0	
A4(q)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Dateianhänge bei E-Mails lasse ich immer erst von meinem Virenprogramm prüfen, bevor ich sie öffne.]	2	3	5	9	2	2	14	0	
A4(r)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich ändere in regelmäßigen Abständen alle meine Passwörter.]	1	1	2	6	1	2	20	1	HK
A4(s)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich benutze Passwörter, die ich mir möglichst leicht merken kann.]	1	4	5	15	1	0	8	3	
A4(t)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.]	5	3	8	3	3	2	13	3	HK
A4(u)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Aufgrund des hohen Sicherheitsrisikos im Internet schränke ich meine Online-Zeit ein.]	3	4	7	4	5	3	9	4	HK
A4(v)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich achte darauf, welche Informationen ich selbst über mich ins Internet stelle.]	0	3	3	4	4	8	13	0	HK
A4(w)	Wie sehr treffen die folgenden Aussagen auf dich zu? [Ich achte darauf, welche Informationen über mich im Internet sichtbar sind.]	2	3	5	4	4	7	12	0	
A5(a)	Ich denke, ich bin in der Lage... [private Informationen über mich zu schützen.]	2	6	8	4	4	5	10	1	
A5(b)	Ich denke, ich bin in der Lage... [private Informationen geheim zu halten.]	1	5	6	3	5	6	11	1	
A5(c)	Ich denke, ich bin in der Lage... [Datenschutz zu verstehen.]	2	18	20	1	1	7	2	1	

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
B1(a)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze verschiedene Passwörter.]	3	6	9	2	4	1	15	1	HK
B1(b)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze sichere Geräte mit persönlichem Passwort.]	3	5	8	3	5	2	13	1	HK
B1(c)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... aktualisiere persönliche Sicherheitseinstellungen in Sozialen Netzwerken gegenüber Grundeinstellungen.]	3	6	9	3	5	2	13	0	HK
B1(d)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze nur Seiten, bei denen ich weiß, dass sie sicher sind.]	1	3	4	8	4	4	12	0	HK
B1(e)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... gebe keine persönlichen Daten in Sozialen Netzwerken preis.]	1	1	2	10	3	3	13	1	
B1(f)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... gebe keine persönlichen Daten beim Mailen preis.]	1	2	3	8	3	2	15	1	
B1(g)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... gebe keine persönlichen Daten beim Online-Shopping preis.]	1	2	3	8	5	2	13	1	
B1(h)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... gebe keine persönlichen Daten beim Chatten preis.]	1	1	2	10	3	2	14	1	
B1(i)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... mache bewusst falsche/irreführende persönliche Angaben.]	2	2	4	5	1	4	16	2	
B1(j)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... lade keine Dateien hoch.]	1	2	3	7	4	2	13	3	
B1(k)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... lade keine Dateien herunter.]	1	2	3	6	6	2	12	3	

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
B1(l)	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... lese die Datenschutzerklärungen auf Webseiten.]	2	9	11	3	2	7	8	1	
B2(a)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze Pop-Up-Blocker oder Adblocker.]	6	3	9	1	12	1	8	1	ANK
B2(b)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze eine Firewall.]	7	2	9	3	11	1	7	1	ANK
B2(c)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze eine Verschlüsselungssoftware.]	7	2	9	3	11	1	7	1	ANK
B2(d)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... aktualisiere regelmäßig meine Antivirensoftware.]	6	3	9	3	12	1	6	1	ANK
B2(e)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze Anti-Malware-Programme .]	6	3	9	2	13	1	6	1	
B2(f)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze Anonymisierungstools.]	6	3	9	2	11	1	8	1	ANK
B2(g)	Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich... [... nutze Anti-Tracking-Software.]	6	3	9	2	11	1	8	1	ANK
B3(a)	Hast Du schon einmal folgende Strategien genutzt? [Aufgehört bestimmte Webseiten zu besuchen]	2	0	2	6	5	9	7	3	
B3(b)	Hast Du schon einmal folgende Strategien genutzt? [Aus Sicherheitsbedenken einen Online-Einkauf unterlassen]	1	1	2	8	5	10	6	1	
B3(c)	Hast Du schon einmal folgende Strategien genutzt? [Einen Online-Dienst nicht genutzt, um eigene Daten nicht für kommerzielle Zwecke herzugeben]	0	1	1	5	9	8	8	1	
B3(d)	Hast Du schon einmal folgende Strategien genutzt? [Ein Pseudonym bei der Anmeldung benutzt]	3	0	3	4	7	3	14	1	
B3(e)	Hast Du schon einmal folgende Strategien genutzt? [Anbieter gebeten, persönliche Daten nicht weiterzugeben]	1	0	1	6	5	5	12	3	

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
B5(a)	Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers? [Nutzerzahlen und Verbreitungsraum]	12	1	13	5	9	0	1	4	Ohne Dim.[2]
B5(b)	Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers? [Zusatz wie Sticker, Sprachnachrichten, Telefonieren, Videoanrufe, ...]	12	2	14	0	12	0	1	5	
B5(c)	Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers? [Anzahl der Dateiformate, die weitergeleitet werden können]	11	2	13	4	12	0	0	3	
B5(d)	Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers? [Schnelligkeit der Übermittlung]	11	3	14	0	12	0	1	5	Ohne Dim.[2]
B5(e)	Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers? [Verschlüsselung bei der Übermittlung]	3	8	11	12	4	3	0	2	RK
B5(f)	Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers? [Verschlüsselte Mitteilungen vom Provider (Anbieter) lesbar]	2	7	9	12	7	2	0	2	
B5(g)	Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers? [Sicherheit der Nachrichten bei Diebstahl des Schlüssels]	1	7	8	12	7	3	0	2	
B5(h)	Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers? [Identifikationsmöglichkeit des Gesprächspartners (Wissen, wer sein Gegenüber ist)]	1	4	5	15	8	2	0	2	RK
C2[3]	Was verbirgt sich hinter dem Begriff "Browserverlauf"? Im Browserverlauf werden ... [... die Adressen der besuchten Websites gespeichert.][4]	11	17	28	0	1	1	2	0	W
C3	Was ist ein "Cookie"? [Ein Computer-Virus, den man sich beim Besuch einer Website einfangen kann.]	9	22	31	1	0	0	0	0	W

[2] Diese Fragen wurden in die finale Studie übernommen, jedoch keiner Dimension zu sortiert, da sie keine Datenschutzkompetenz abfragen.

[3] An dieser Stelle wurde mit C2 weitergezählt, da C1 nur eine Vorbedingung zum Erscheinen bestimmter Fragen abgefragt hat.

[4] An dieser und den folgenden Stellen im Block C wurde nur die erste, möglicherweise auch falsche Antwortoption genannt.

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
C4	Was versteht man unter dem Begriff "Cache"? [Einen Puffer-Speicher, der das Surfen im Internet beschleunigt.]	9	22	31	0	0	0	0	1	
C5	Was versteht man unter einem "Trojaner"? Ein Trojaner ist ein Computerprogramm, dass ... [... als nützliche Anwendung getarnt ist, im Hintergrund aber eine andere Funktion erfüllt.]	7	24	31	1	0	0	0	0	W
C6	Was ist ein Bot-Netz? [Ein Netzwerk von Computern, die über eine Schadsoftware miteinander verbunden sind und von einem zentralen Computer im Internet (Server) aus ferngesteuert werden können.]	6	25	31	1	0	0	0	0	
C7	Was ist eine "Firewall"? [Ein Sicherungssystem, das den Computer vor unerwünschten Netzangriffen schützen soll.]	8	24	32	0	0	0	0	0	W
C8	Welche Aufgabe hat eine Firewall? [Sie überwacht den eingehenden und ausgehenden Datenverkehr im Internet und kann so die Verbreitung von Viren und andere Schadprogrammen eindämmen.]	6	26	32	0	0	0	0	0	
D1	Welche der folgenden Abkürzungen steht für eine Art der Verschlüsselung in drahtlosen Netzwerken (WLANs)? [WEP]	9	23	32	0	0	0	0	0	
D2	Welches der folgenden Dinge kann nicht passieren, wenn man einen Virus auf dem Computer hat? [Vom eigenen Computer aus werden unerwünschte E-Mail-Nachrichten (Spam) versandt.]	5	23	28	3	0	1	0	0	
D3	Welche Arten von Daten können von einem Virus abgegriffen und an Fremde verschickt werden? [Prinzipiell alle Daten, die auf dem Computer gespeichert sind oder eingegeben werden, inklusive Passwörtern und Zugangsdaten (z. B. zum Online-Banking, Kreditkartennummern etc.)]	4	24	28	3	0	1	0	0	
D4	Welche der folgenden URLs garantiert einen mit hoher Wahrscheinlichkeit datenabhörsicheren Zugriff auf die Webseite? [https://www.sparkasse.de]	6	22	28	3	0	1	0	0	W
D5(a)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [Im Betriebssystem integrierte Firewall (z.B. Windows Firewall, Apple Firewall)]	10	3	13	4	9	1	5	0	

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
D5(b)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [Aktive Inhalte im Browser (z.B. JavaScript, ActiveX)]	6	3	9	3	5	11	4	0	UK
D5(c)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [Add-Ons im Browser (z.B. Browser Helper Objects)]	10	4	14	3	7	3	5	0	
D5(d)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [automatische Update-Services (z.B. Windows Update)]	6	4	10	1	15	1	5	0	
D5(e)	Im Folgenden geht es nun um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf dem Computer, den du nutzt, aktiviert ist oder nicht. [Benutzerkontensteuerung, wie hier zu sehen:<Q-Sortierer: Hier erscheint das Bild zur Benutzerkontensteuerung>]	4	5	9	2	15	2	4	0	
D6	Sortiere die folgenden Dateianhänge je nach der Gefahr, einen Virus damit zu erhalten. Beim ersten Element ist die Gefahr am größten: <Rank 1>	4	15	19	10	0	3	0	0	
E1(a)	Sind folgende Aussagen wahr oder falsch? [Die Weiterleitung anonymisierter Nutzerdaten zu Marktforschungszwecken ist in der EU gesetzlich erlaubt.]	4	27	31	0	0	1	0	0	
E1(b)	Sind folgende Aussagen wahr oder falsch? [Für alle Sozialen Netzwerkseiten gelten in Deutschland die gleichen Standard-AGBs. Abweichungen müssen von den Betreibern kenntlich gemacht werden.]	4	27	31	0	0	1	0	0	
E1(c)	Sind folgende Aussagen wahr oder falsch? [Laut dem deutschen Gesetz haben Nutzer von Online-Anwendungen, die personenbezogene Daten erheben und verarbeiten, einen Anspruch darauf, die über sie gespeicherten Daten einzusehen.]	4	26	30	0	1	0	1	0	
E1(d)	Sind folgende Aussagen wahr oder falsch? [Man muss Deine Erlaubnis einholen, wenn man ein Foto oder Video von dir hochlädt, auf dem Du klar zu erkennen bist.]	4	26	30	1	0	0	1	0	W

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
E1(e)	Sind folgende Aussagen wahr oder falsch? [Wenn eine Firma dein Internetverhalten über mehrere Seiten verfolgen möchte, muss sie zuerst dein Einverständnis einholen.]	4	26	30	1	0	1	0	0	W
E1(f)	Sind folgende Aussagen wahr oder falsch? [Wenn du ein Zeitschriftenabonnement per Mail oder telefonisch bestellst, dann ist es dem Verlag nicht erlaubt, deine Adresse und Telefonnummer an andere Firmen ohne deine Genehmigung zu verkaufen.]	4	27	31	0	0	1	0	0	
E2(a)	Wenn eine Website eine Datenschutzerklärung veröffentlicht, bedeutet das, [dass die Website keine Informationen über dich mit anderen Firmen teilen darf, bis du deine Genehmigung gegeben hast.]	4	24	28	2	1	1	0	0	W
E2(b)	Wenn eine Website eine Datenschutzerklärung veröffentlicht, bedeutet das, [dass die Website deine Adresse und dein Kaufverhalten nicht der Regierung mitteilen darf.]	4	24	28	2	1	1	0	0	W
E2(c)	Wenn eine Website eine Datenschutzerklärung veröffentlicht, bedeutet das, [dass die Website Informationen über dich löschen muss (wie Name und Adresse), wenn du sie aufforderst dies zu tun.]	4	24	28	2	1	1	0	0	
E3	Informationelle Selbstbestimmung ist... [... ein Grundrecht deutscher Bürger.]	6	23	29	0	0	1	2	0	
F1	Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken (nicht) zu veröffentlichen? [Vorname]	1	2	3	15	1	10	3	0	RK
G1	Hast du die Privatsphärenoptionen in <Soziales Netzwerk> angepasst? [Ja]	5	0	5	4	7	10	5	1	UK
G2	Was hast du geändert? [Sichtbarkeit des Profils]	3	2	5	3	6	9	7	2	UK
G3(a)	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Ich überlege mir sehr genau, welche Informationen ich auf <Soziales Netzwerk> über mich preisgebe und welche nicht.]	0	2	2	9	3	11	6	1	

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
G3(b)	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Wenn ich auf <Soziales Netzwerk> etwas veröffentliche, denke ich nicht darüber nach, wer es später sehen kann.]	0	0	0	15	2	10	4	1	RK
G3(c)	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Ich mache mir keine Sorgen um meine Daten im Internet, weil ich weiß, wie ich sie schützen kann.]	0	2	2	9	1	12	7	1	
G3(d)	Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [Es ist mir wichtig, selbst bestimmen zu können, wer im Internet etwas über mich erfährt und wer nicht.]	0	1	1	6	3	12	7	3	UK
G4(a)	Sind folgende Aussagen wahr oder falsch? [Die National Security Agency (NSA) greift nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.]	4	27	31	0	0	1	0	0	W
G4(b)	Sind folgende Aussagen wahr oder falsch? [Betreiber Sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar nicht nutzen.]	7	23	30	0	1	1	0	0	W
G4(c)	Sind folgende Aussagen wahr oder falsch? [Daten, die Betreiber Sozialer Netzwerke (z. B. Facebook) über die Nutzer sammeln, werden nach 5 Jahren gelöscht.]	6	25	31	0	0	1	0	0	
G4(d)	Sind folgende Aussagen wahr oder falsch? [Unternehmen kombinieren Daten, die auf verschiedenen Websites im Internet hinterlassen werden und stellen daraus Nutzerprofile zusammen.]	7	23	30	0	0	2	0	0	
G4(e)	Sind folgende Aussagen wahr oder falsch? [E-Mails werden häufig über mehrere Rechner weitergeleitet, bevor sie bei ihrem eigentlichen Empfänger ankommen.]	10	20	30	1	0	1	0	0	
G4(f)	Sind folgende Aussagen wahr oder falsch? [Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.]	6	25	31	0	0	1	0	0	W

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
G4(g)	Sind folgende Aussagen wahr oder falsch? [Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.]	5	24	29	1	0	2	0	0	W
G4(h)	Sind folgende Aussagen wahr oder falsch? [Durch das Surfen im „Private Browsing"-Modus kann die Rekonstruktion des eigenen Surfverhaltens erschwert werden, da keine Browserinformationen gespeichert werden.]	4	22	26	2	2	2	0	0	W
G4(i)	Sind folgende Aussagen wahr oder falsch? [Durch die Nutzung von falschen Namen oder Pseudonymen kann die Identifikation der eigenen Person im Internet zumindest erschwert werden.]	3	23	26	1	2	2	1	0	
G4(j)	Sind folgende Aussagen wahr oder falsch? [Auch wenn selbst schwere Passwörter von IT-Profis geknackt werden können, ist es sinnvoll Passwörter zu verwenden, die aus einer Kombination aus Buchstaben, Zahlen und Sonderzeichen bestehen und keine Wörter, Namen oder einfache Zahlenkombinationen enthalten.]	2	24	26	1	1	3	1	0	
G4(k)	Sind folgende Aussagen wahr oder falsch? [Um den Zugang zu eigenen Daten zu erschweren, sollte man verschiedene Passwörter und Benutzernamen für unterschiedliche Anwendungen nutzen und diese häufig ändern.]	3	23	26	0	3	2	1	0	
G4(l)	Sind folgende Aussagen wahr oder falsch? [Um sich vor Hackerangriffen zu schützen ist es sinnvoll, das eigene WLAN auszuschalten, wenn dieses nicht gebraucht wird.]	3	22	25	1	2	2	2	0	
G4(m)	Sind folgende Aussagen wahr oder falsch? [Die Nutzung von Anonymisierungsprogrammen kann vor der Sammlung und Auswertung der eigenen Daten durch Geheimdienste und andere Institutionen schützen.]	6	23	29	0	1	2	0	0	

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
G4(n)	Sind folgende Aussagen wahr oder falsch? [Online-Shops (z.B. Amazon) werten das Nutzungsverhalten von Kunden aus und erstellen auf dieser Basis Kaufempfehlungen oder entsprechend zugeschnittene Werbung.]	8	22	30	0	1	1	0	0	W
G4(o)	Sind folgende Aussagen wahr oder falsch? [Unternehmen sind in der Lage Nutzern Online-Werbung anzuzeigen, die auf ihrem Surf-Verhalten basiert.]	7	23	30	0	1	1	0	0	
G4(p)	Sind folgende Aussagen wahr oder falsch? [Alle Browser bieten die Möglichkeit, das Speichern von Drittanbieter-Cookies zu unterbinden.]	7	23	30	1	0	1	0	0	
G4(q)	Sind folgende Aussagen wahr oder falsch? [Alle Browser unterstützen automatisch das aktuelle Transport Layer Security Verfahren (TLS 1.2.), welches vor allem mit HTTPS eingesetzt wird.]	6	23	29	2	0	1	0	0	
H1(a)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Soziale Netzwerke.]	0	2	2	12	0	15	1	2	
H1(b)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Betriebssysteme.]	0	1	1	13	0	15	1	2	
H1(c)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Anti-Viren-Systeme.]	0	2	2	12	0	15	1	2	
H1(d)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Online-Händler.]	0	2	2	12	0	15	1	2	
H1(e)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Online-Spiele.]	0	1	1	12	1	15	1	2	
H1(f)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in App-Stores bzw. die Apps-/Softwareentwickler.]	0	2	2	12	0	15	1	2	
H1(g)	Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu? [Ich habe Vertrauen in Website-Anbieter, dass sie vertrauensvoll mit meinen persönlichen Daten umgehen.]	0	0	0	14	0	15	1	2	

Item	Frage	Erstauswahl							Nicht beantwortet	Endgültige Zuordnung zur Dimension
		OW	HW	W	RK	ANK	UK	HK		
H2[5]	Was sind für dich Risiken im Internet? [Infizierung des Computers mit Schadprogrammen]	1	3	4	21	1	5	0	1	RK
H3	Jetzt geht es um deine Einschätzungen zu Risiken im Umgang mit Computern und Internet. Wie hoch ist deiner Ansicht nach das Risiko, … [… dass beim Onlineshopping die Kontodaten ausgespäht werden?]	0	1	1	22	2	7	0	0	RK
H4	Bei welcher der folgenden E-Mails könnte es sich um einen typischen Betrugsversuch (Phishing) handeln? <Hier erscheinen zwei E-Mails der Sparkasse München>	1	2	3	17	1	9	2	0	

Endgültige Auswahl und Zuordnung zu Dimension sind zeilenweise komplett blau markiert. Der daraus resultierende Fragebogen für die Pilotierung befindet sich in Anhang A4.5.

[5] Im Fall von H2 und H3 wurde nur die jeweils erste Option genannt.

ANHANG 4.5

Fragebogen der Pilotierung

Die folgenden Seiten umfassen den aus Lime Survey exportierten Fragebogen der Pilotierung vom November 2017.

Herzlich Willkommen

zur Umfrage zum Thema *Datenschutz und Jugendliche*. Auf den folgenden acht Seiten sind Fragen notiert, die Du durch einfaches ankreuzen beantworten kannst. Bitte lies die Aufgabe bzw. Fragestellung aufmerksam und sorgfältig durch (wie bei einer Klassenarbeit), bevor Du mit dem Antworten beginnst. Deine Antworten müssen frei und vor allem ehrlich gegeben werden, da diese sonst nutzlos für die Auswertung sind.

Die Umfrage ist anonym, das heißt, dass Deine Antworten nicht auf Deine Person zurückverfolgt werden können. Insbesondere können weder Deine Eltern noch Deine Lehrer Deine Antworten einsehen, nur das Gesamtergebnis aller an der Studie teilnehmenden Schülerinnen und Schüler wird auf Wunsch weitergegeben.

Teil A: Soziale Netzwerke

A1. Welches Soziale Netzwerk nutzt Du am meisten? [1]

- ☐ Facebook [2]
- ☐ Google+
- ☐ Twitter
- ☐ Youtube
- ☐ Tumblr
- ☐ Instagram
- ☐ MySpace
- ☐ Snapchat
- ☐ LinkedIn
- ☐ Pinterest
- ☐ Steam
- ☐ Twitch
- ☐ Ich nutze kein soziales Netzwerk

[1] Die Frage A1 wurde genutzt, um Fragen zu personalisieren: So wird im Folgenden {INSERTANS:211017X24370X336284} durch das Soziale Netzwerk, welches hier gewählt wurde, ersetzt.
[2] Die Linien zeigen an, dass nur eine Antwortoption auswählbar ist.

A2. Wie sensibel sind folgende Daten, um sie in sozialen Netzwerken NICHT zu veröffentlichen?

	Sehr sensibel, sollten nicht veröffentlicht werden			Unsensibel, kann man bedenkenlos veröffentlichen	Weiß nicht
Vorname	☐	☐	☐	☐	☐
Nachname	☐	☐	☐	☐	☐
Nickname / Spitzname	☐	☐	☐	☐	☐
Geburtsdatum	☐	☐	☐	☐	☐
Adresse mit Straße + Hausnummer, Wohnort	☐	☐	☐	☐	☐
Telefon- / Handynummer	☐	☐	☐	☐	☐
E-Mailadresse	☐	☐	☐	☐	☐
Fotos	☐	☐	☐	☐	☐
Kontakte	☐	☐	☐	☐	☐
Lieblingsfilme / -musik / -bücher / -serien	☐	☐	☐	☐	☐
Interessen / Hobbies	☐	☐	☐	☐	☐
Lieblingsorte	☐	☐	☐	☐	☐
Eigene Erlebnisse	☐	☐	☐	☐	☐
Eigene Gedanken / Gefühle / Sorgen	☐	☐	☐	☐	☐
Religion	☐	☐	☐	☐	☐

Teil B: Privatsphäre Soziale Netzwerke

B1. Hast Du die Privatsphäreneinstellungen in {INSERTANS:211017X24370X336284}[3] geändert?

- ☐ Ja
- ☐ Nein
- ☐ Teilweise

B2. Was hast Du geändert?

- ☐ Sichtbarkeit des Profils innerhalb {INSERTANS:211017X24370X336284}[3]
- ☐ Sichtbarkeit des Profils außerhalb {INSERTANS:211017X24370X336284}[3]
- ☐ Sichtbarkeit der Posts

[3] {INSERTANS:...} wurde ersetzt durch das Soziale Netzwerk aus der Frage A1.

Wer auf meinen Seiten posten darf ☐

Wer mich kontaktieren darf ☐

Für wen ich zu finden bin ☐

Sonstiges ☐

Sonstiges

B3. Was würdest Du in den Privatsphäreneinstellungen ändern, wenn Du ein Soziales Netzwerk nutzen würdest?

Diese Frage wird nur angezeigt, wenn kein SN genutzt wird

Sichtbarkeit des Profils innerhalb des Sozialen Netzwerks ☐

Sichtbarkeit des Profils außerhalb des Sozialen Netzwerks ☐

Sichtbarkeit der Posts ☐

Wer auf meinen Seiten posten darf ☐

Wer mich kontaktieren darf ☐

Für wen ich zu finden bin ☐

Sonstiges ☐

Sonstiges

B4. Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu?

	trifft voll und ganz zu			trifft überhaupt nicht zu
Ich achte darauf, welche Informationen ich selbst ins Internet oder {INSERTANS:211017X24370X336284}[3] stelle.	☐	☐	☐	☐
Wenn ich im Internet oder auf {INSERTANS:211017X24370X336284}[3] etwas veröffentliche, denke ich nicht darüber nach, wer es später sehen kann.	☐	☐	☐	☐
Ich mache mir keine Sorgen um meine Daten im Internet oder auf {INSERTANS:211017X24370X336284}[3], weil ich weiß, wie ich sie schützen kann.	☐	☐	☐	☐
Es ist mir wichtig, selbst bestimmen zu können, wer durch das Internet oder durch {INSERTANS:211017X24370X336284}[3] etwas über mich erfährt und wer nicht.	☐	☐	☐	☐

[3] {INSERTANS:...} wurde ersetzt durch das Soziale Netzwerk aus der Frage A1.

B5. **Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu?**

Diese Frage wird nur angezeigt, wenn kein Soziales Netzwerk genutzt wird

	trifft voll und ganz zu			trifft überhaupt nicht zu
Ich achte darauf, welche Informationen ich selbst ins Internet stelle.	☐	☐	☐	☐
Wenn ich im Internet etwas veröffentliche, denke ich nicht darüber nach, wer es später sehen kann.	☐	☐	☐	☐
Ich mache mir keine Sorgen um meine Daten im Internet, weil ich weiß, wie ich sie schützen kann.	☐	☐	☐	☐
Es ist mir wichtig, selbst bestimmen zu können, wer durch das Internet etwas über mich erfährt und wer nicht.	☐	☐	☐	☐

Teil C: Wissensfragen

C1.

Was versteht man unter einem "Trojaner"?Ein Trojaner ist ein Computerprogramm, dass ...

- ☐ ... den Rechner vor Viren und anderen Schadprogrammen schützt.
- ☐ ... als Computervirus in den 90ern Schaden anrichtete, heute aber nicht mehr existiert.
- ☐ ... als nützliche Anwendung getarnt ist, im Hintergrund aber eine andere Funktion erfüllt.
- ☐ ... nur zum Spaß entwickelt wurde und keine besondere Funktion hat.
- ☐ Weiß ich nicht.

C2. **Was ist ein "Cookie"?**

- ☐ Ein Computer-Virus, den man sich beim Besuch einer Internetseite einfangen kann.
- ☐ Ein Zusatzprogramm für den Browser, das sicheres Surfen ermöglicht.
- ☐ Ein Programm, mit dem man die Datenspeicherung von Web-Anbietern unterbinden kann.
- ☐ Eine Datei, die es Internetseiten ermöglicht, den Nutzer beim erneuten Besuch wiederzuerkennen.
- ☐ Weiß ich nicht.

C3. **Was ist eine "Firewall"?**

- ☐ Ein Sicherungssystem, das den Computer vor unerwünschten Netzangriffen schützen soll.
- ☐ Ein veraltetes Schutzprogramm gegen Computer-Viren.
- ☐ Ein Zusatzprogramm für den Browser, das sicheres Surfen ermöglicht.
- ☐ Eine neue technische Entwicklung, die verhindert, dass Daten bei einem Kurzschluss verloren gehen.
- ☐ Weiß ich nicht.

C4. **Was verbirgt sicht hinter dem Begriff "Browserverlauf"?**

Im Browserverlauf werden ...

... die Adressen der besuchten Internetseiten gespeichert. ☐

... Cookies von besuchten Websites abgelegt. ☐

... potenziell infizierte Internetseiten separat abgelegt. ☐

... je nach Browsertyp unterschiedliche Informationen über den Nutzer gespeichert. ☐

Weiß ich nicht. ☐

C5. **Welche der folgenden URLs garantiert einen mit hoher Wahrscheinlichkeit datenabhörsicheren Zugriff auf die Internetseite der Sparkasse?**

Antwortmöglichkeit bitte sorgfältig lesen!

http://www.sparkasse.de ☐

https://www.sparkasse.de ☐

http://www.sicher.sparkasse.de ☐

http://banking.sparkasse.de ☐

Weiß nicht ☐

Teil D: Messenger und Tools

D1. **Nutzt Du einen Messenger wie z.B. WhatsApp?**

Ja ☐

Nein ☐

D2. **Welche Browser kennst Du um durch das Internet zu surfen?**

Mozilla Firefox ☐

Internet Explorer / Microsoft Edge ☐

Google Chrome ☐

Safari ☐

Opera ☐

Keinen ☐

Sonstiges ☐

Sonstiges

D3. Welche Browser nutzt Du um durch das Internet zu surfen?

- [ ] Mozilla Firefox
- [ ] Internet Explorer / Microsoft Edge
- [ ] Google Chrome
- [ ] Safari
- [ ] Opera
- [ ] Keinen
- [ ] Keinen
- [ ] Sonstiges

Sonstiges

D4. Welche Browsertools kennst du?

- [ ] Ghostery
- [ ] Adblock Plus
- [ ] Bug me not
- [ ] Firebug
- [ ] Flagfox
- [ ] Self-Destructing-Cookies
- [ ] NoScript
- [ ] Keine
- [ ] Sonstiges

Sonstiges

D5. Welche Browsertools nutzt du?

- [ ] Ghostery
- [ ] Adblock Plus
- [ ] Bug me not
- [ ] Firebug
- [ ] Flagfox
- [ ] Self-Destructing-Cookies

NoScript ☐
Keine ☐
Keine ☐
Sonstiges ☐

Sonstiges

D6. Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers?

	sehr wichtig			unwichtig
Die Verschlüsselung bei der Übermittlung der Daten.	☐	☐	☐	☐
Die Identifikationsmöglichkeit des Gesprächspartners, das heißt zu wissen, wer mein Gegenüber ist.	☐	☐	☐	☐
Die Anzahl der Nutzer im Freundes- und Familienkreis.	☐	☐	☐	☐
Die Geschwindigkeit der Übermittlung von Nachrichten und Daten.	☐	☐	☐	☐

Teil E: Wissensfragen 2

E1. Wenn auf einer Internetseite eine Datenschutzerklärung veröffentlicht wurde,bedeutet das,

	Ja	Nein	Weiß nicht
dass der Anbieter der Internetseite keine Informationen über Dich mit anderen Firmen teilen darf, bis Du Deine Genehmigung gegeben hast.	☐	☐	☐
dass der Anbieter der Internetseite Deine Adresse und Dein Kaufverhalten nicht der Regierung mitteilen darf.	☐	☐	☐
dass der Anbieter der Internetseite Informationen über Dich löschen muss (wie Name und Adresse), wenn Du ihn aufforderst dies zu tun.	☐	☐	☐

E2. Sind folgende Aussagen wahr oder falsch?

	wahr	falsch	weiß nicht
Für alle sozialen Netzwerkseiten (z.B. Facebook) gelten in Deutschland die gleichen Standard-AGBs (Allgemeine Geschäftsbedingungen). Abweichungen müssen von den Betreibern kenntlich gemacht werden.	☐	☐	☐
Man muss Deine Erlaubnis einholen, wenn man ein Foto oder Video von dir hochlädt, auf dem Du klar zu erkennen bist.	☐	☐	☐
Wenn eine Firma dein Internetverhalten über mehrere Seiten verfolgen möchte, muss sie zuerst dein Einverständnis einholen.	☐	☐	☐
Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.	☐	☐	☐
Ich verwende Passwörter, die aus einer Kombination aus Buchstaben, Zahlen und Sonderzeichen bestehen und keine Wörter, Namen oder einfache Zahlenkombinationen enthalten.	☐	☐	☐

	wahr	falsch	weiß nicht
Ich nutze Anonymisierungsprogramme, um meine Daten vor der Sammlung und Auswertung durch Geheimdienste und andere Institutionen schützen.	☐	☐	☐

E3. Sind folgende Aussagen wahr oder falsch?

	wahr	falsch	weiß nicht
Die Geheimdienste (wie zum Beispiel der amerikanische Geheimdinest NSA [National Security Agency]) greifen nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.	☐	☐	☐
Betreiber sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar nicht nutzen.	☐	☐	☐
E-Mails werden häufig über mehrere Rechner weitergeleitet, bevor sie bei ihrem eigentlichen Empfänger ankommen.	☐	☐	☐
Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.	☐	☐	☐
Durch das Surfen im „Private Browsing"-Modus ist man anonym im Internet, da keine Browserinformationen gespeichert werden.	☐	☐	☐
Online-Shops (z.B. Amazon) werten das Nutzungsverhalten von Kunden aus und erstellen auf dieser Basis Kaufempfehlungen oder entsprechend zugeschnittene Werbung.	☐	☐	☐

Teil F: Risikoeinschätzung

F1. Was sind für dich Risiken im Internet?

	Ja	Nein	Unsicher
Die unerwünschte Weitergabe von persönlichen Daten an Dritte	☐	☐	☐
Das Ausspionieren meiner persönlichen Daten	☐	☐	☐
Das Empfangen von Spam-Mails	☐	☐	☐
Die Beleidigungen und Belästigungen im Internet	☐	☐	☐
Das Versenden unerwünschter E-Mails in meinem Namen	☐	☐	☐
Andere wissen, was ich mache, oder kennen meinen Aufenthaltsort	☐	☐	☐
Die Veröffentlichung peinlicher/intimer Chats/Fotos/…	☐	☐	☐

F2. Jetzt geht es um DEINE Einschätzungen zu Risiken im Umgang mit Computern und Internet.

Wie hoch ist Deiner Ansicht nach das Risiko, …

	sehr geringes Risiko			sehr hohes Risiko
… dass der Computer durch das Öffnen von Mailanhängen mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐

	sehr geringes Risiko			sehr hohes Risiko
… dass man es nicht merkt, wenn der Rechner mit einem Computervirus infiziert ist?	☐	☐	☐	☐
… dass ein Computervirus von der Antivirensoftware nicht erkannt wird?	☐	☐	☐	☐
… dass der Computer durch den Download von Dateien über Tauschbörsen (z.B. eMule, BitTorrent) mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐
… dass der Computer beim Surfen im Internet (ohne Dateien herunterzuladen) mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐

Teil G: Maßnahmen Datenschutz

G1. Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? Ich...

	Ja	Nein	Weiß nicht
... nutze Pop-Up- Blocker oder Adblocker.	☐	☐	☐
... nutze eine Firewall.	☐	☐	☐
... nutze eine Verschlüsselungssoftware beim E-Mailen und Chatten.	☐	☐	☐
... aktualisiere regelmäßig meine Anti-Viren-Software.	☐	☐	☐
... nutze Anti-Malware-Programme. (Malware ist jede Art von Computerprogramm, die entwickelt wurden, um unerwünschte oder gegebenenfalls schädliche Funktionen auszuführen.)	☐	☐	☐
... nutze Anonymisierungstools. (Ein Anonymisierungstool ist eine Software, die Daten beim Surfen so verändert, dass keine Rückschlüsse auf Dich als Besucher der Internetseiten gezogen werden können.)	☐	☐	☐
... nutze Anti-Tracking-Software. (Anti-Tracking-Software ist eine Software, die ein Nachverfolgen des Besuchs von Internetseiten verhindert.)	☐	☐	☐
... nutze verschiedene Passwörter.	☐	☐	☐
... nutze sichere Geräte mit persönlichem Passwort.	☐	☐	☐
... aktualisiere persönliche Sicherheitseinstellungen in sozialen Netzwerken gegenüber Grundeinstellungen.	☐	☐	☐
... nutze nur Seiten, bei denen ich weiß, dass sie sicher sind.	☐	☐	☐
... habe Aktive Inhalte im Browser (z.B. Javascript, ActiveX) aktiviert.	☐	☐	☐
... habe eine Benutzerkontensteuerung eingerichtet, wie hier zu sehen:	☐	☐	☐

(Das Bild befindet sich am Ende dieses Fragebogens.)

Teil H: Eigenes Verhalten

H1. Wie sehr treffen die folgenden Aussagen auf Dich zu?

	trifft überhaupt nicht zu				trifft voll und ganz zu	weiß nicht
Ich suche immer erst nach Möglichkeiten, Musik im Internet kostenlos zu bekommen, bevor ich daran denke, sie zu kaufen.	☐	☐	☐	☐	☐	☐
Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.	☐	☐	☐	☐	☐	☐
Ich sichere in regelmäßigen Abständen die wichtigsten Daten auf einem CD/DVD-Rohling oder einer externen Festplatte.	☐	☐	☐	☐	☐	☐
Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.	☐	☐	☐	☐	☐	☐
Wenn ich mir die Originalversion einer Software nicht leisten kann, suche ich nach kostenlosen und legalen Freeware-Alternativen.	☐	☐	☐	☐	☐	☐
Ich denke nicht lange darüber nach, einen E-Mail-Anhang zu öffnen – ich tue es einfach.	☐	☐	☐	☐	☐	☐
Wenn ich per E-Mail oder im Chat einen Link zugesendet bekomme, klicke ich ihn meistens an, auch wenn ich mir nicht sicher bin, auf welcher Seite ich lande.	☐	☐	☐	☐	☐	☐
Ich achte nicht darauf, von welchen Seiten die Dateien stammen, die ich herunterlade.	☐	☐	☐	☐	☐	☐
E-Mails, bei denen ich die Vermutung habe, dass es sich um unerwünschte Nachrichten (Spam) handelt, lösche ich sofort.	☐	☐	☐	☐	☐	☐
Ich ändere in regelmäßigen Abständen alle meine Passwörter.	☐	☐	☐	☐	☐	☐
Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.	☐	☐	☐	☐	☐	☐
Aufgrund des hohen Sicherheitsrisikos im Internet schränke ich meine Online-Zeit ein.	☐	☐	☐	☐	☐	☐
Ich achte darauf, welche Informationen ich selbst über mich ins Internet stelle.	☐	☐	☐	☐	☐	☐

Teil I: Persönliche Informationen

I1. Bist du männlich oder weiblich?

☐ weiblich

☐ männlich

I2. Wie alt bist du?

I3. Welche Schulform besuchst Du?

- ☐ Realschule Plus
- ☐ Gymnasium
- ☐ IGS

I4. Worüber hättest Du gerne mehr Informationen?

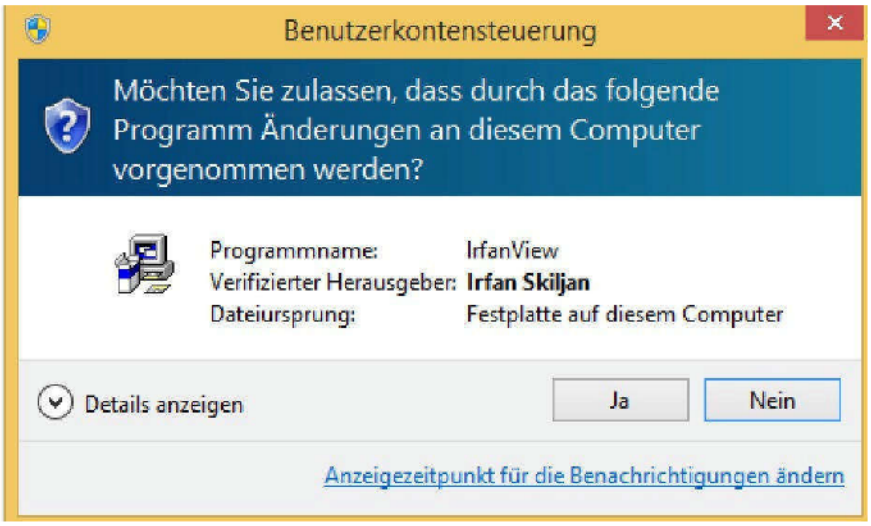
	Ja	Unsicher	Nein
… zum Schutz meiner Daten im Internet.	☐	☐	☐
… zur rechtlichen Situation in Bezug auf den Schutz meiner Daten.	☐	☐	☐
… zu technischen Möglichkeiten des Schutzes meiner Daten.	☐	☐	☐
… zu den Gefahren beim Surfen im Internet	☐	☐	☐

I5. Hier hast Du die Möglichkeit, wenn Du möchtest, weitere Wünsche und Anregungen bezüglich dieser Studie zum Thema Datenschutz zu nennen:

Vielen Dank für die Teilnahme an der Umfrage.

Mit den Ergebnisse und insbesondere mit Deiner Rückmeldung können wir den Fragebogen für die im Dezember stattfindende Gesamterhebung verbessern. An dieser Gesamterhebung wirst Du dann aber nicht mehr teilnehmen, da Dir dieser Fragebogen nun bekannt ist.

Bild zu G1: Benutzerkontensteuerung



ANHANG 4.6

Unterlagen für Schule, Studienteilnehmer und Erziehungsberechtigte

Die folgenden Seiten umfassen die Unterlagen, die an die Schulen per E-Mail versandt und an die Studienteilnehmer und die Erziehungsberechtigten ausgeteilt worden sind.

UNIVERSITÄT KOBLENZ · LANDAU

Fachbereich 4: Informatik
AG Fachdidaktik Informatik

Alexander Hug

Haus: Universitätsstraße 1; D-56070 Koblenz
Postfach: 201 602; D-56016 Koblenz

Sekretariat: +49-261-287-2665
Durchwahl: +49-261-287-2664
Telefax: +49-261-287-100-2664
E-Mail: hug@uni-koblenz.de
http://www.uni-koblenz.de/FB4

Alexander Hug ■ FB 4 ■ Uni Koblenz ■ Postfach 201 602 ■ D-56016 Koblenz

An die Schulleitungen
der Realschulen Plus
der Gymnasien
der Integrierten Gesamtschulen

in Rheinland-Pfalz

Koblenz, 27.11.2017

Studie zum Thema „Datenschutz und Jugendliche“

Sehr geehrte Damen und Herren,

in regelmäßigen Abständen können wir in den Medien lesen, dass Jugendliche eine schlecht ausgebildete Datenschutzkompetenz besitzen. Als sog. *Digital Natives* nutzen sie Soziale Medien und erschaffen in der digitalen Welt ihr zweites Ich, jedoch sind sie leider nur bedingt in der Lage, sich und ihre Daten in dieser zweiten Welt auch richtig zu schützen.

Im Rahmen eines Forschungsprojektes an der Universität Koblenz-Landau untersuche ich das Datenschutzverhalten von Jugendlichen. Ausgehend von einem von mir entwickelten Datenschutzkompetenzmodell möchte ich im Rahmen einer landesweiten Studie die Datenschutzkompetenz Jugendlicher der **Klassenstufen 5 bis 7** allgemeinbildender Schulen untersuchen. Die Studie habe ich bei der ADD Trier angezeigt und die Durchführung ist mir genehmigt worden.

Ich möchte Sie hiermit bitten, mich durch Teilnahme Ihrer Schule bei der Durchführung dieser Studie zu unterstützen. Durch die Ergebnisse sollen die Schwachpunkte im Bereich der Datenschutzkompetenz aufgedeckt werden, sodass in einem nachfolgenden Schritt Handlungsempfehlungen für die Schule und den Unterricht daraus erwachsen, um die Jugendlichen besser auf die digitale Welt vorzubereiten. Diese Empfehlungen werde ich Ihnen dann sehr gerne zur Verfügung stellen.

Bei der Studie handelt es sich um eine Online-Befragung für die o. g. Klassenstufen, die je nach Alter und Erfahrung der Schülerinnen und Schüler zwischen 20 bis 30 Minuten Zeit in Anspruch nehmen wird, sodass die Erhebung innerhalb einer Unterrichtsstunde durchgeführt werden kann. Die Beantwortung der Fragen kann am PC, einem Tablett oder auch einem Smartphone erfolgen, sodass es keiner Vorbereitungen o. ä. für die Durchführung bedarf.

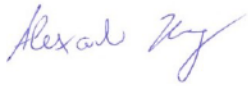
Allerdings müssen die Erziehungsberechtigten vorab eine Einverständniserklärung abgeben, die aus Datenschutzgründen auch in der Schule verbleibt. Im Vorfeld wurde durch die ADD geprüft, dass keine persönlichen Daten abgefragt werden, die nach der Erhebung Rückschlüsse auf eine Schülerin oder einen Schüler zulassen.

Für die Durchführung der Studie ist der Zeitraum vom 04.12.17 bis 26.01.18 vorgesehen, sodass mit den Ergebnissen im Frühjahr 2018 zu rechnen ist. Diese werden der ADD zur Verfügung gestellt und können bei mir abgefragt werden, sofern die teilnehmende Schule dies wünscht.

Weitere Informationen entnehmen Sie bitte dem beigefügten Leitfaden und den Anlagen.

Abschließend darf ich Sie freundlich um Ihre Unterstützung bitten und stehe bei weiteren Rückfragen gerne zur Verfügung

Mit freundlichen Grüßen



Leitfaden zur Durchführung der Studie „Jugendliche und Datenschutz“

Die folgende Zusammenstellung soll es Ihnen als Schulleiterin bzw. als Schulleiter (oder von Ihnen beauftragten Person) die Teilnahme an der Studie insbesondere aus organisatorischer Sicht erleichtern:

1) Überlegen Sie sich bitte, welche Klassen Ihrer Schule der Jahrgangsstufen 5 bis 7 an der Studie teilnehmen sollen. Je größer die Teilnehmerzahl an Schülerinnen und Schülern sein wird, desto größer ist die Aussagekraft der erhobenen Daten. Daher wäre es von Vorteil, wenn so vielen Jugendlichen wie möglich aus Ihrer Schule die Chance der Teilnahme eröffnet wird. Voraussetzungen für die Teilnahme sind,
   (a) dass es eine Lehrkraft in der jeweiligen Klasse gibt, die sich bereit erklärt hat, die Klasse zu beaufsichtigen (Fachkenntnisse werden von der Lehrkraft nicht benötigt, da die Schülerinnen und Schüler eigenständig den Erhebungsbogen ausfüllen sollen, daher bieten sich Klassenleiter- oder Vertretungsstunden an),
   (b) dass ein Computerraum zur Verfügung steht, sofern nicht mit eigenen Smartphones gearbeitet wird (außer einem Internetzugang mit Browser wird nichts an den Rechnern benötigt) und
   (c) dass die entsprechenden Einverständniserklärungen vorliegen (s. Punkt 3).
2) Bitte füllen Sie das Formular *Einverständniserklärung der Schule zur Teilnahme an der Studie „Datenschutz und Jugendliche“ der Universität Koblenz-Landau* aus und senden Sie es unterschrieben zurück. Dies kann als eingescannter Dokumentanhang einer E-Mail oder als Fax oder als Brief erfolgen. Die Kontaktdaten finden Sie u. a. in der Fußnote des Formulars.
3) Bitte teilen Sie die **drei** Dokumente:
   Informationsschreiben für die Teilnehmerinnen und Teilnehmer an der Studie zum Thema „Datenschutz und Jugendliche“,
   Informationsschreiben für die Sorgeberechtigten der Teilnehmerinnen und Teilnehmer an Studie zum Thema „Datenschutz und Jugendliche“ und
   Einverständniserklärung zur Teilnahme an der Studie „Datenschutz und Jugendliche“ der Universität Koblenz-Landau
   an die Schülerinnen und Schüler der teilnehmenden Klassen einige Tage vor der Studiendurchführung aus. Die zurückgegebenen Einverständniserklärungen der Erziehungsberechtigten sammeln Sie (aus Datenschutzgründen) bitte an Ihrer Schule.
4) Da die Schülerinnen und Schüler aufgrund der Unterlagen informiert sind, muss die beaufsichtigenden Lehrkraft nichts weiter tun, als den Jugendlichen die URL mitzuteilen (s. Punkt 5). In Einzelarbeit wird der Fragebogen beantwortet, was je nach Alter und Vorkenntnissen 20 bis 30 Minuten dauern wird.
5) Die Studie ist unter der URL http://uni-ko-ld.de/kv ab dem 04.12.2017 erreichbar und bis zum 26.01.18 freigeschaltet. Es findet eine Weiterleitung von dieser Adresse auf den Server von LimeSurvey statt, der von der Universität in Landau gehostet wird.

Sollten Sie bei der Durchführung auf technische Probleme stoßen, was leider nicht ganz ausgeschlossen werden kann, dann teilen Sie mir dies bitte umgehend mit, damit wir an der Problemlösung arbeiten können.

Für Ihre Mitarbeit danke ich Ihnen.

Alexander Hug, Universität Koblenz-Landau, FB Informatik, AG Didaktik der Informatik
Universitätsstraße 1, 56070 Koblenz, Tel. 0261/287-2664, Fax 0261/287-1002664, E-Mail hug@uni-koblenz.de

Universität Koblenz-Landau
Fachbereich Informatik
Alexander Hug

UNIVERSITÄT KOBLENZ · LANDAU

Informationsschreiben für die Teilnehmerinnen und Teilnehmer an der Studie zum Thema „Datenschutz und Jugendliche“

Liebe Schülerinnen und Schüler,

wir sind eine Forschungsgruppe der Universität Koblenz-Landau am Standort Koblenz und beschäftigen uns im Rahmen eines großen Projektes mit der Frage, wie wir Jugendliche besser davor bewahren können, damit so große Unternehmen wie Facebook® oder Google® nicht Eure Daten ausspähen und für ihre Zwecke nutzen. Dafür ist es für uns immens wichtig, dass wir auch wissen, wie es um Eure Kompetenz im Umgang mit Datenschutz steht. Dazu haben wir einen Fragenkatalog entwickelt, den Ihr bitte online ausfüllt. Dies wird nicht länger als 30 Minuten Eurer Zeit in Anspruch nehmen.

Eure Teilnahme an dieser Befragung ist vollkommen freiwillig und steht in keinem Zusammenhang mit irgendeinem Eurer Schulfächer. Auch wenn Ihr Euch gegen eine Teilnahme entscheidet oder während der Beantwortung des Fragekatalogs die Teilnahme beenden möchtet, so entstehen Euch keine Nachteile dadurch.

Wir fragen zum Ende des Fragebogens nur noch Euer Geschlecht und Euer Alter ab, sodass keine personenbezogenen Daten entstehen, die uns Rückschlüsse zu Einer bzw. zu Einem von Euch erlauben. Daher bitten wir Euch – im Fall einer Teilnahme – auch um die wahrheitsgemäße Beantwortung der Fragen, denn sonst ist die Erhebung für uns wertlos.

Natürlich hoffen wir auf Eure Teilnahme und sagen an dieser Stelle schon einmal ein riesiges „Dankeschön“. Solltet Ihr noch weitere Fragen an uns haben, dann findet Ihr unsere Kontaktdaten in der Fußzeile dieses Schreibens.

Viele Grüße

für das Team der Forschungsgruppe

Alexander Hug, Universität Koblenz-Landau, FB Informatik, AG Didaktik der Informatik
Universitätsstraße 1, 56070 Koblenz, Tel. 0261/287-2664, Fax 0261/287-1002664, E-Mail hug@uni-koblenz.de

Universität Koblenz-Landau
Fachbereich Informatik
Alexander Hug

Informationsschreiben für die Sorgeberechtigten der Teilnehmerinnen und Teilnehmer an der Studie zum Thema „Datenschutz und Jugendliche“

Sehr geehrte Damen und Herren,
liebe Sorgeberechtigte,

die Forschungsgruppe „Didaktik der Informatik“ der Universität Koblenz-Landau beschäftigt sich im Rahmen eines großen Projektes mit dem Thema „Datenschutz und Unterricht“. Ziel ist es, Unterrichtsempfehlungen zur Förderung der Datenschutzkompetenz bei Jugendlichen zu entwickeln.
Dazu planen wir eine Rheinland-Pfalz-weite Online-Umfrage unter möglichst vielen Schülerinnen und Schüler aller allgemeinbildenden Schulen der Klassenstufe 5 bis 7.

Erste Informationen zu der Erhebung können Sie dem Schreiben an die Schülerinnen und Schüler entnehmen. Mit diesem Schreiben möchten wir sie über Folgendes informieren:

1. Die Teilnahme an dieser Befragung ist für die Schülerinnen und Schüler vollkommen freiwillig und steht in keinem Zusammenhang mit irgendeinem der Schulfächer. Auch wenn Sie sich gegen eine Teilnahme Ihrer Tochter oder Ihres Sohnes entscheiden oder sie bzw. er während der Beantwortung des Fragekatalogs die Teilnahme beenden möchtet, so erwachsen den Kindern keine Nachteile dadurch.
2. Zum Ende des Fragebogens werden das Geschlecht und das Alter abgefragt, sodass keine personenbezogenen Daten entstehen, die uns Rückschlüsse zu einer konkreten Schülerin oder zu einem konkreten Schüler erlauben.
3. Die erhobenen Daten werden auf einem Server der Universität (und damit in Deutschland) während des Projektzeitraums gespeichert und danach vollständig gelöscht (vermutlich zum 31.12.2018).
4. Die Ergebnisse der Studie werden auf wissenschaftlichen Konferenzen vorgestellt und in Fachpublikationen veröffentlicht. Auf Wunsch können Sie über die Schulleitung Ihrer Schule die Ergebnisse der Studie zur Kenntnis nehmen.
5. Für weitere Fragen stehe ich zur Verfügung. Meine Kontaktdaten können Sie der Fußzeile entnehmen.

Ich darf Sie bitten, die angehängte Einverständniserklärung, die in der Schule verbleiben und nicht der Projektgruppe zur Verfügung gestellt wird, zu unterschreiben. Je mehr Schülerinnen und Schüler daran teilnehmen, desto aussagekräftiger sind die Daten. Ihre Einverständniserklärung können Sie vor Beginn der Datenerhebung ohne Angabe von Gründen noch widerrufen, ohne dass dadurch Nachteile für Ihr Kind entstehen. Ein späterer Widerruf ist nicht mehr möglich, da wir aus den gesammelten Daten nicht den einen Datensatz Ihrer Tochter oder Ihres Sohnes herausfiltern können.

In der Hoffnung, dass Sie Ihr Einverständnis geben, darf ich mich bei Ihnen bedanken und verbleibe mit freundlichen Grüßen

Alexander Hug, Universität Koblenz-Landau, FB Informatik, AG Didaktik der Informatik
Universitätsstraße 1, 56070 Koblenz, Tel. 0261/287-2664, Fax 0261/287-1002664, E-Mail hug@uni-koblenz.de

Anlage:

Vor- und Nachname des Sorgeberechtigten/der Sorgeberechtigten

Anschrift

Einverständniserklärung zur Teilnahme an der Studie „Datenschutz und Jugendliche“ der Universität Koblenz-Landau

Hiermit erkläre ich/erklären wir, dass unsere Tochter bzw. unser Sohn _____

_____ Klasse _____, an der o. g. Studie teilnehmen darf.

Das Informationsblatt, welches insbesondere Auskunft über das Ziel der Studie, die Freiwilligkeit der Teilnahme, dem Ausschluss einer Benachteiligung bei Nicht-Teilnahme oder dem Widerruf der Teilnahme, die Aufbewahrung und späteren Vernichtung der Daten und den Kontaktdaten des Vertreters der Universität Koblenz-Landau beinhaltet, habe ich/haben wir erhalten.

Diese Einverständniserklärung verbleibt in der Schule.

Ort, Datum

Unterschrift(en)

Alexander Hug, Universität Koblenz-Landau, FB Informatik, AG Didaktik der Informatik
Universitätsstraße 1, 56070 Koblenz, Tel. 0261/287-2664, Fax 0261/287-1002664, E-Mail hug@uni-koblenz.de

Stempel der Schule mit Kontaktdaten

Einverständniserklärung der Schule zur Teilnahme an der Studie „Datenschutz und Jugendliche“ der Universität Koblenz-Landau

Hiermit wird erklärt, dass unsere o. g. Schule an der Studie „Datenschutz und Jugendliche“

- o teilnehmen
- o nicht teilnehmen

wird.

Das Informationsblatt an die Schülerinnen und Schüler und an die Eltern, welches insbesondere Auskunft über das Ziel der Studie, die Freiwilligkeit der Teilnahme, dem Ausschluss einer Benachteiligung bei Nicht-Teilnahme oder dem Widerruf der Teilnahme, die Aufbewahrung und späteren Vernichtung der Daten und den Kontaktdaten des Vertreters der Universität Koblenz-Landau beinhaltet, haben wir erhalten.

Ort, Datum

Unterschrift des Schulleiters/der Schulleiterin

Alexander Hug, Universität Koblenz-Landau, FB Informatik, AG Didaktik der Informatik
Universitätsstraße 1, 56070 Koblenz, Tel. 0261/287-2664, Fax 0261/287-1002664, E-Mail hug@uni-koblenz.de

ANHANG 4.7

Fragebogen der finalen Erhebung

Die folgenden Seiten umfassen den aus Lime Survey exportierten Fragebogen der Studie vom Dezember 2017 und Januar 2018.

Speziell für diesen Ausdruck sind hinter der jeweiligen Frage bzw. dem jeweiligen Item in rot abgekürzt die jeweilige Dimension des Datenschutzkompetenzmodells notiert, die sich aufgrund der Auswertung der Q-Sortierung (vgl. Anhang A4.4) ergibt, und in blau die Nummer der überprüften Datenschutzkompetenz angeben (vgl. 3.5, Tab. 3.8).

Vor Beginn bitte diesen Hinweis sorgfältig lesen!

Herzlich Willkommen,

zu der Umfrage zum Thema *Datenschutz und Jugendliche*.

Auf den folgenden neun Seiten sind Fragen notiert, die Du durch einfaches Ankreuzen beantworten kannst. Bitte lies die Aufgabe bzw. Fragestellung aufmerksam und sorgfältig durch (wie bei einer Klassenarbeit), bevor Du mit dem Antworten beginnst. Deine Antworten müssen frei und vor allem ehrlich gegeben werden, da diese sonst für die Auswertung nutzlos sind. Bei einigen Fragen wirst Du um eine Einschätzung gebeten. Die Skala reicht dabei von 1 bis 5 (z. B. 1 = *"trifft voll und ganz zu"* bis 5 = *"trifft überhaupt nicht zu"*). Solltest Du Dir mit Deiner Antwort unsicher sein, dann wähle in diesem Fall das Feld in der Mitte aus.

Die Umfrage ist anonym, das heißt, dass Deine Antworten nicht auf Deine Person zurückverfolgt werden können. Weder Deine Eltern noch Deine Lehrer können Deine Antworten einsehen, nur das Gesamtergebnis aller an der Studie teilnehmenden Schülerinnen und Schüler wird auf Wunsch an die Schule weitergegeben.

Nun kannst Du starten, indem Du unten rechts auf "Weiter" klickst.

Teil A: Soziale Netzwerke

A1. Welche Sozialen Netzwerke nutzt Du?

- ☐ Facebook
- ☐ Google+
- ☐ Twitter
- ☐ Youtube
- ☐ Tumblr
- ☐ Instagram
- ☐ MySpace
- ☐ Snapchat
- ☐ Pinterest

Steam ☐

Twitch ☐

Ich nutze kein soziales Netzwerk ☐

A2. Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen?

RK 6 + 8

	Sehr sensibel, sollten nicht veröffentlicht werden				Unsensibel, kann man bedenkenlos veröffentlichen
Vorname	☐	☐	☐	☐	☐
Nachname	☐	☐	☐	☐	☐
Nickname / Spitzname	☐	☐	☐	☐	☐
Geburtsdatum	☐	☐	☐	☐	☐
Adresse mit Straße + Hausnummer, Wohnort	☐	☐	☐	☐	☐
Telefon- / Handynummer	☐	☐	☐	☐	☐
E-Mail-Adresse	☐	☐	☐	☐	☐
Fotos	☐	☐	☐	☐	☐
Kontakte	☐	☐	☐	☐	☐
Lieblingsfilme / -musik / -bücher / -serien	☐	☐	☐	☐	☐
Interessen / Hobbies	☐	☐	☐	☐	☐
Lieblingsorte	☐	☐	☐	☐	☐
Eigene Erlebnisse	☐	☐	☐	☐	☐
Eigene Gedanken / Gefühle / Sorgen	☐	☐	☐	☐	☐
Religion	☐	☐	☐	☐	☐

A3. Welches Deiner Sozialen Netzwerke nutzt Du am MEISTEN?[1]

- Facebook ☐[2]
- Google+ ☐
- Twitter ☐
- Youtube ☐
- Tumblr ☐
- Instagram ☐
- MySpace ☐
- Snapchat ☐
- Pinterest ☐
- Steam ☐
- Twitch ☐
- Ich nutze kein soziales Netzwerk ☐

Teil B: Privatsphäre Soziale Netzwerke

B1. Hast Du die Privatsphäreneinstellungen in {INSERTANS:242694X25032X344328}[3] geändert? Wenn ja, was?

UK 7 + 8

- Ich habe nichts geändert, weil ich den Einstellungen des Anbieters vertraue ☐
- Sichtbarkeit meines Profils innerhalb {INSERTANS:242694X25032X344328}[3] ☐
- Sichtbarkeit meines Profils außerhalb {INSERTANS:242694X25032X344328}[3] ☐
- Sichtbarkeit meiner Posts ☐
- Wer auf meinen Seiten posten darf ☐
- Wer mich kontaktieren darf ☐
- Für wen ich zu finden bin ☐

B2. Was würdest Du in den Privatsphäreneinstellungen ändern, wenn Du ein Soziales Netzwerk nutzen würdest?

UK 7 + 8

erscheint nur wenn in A3 kein Soziales Netzwerk ausgewählt wurde

- Ich würde nichts ändern, weil ich den Einstellungen des Anbieters vertraue ☐
- Sichtbarkeit meines Profils innerhalb des Sozialen Netzwerks ☐
- Sichtbarkeit meines Profils außerhalb des Sozialen Netzwerks ☐
- Sichtbarkeit meiner Posts ☐
- Wer auf meinen Seiten posten darf ☐

[1] Die Frage A3 wurde genutzt, um Fragen zu personalisieren: So wird im Folgenden {INSERTANS:211017X24370X336284} durch das Soziale Netzwerk, welches hier gewählt wurde, ersetzt.
[2] Die Linien zeigen an, dass nur eine Antwortoption auswählbar ist.
[3] {INSERTANS:...} wurde ersetzt durch das Soziale Netzwerk aus der Frage A3.

Wer mich kontaktieren darf ☐

Für wen ich zu finden bin ☐

B3. Jetzt geht es um Informationen, die andere über Dich im Internet und in {INSERTANS:242694X25032X344328}[3] finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu?

	trifft voll und ganz zu				trifft überhaupt nicht zu	
Ich achte darauf, welche Informationen ich selbst ins Internet oder in {INSERTANS:242694X25032X344328}[3] stelle.	☐	☐	☐	☐	☐	HK 16 + 11
Wenn ich im Internet oder in {INSERTANS:242694X25032X344328}[3] etwas veröffentliche, denke ich nicht darüber nach, wer es später sehen kann.	☐	☐	☐	☐	☐	7
Es ist mir wichtig, selbst bestimmen zu können, wer durch das Internet oder durch {INSERTANS:242694X25032X344328}[3] etwas über mich erfährt und wer nicht.	☐	☐	☐	☐	☐	UK 7

B4. Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu?

erscheint nur wenn in A3 kein Soziales Netzwerk ausgewählt wurde

	trifft voll und ganz zu				trifft überhaupt nicht zu	
Ich achte darauf, welche Informationen ich selbst ins Internet stelle.	☐	☐	☐	☐	☐	HK 16 + 11
Wenn ich im Internet etwas veröffentliche, denke ich nicht darüber nach, wer es später sehen kann.	☐	☐	☐	☐	☐	7
Es ist mir wichtig, selbst bestimmen zu können, wer durch das Internet etwas über mich erfährt und wer nicht.	☐	☐	☐	☐	☐	UK 7

Teil C: Wissensfragen

C1.

Was versteht man unter einem "Trojaner"? W 1

Ein Trojaner ist ein Computerprogramm, das den Rechner vor Viren und anderen Schadprogrammen schützt. ☐

Ein Trojaner ist ein Computerprogramm, das als Computervirus in den 90ern Schaden anrichtete, heute aber nicht mehr existiert. ☐

Ein Trojaner ist ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber eine andere Funktion erfüllt. ☐

Ein Trojaner ist ein Computerprogramm, das nur zum Spaß entwickelt wurde und keine besondere Funktion hat. ☐

Weiß ich nicht. ☐

C2. Was ist ein "Cookie"? W 1

Ein Cookie ist ein Computer-Virus, den man sich beim Besuch einer Internetseite einfangen kann. ☐

Ein Cookie ist ein Zusatzprogramm für den Browser, das sicheres Surfen ermöglicht. ☐

Ein Cookie ist ein Programm, mit dem man die Datenspeicherung von Web-Anbietern unterbinden kann. ☐

Ein Cookie ist eine Datei, die es Internetseiten ermöglicht, den Nutzer beim erneuten Besuch wiederzuerkennen. ☐

[3] {INSERTANS:...} wurde ersetzt durch das Soziale Netzwerk aus der Frage A3.

Weiß ich nicht. ☐

C3. Was ist eine "Firewall"? W 1

Eine Firewall ist ein Sicherungssystem, das den Computer vor unerwünschten Netzangriffen schützen soll. ☐

Eine Firewall ist ein veraltetes Schutzprogramm gegen Computer-Viren. ☐

Eine Firewall ist ein Zusatzprogramm für den Browser, das sicheres Surfen ermöglicht. ☐

Eine Firewall ist eine neue technische Entwicklung, die verhindert, dass Daten bei einem Kurzschluss verloren gehen. ☐

Weiß ich nicht. ☐

C4. Was verbirgt sich hinter dem Begriff "Browserverlauf"? W 1

Im Browserverlauf werden die Adressen der besuchten Internetseiten gespeichert. ☐

Im Browserverlauf werden Cookies von besuchten Websites abgelegt. ☐

Im Browserverlauf werden potenziell infizierte Internetseiten separat abgelegt. ☐

Im Browserverlauf werden je nach Browsertyp unterschiedliche Informationen über den Nutzer gespeichert. ☐

Weiß ich nicht. ☐

C5. Welche der folgenden URLs (Internetseiten-Adressen) garantiert einen mit hoher Wahrscheinlichkeit datenabhörsicheren Zugriff auf die Internetseite der Sparkasse? W 1

Antwortmöglichkeiten bitte sorgfältig lesen!

http://www.sparkasse.de ☐

https://www.sparkasse.de ☐

http://www.sicher.sparkasse.de ☐

http://banking.sparkasse.de ☐

Weiß nicht ☐

Teil D: Messenger und Tools

D1. Nutzt Du einen Messenger (wie z.B. WhatsApp)?

Ja ☐

Nein ☐

D2. Welche Browser kennst Du, um durch das Internet zu surfen?

Mozilla Firefox ☐

Internet Explorer / Microsoft Edge ☐

Google Chrome ☐

Apple Safari ☐
Opera ☐
Keinen ☐
Sonstiges ☐

Sonstiges

D3. Welche Browser nutzt Du, um durch das Internet zu surfen?

Mozilla Firefox ☐
Internet Explorer / Microsoft Edge ☐
Google Chrome ☐
Apple Safari ☐
Opera ☐
Keinen ☐
Sonstiges ☐

Sonstiges

D4. Welche Browsertools kennst du?

Ghostery ☐
Adblock Plus ☐
Bug me not ☐
Firebug ☐
Flagfox ☐
Self-Destructing-Cookies ☐
NoScript ☐
Keine ☐
Sonstiges ☐

Sonstiges

D5. Welche Browsertools nutzt du?

Ghostery ☐

Adblock Plus ☐
Bug me not ☐
Firebug ☐
Flagfox ☐
Self-Destructing-Cookies ☐
NoScript ☐
Keine ☐
Keine[4] ☐
Sonstiges ☐

Sonstiges

D6. Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers?

	sehr wichtig				unwichtig	
Die Verschlüsselung bei der Übermittlung der Daten	☐	☐	☐	☐	☐	RK 8
Die Identifikationsmöglichkeit des Gesprächspartners, das heißt zu wissen, wer mein Gegenüber ist	☐	☐	☐	☐	☐	RK 8
Die Anzahl der Nutzer im Freundes- und Familienkreis	☐	☐	☐	☐	☐	
Die Geschwindigkeit der Übermittlung von Nachrichten und Daten	☐	☐	☐	☐	☐	

Teil E: Wissensfragen 2

E1. Sind folgende Aussagen wahr oder falsch? W

	wahr	falsch	weiß nicht	
Wenn auf einer Internetseite eine Datenschutzerklärung veröffentlicht wurde, bedeutet das, dass der Anbieter der Internetseite Deine Adresse und Dein Kaufverhalten nicht der Regierung mitteilen darf.	☐	☐	☐	2
Man muss Deine Erlaubnis einholen, wenn man ein Foto oder Video von Dir hochlädt, auf dem Du klar zu erkennen bist.	☐	☐	☐	3
Wenn auf einer Internetseite eine Datenschutzerklärung veröffentlicht wurde, bedeutet das, dass der Anbieter der Internetseite keine Informationen über Dich mit anderen Firmen teilen darf, bis Du Deine Genehmigung gegeben hast.	☐	☐	☐	2
Wenn eine Firma Dein Internetverhalten über mehrere Seiten verfolgen möchte, muss sie zuerst Dein Einverständnis einholen.	☐	☐	☐	3
Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.	☐	☐	☐	3

[4] In LimeSurvey wurde die Frage D5. nur mit Antwortmöglichkeiten, die in der Frage D4. ausgewählt wurden angezeigt. Wurde jedoch in D4. "Keine" ausgewählt, erschien die Frage D5. erst garnicht und somit auch keine doppelte Antwortmöglichkeit "Keine".

E2. Sind folgende Aussagen wahr oder falsch? W

	wahr	falsch	weiß nicht	
Die Geheimdienste (wie zum Beispiel der amerikanische Geheimdienst NSA [National Security Agency]) greifen nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.	☐	☐	☐	4
Betreiber Sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar NICHT nutzen.	☐	☐	☐	4
Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.	☐	☐	☐	5
Durch das Surfen im „Private Browsing"-Modus ist man anonym im Internet, da keine Browserinformationen gespeichert werden.	☐	☐	☐	5
Online-Shops (z.B. Amazon) werten das Nutzungsverhalten von Kunden aus und erstellen auf dieser Basis Kaufempfehlungen oder entsprechend zugeschnittene Werbung.	☐	☐	☐	4

Teil F: Risikoeinschätzung

F1. Was sind für dich Risiken im Internet? RK

	sehr hohes Risiko				sehr geringes Risiko	
Die unerwünschte Weitergabe von persönlichen Daten an Dritte	☐	☐	☐	☐	☐	6
Das Ausspionieren meiner persönlichen Daten	☐	☐	☐	☐	☐	6
Das Empfangen von Spam-Mails	☐	☐	☐	☐	☐	9
Die Beleidigungen und Belästigungen im Internet	☐	☐	☐	☐	☐	9
Das Versenden unerwünschter E-Mails in meinem Namen	☐	☐	☐	☐	☐	10
Andere wissen, was ich mache, oder kennen meinen Aufenthaltsort	☐	☐	☐	☐	☐	11
Die Veröffentlichung peinlicher/intimer Chats/Fotos/…	☐	☐	☐	☐	☐	6

F2. Jetzt geht es um DEINE Einschätzungen zu Risiken im Umgang mit Computern und Internet. RK

	sehr hohes Risiko				sehr geringes Risiko	
Wie hoch ist Deiner Ansicht nach das Risiko, dass der Computer durch das Öffnen von Mailanhängen mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐	☐	12
Wie hoch ist Deiner Ansicht nach das Risiko, dass man es nicht merkt, wenn der Rechner mit einem Computervirus infiziert ist?	☐	☐	☐	☐	☐	13
Wie hoch ist Deiner Ansicht nach das Risiko, dass ein Computervirus von der Antivirensoftware nicht erkannt wird?	☐	☐	☐	☐	☐	13

	sehr hohes Risiko				sehr geringes Risiko	
Wie hoch ist Deiner Ansicht nach das Risiko, dass der Computer durch den Download von Dateien über Tauschbörsen (z.B. eMule, BitTorrent) mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐	☐	12
Wie hoch ist Deiner Ansicht nach das Risiko, dass der Computer beim Surfen im Internet (ohne Dateien herunterzuladen) mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐	☐	12

Teil G: Maßnahmen Datenschutz

G1. Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? ANK 5

	Ja	Nein	Weiß nicht
Ich nutze Pop-Up-Blocker oder Adblocker.	☐	☐	☐
Ich nutze eine Firewall.	☐	☐	☐
Ich nutze eine Verschlüsselungssoftware beim E-Mailen und Chatten.	☐	☐	☐
Ich aktualisiere regelmäßig meine Anti-Viren-Software.	☐	☐	☐
Ich nutze Anonymisierungstools. (Ein Anonymisierungstool ist eine Software, die Daten beim Surfen so verändert, dass keine Rückschlüsse auf Dich als Besucher der Internetseiten gezogen werden können.)	☐	☐	☐
Ich nutze Anti-Tracking-Software. (Anti-Tracking-Software ist eine Software, die ein Nachverfolgen des Besuchs von Internetseiten verhindert.)	☐	☐	☐

G2. Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten?

	Ja	Nein	Weiß nicht	
Ich nutze verschiedene Passwörter.	☐	☐	☐	HK 5
Ich nutze sichere Geräte mit persönlichem Passwort.	☐	☐	☐	HK 5
Unter der Annahme, dass ich ein Soziales Netzwerk nutze, aktualisiere ich persönliche Sicherheitseinstellungen in Sozialen Netzwerken gegenüber Grundeinstellungen.	☐	☐	☐	HK 5
Ich nutze nur Seiten, bei denen ich weiß, dass sie sicher sind.	☐	☐	☐	HK 5
Ich habe aktive Inhalte im Browser (z. B. Javascript, ActiveX) deaktiviert.	☐	☐	☐	UK 5 + 13

Teil H: Eigenes Verhalten

H1. Wie sehr treffen die folgenden Aussagen auf Dich zu?

	trifft voll und ganz zu				trifft überhaupt nicht zu		
Ich suche immer erst nach Möglichkeiten, Musik im Internet kostenlos zu bekommen, bevor ich daran denke, sie zu kaufen.	☐	☐	☐	☐	☐	ANK	17
Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.	☐	☐	☐	☐	☐	HK	5
Ich sichere in regelmäßigen Abständen die wichtigsten Daten auf einem CD/DVD-Rohling oder einer externen Festplatte.	☐	☐	☐	☐	☐	HK	5
Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.	☐	☐	☐	☐	☐	UK	9 + 14
Wenn ich mir die Originalversion einer Software nicht leisten kann, suche ich nach kostenlosen und legalen Freeware-Alternativen.	☐	☐	☐	☐	☐	ANK	17
Ich denke nicht lange darüber nach, einen E-Mail-Anhang zu öffnen – ich tue es einfach.	☐	☐	☐	☐	☐	RK	14
Wenn ich per E-Mail oder im Chat einen Link zugesendet bekomme, klicke ich ihn meistens an, auch wenn ich mir nicht sicher bin, auf welcher Seite ich lande.	☐	☐	☐	☐	☐	RK	14
Ich achte nicht darauf, von welchen Seiten die Dateien stammen, die ich herunterlade.	☐	☐	☐	☐	☐	RK	14
E-Mails, bei denen ich die Vermutung habe, dass es sich um unerwünschte Nachrichten (Spam) handelt, lösche ich sofort.	☐	☐	☐	☐	☐	HK	5
Ich ändere in regelmäßigen Abständen alle meine Passwörter.	☐	☐	☐	☐	☐	HK	15
Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.	☐	☐	☐	☐	☐	HK	15
Aufgrund des hohen Sicherheitsrisikos im Internet schränke ich meine Online-Zeit ein.	☐	☐	☐	☐	☐	HK	16

Teil I: Persönliche Informationen

I1. Bist Du männlich oder weiblich?

☐ weiblich

☐ männlich

I2. Wie alt bist Du?

☐☐

I3. Welche Schulform besuchst Du?

☐ Realschule Plus

☐ Gymnasium

☐ IGS

I4. Worüber hättest Du gerne mehr Informationen?

	Ja	Unsicher	Nein
… zum Schutz meiner Daten im Internet.	☐	☐	☐
… zur rechtlichen Situation in Bezug auf den Schutz meiner Daten.	☐	☐	☐
… zu technischen Möglichkeiten des Schutzes meiner Daten.	☐	☐	☐
… zu den Gefahren beim Surfen im Internet	☐	☐	☐

I5. Hier hast Du die Möglichkeit, wenn Du möchtest, weitere Wünsche und Anregungen bezüglich dieser Studie zum Thema Datenschutz zu nennen:

Vielen Dank für die Teilnahme an der Umfrage.

Du kannst das Browserfenster nun schließen.

ANHANG 4.8

Codierung des finalen Fragebogens für die Auswertung

Die folgenden Seiten umfassen die Codierung des finalen Fragebogens. Innerhalb des Fragebogens sind die für die Auswertung notwendigen Informationen an den Items und Fragen eingetragen. Diesem Fragebogen folgt die Beschreibung des Berechnungswegs zur Bestimmung der Kompetenznote der deskriptiven Auswertung und die Beschreibung der Auswertung der bivariaten Analyse.

Vor Beginn bitte diesen Hinweis sorgfältig lesen!

Herzlich Willkommen,

zu der Umfrage zum Thema *Datenschutz und Jugendliche*.

Auf den folgenden neun Seiten sind Fragen notiert, die Du durch einfaches Ankreuzen beantworten kannst. Bitte lies die Aufgabe bzw. Fragestellung aufmerksam und sorgfältig durch (wie bei einer Klassenarbeit), bevor Du mit dem Antworten beginnst. Deine Antworten müssen frei und vor allem ehrlich gegeben werden, da diese sonst für die Auswertung nutzlos sind. Bei einigen Fragen wirst Du um eine Einschätzung gebeten. Die Skala reicht dabei von 1 bis 5 (z. B. 1 = *"trifft voll und ganz zu"* bis 5 = *"trifft überhaupt nicht zu"*). Solltest Du Dir mit Deiner Antwort unsicher sein, dann wähle in diesem Fall das Feld in der Mitte aus.

Die Umfrage ist anonym, das heißt, dass Deine Antworten nicht auf Deine Person zurückverfolgt werden können. Weder Deine Eltern noch Deine Lehrer können Deine Antworten einsehen, nur das Gesamtergebnis aller an der Studie teilnehmenden Schülerinnen und Schüler wird auf Wunsch an die Schule weitergegeben.

Nun kannst Du starten, indem Du unten rechts auf "Weiter" klickst.

Teil A: Soziale Netzwerke

A1. Welche Sozialen Netzwerke nutzt Du?

- ☐ Facebook
- ☐ Google+
- ☐ Twitter
- ☐ Youtube
- ☐ Tumblr
- ☐ Instagram
- ☐ MySpace
- ☐ Snapchat
- ☐ Pinterest

Steam ☐

Twitch ☐

Ich nutze kein soziales Netzwerk ☐

A2. Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? RK

	Sehr sensibel, sollten nicht veröffentlicht werden				Unsensibel, kann man bedenkenlos veröffentlichen
Vorname	☐	☐	X	☐	☐
Nachname	☐	X	☐	☐	☐
Nickname / Spitzname	☐	☐	☐	X	☐
Geburtsdatum	X	☐	☐	☐	☐
Adresse mit Straße + Hausnummer, Wohnort	X	☐	☐	☐	☐
Telefon- / Handynummer	X	☐	☐	☐	☐
E-Mail-Adresse	☐	☐	X	☐	☐
Fotos	☐	X	☐	☐	☐
Kontakte	X	☐	☐	☐	☐
Lieblingsfilme / -musik / -bücher / -serien	☐	☐	X	☐	☐
Interessen / Hobbies	☐	☐	☐	X	☐
Lieblingsorte	☐	☐	☐	X	☐
Eigene Erlebnisse	☐	X	☐	☐	☐
Eigene Gedanken / Gefühle / Sorgen	X	☐	☐	☐	☐
Religion	X	☐	☐	☐	☐

A3. Welches Deiner Sozialen Netzwerke nutzt Du am MEISTEN?[1]

- Facebook ☐[2]
- Google+ ☐
- Twitter ☐
- Youtube ☐
- Tumblr ☐
- Instagram ☐
- MySpace ☐
- Snapchat ☐
- Pinterest ☐
- Steam ☐
- Twitch ☐
- Ich nutze kein soziales Netzwerk ☐

Teil B: Privatsphäre Soziale Netzwerke

B1. Hast Du die Privatsphäreneinstellungen in {INSERTANS:242694X25032X344328}[3] geändert? Wenn ja, was?

UK

- Ich habe nichts geändert, weil ich den Einstellungen des Anbieters vertraue ☐ **0**
- Sichtbarkeit meines Profils innerhalb {INSERTANS:242694X25032X344328}[3] ☐
- Sichtbarkeit meines Profils außerhalb {INSERTANS:242694X25032X344328}[3] ☐
- Sichtbarkeit meiner Posts ☐
- Wer auf meinen Seiten posten darf ☐
- Wer mich kontaktieren darf ☐
- Für wen ich zu finden bin ☐

je nach Ankreuzverhalten werden 1 bis 4 Punkte vergeben

B2. Was würdest Du in den Privatsphäreneinstellungen ändern, wenn Du ein Soziales Netzwerk nutzen würdest?

UK

erscheint nur wenn in A3 kein Soziales Netzwerk ausgewählt wurde

- Ich würde nichts ändern, weil ich den Einstellungen des Anbieters vertraue ☐ **0**
- Sichtbarkeit meines Profils innerhalb des Sozialen Netzwerks ☐
- Sichtbarkeit meines Profils außerhalb des Sozialen Netzwerks ☐
- Sichtbarkeit meiner Posts ☐
- Wer auf meinen Seiten posten darf ☐

je nach Ankreuzverhalten werden 1 bis 4 Punkte vergeben

[1] Die Frage A3 wurde genutzt, um Fragen zu personalisieren: So wird im Folgenden {INSERTANS:211017X24370X336284} durch das Soziale Netzwerk, welches hier gewählt wurde, ersetzt.
[2] Die Linien zeigen an, dass nur eine Antwortoption auswählbar ist.
[3] {INSERTANS:...} wurde ersetzt durch das Soziale Netzwerk aus der Frage A3.

Wer mich kontaktieren darf ☐

Für wen ich zu finden bin ☐

B3. Jetzt geht es um Informationen, die andere über Dich im Internet und in {INSERTANS:242694X25032X344328}[3] finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu?

	trifft voll und ganz zu				trifft überhaupt nicht zu	
Ich achte darauf, welche Informationen ich selbst ins Internet oder in {INSERTANS:242694X25032X344328}[3] stelle.	4	3	2	1	0	HK
Wenn ich im Internet oder in {INSERTANS:242694X25032X344328}[3] etwas veröffentliche, denke ich nicht darüber nach, wer es später sehen kann.	0	1	2	3	4	UK
Es ist mir wichtig, selbst bestimmen zu können, wer durch das Internet oder durch {INSERTANS:242694X25032X344328}[3] etwas über mich erfährt und wer nicht.	4	3	2	1	0	UK

B4. Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu?

erscheint nur wenn in A3 kein Soziales Netzwerk ausgewählt wurde

	trifft voll und ganz zu				trifft überhaupt nicht zu	
Ich achte darauf, welche Informationen ich selbst ins Internet stelle.	4	3	2	1	0	HK
Wenn ich im Internet etwas veröffentliche, denke ich nicht darüber nach, wer es später sehen kann.	0	1	2	3	4	UK
Es ist mir wichtig, selbst bestimmen zu können, wer durch das Internet etwas über mich erfährt und wer nicht.	4	3	2	1	0	UK

Teil C: Wissensfragen

C1.

Was versteht man unter einem "Trojaner"? W

Ein Trojaner ist ein Computerprogramm, das den Rechner vor Viren und anderen Schadprogrammen schützt. ☐

Ein Trojaner ist ein Computerprogramm, das als Computervirus in den 90ern Schaden anrichtete, heute aber nicht mehr existiert. ☐

Ein Trojaner ist ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber eine andere Funktion erfüllt. ☒

Ein Trojaner ist ein Computerprogramm, das nur zum Spaß entwickelt wurde und keine besondere Funktion hat. ☐

Weiß ich nicht. ☐

C2. Was ist ein "Cookie"? W

Ein Cookie ist ein Computer-Virus, den man sich beim Besuch einer Internetseite einfangen kann. ☐

Ein Cookie ist ein Zusatzprogramm für den Browser, das sicheres Surfen ermöglicht. ☐

Ein Cookie ist ein Programm, mit dem man die Datenspeicherung von Web-Anbietern unterbinden kann. ☐

Ein Cookie ist eine Datei, die es Internetseiten ermöglicht, den Nutzer beim erneuten Besuch wiederzuerkennen. ☒

[3] {INSERTANS:...} wurde ersetzt durch das Soziale Netzwerk aus der Frage A3.

Weiß ich nicht. ☐

C3. Was ist eine "Firewall"? W

Eine Firewall ist ein Sicherungssystem, das den Computer vor unerwünschten Netzangriffen schützen soll. ☒

Eine Firewall ist ein veraltetes Schutzprogramm gegen Computer-Viren. ☐

Eine Firewall ist ein Zusatzprogramm für den Browser, das sicheres Surfen ermöglicht. ☐

Eine Firewall ist eine neue technische Entwicklung, die verhindert, dass Daten bei einem Kurzschluss verloren gehen. ☐

Weiß ich nicht. ☐

C4. Was verbirgt sich hinter dem Begriff "Browserverlauf"? W

Im Browserverlauf werden die Adressen der besuchten Internetseiten gespeichert. ☒

Im Browserverlauf werden Cookies von besuchten Websites abgelegt. ☐

Im Browserverlauf werden potenziell infizierte Internetseiten separat abgelegt. ☐

Im Browserverlauf werden je nach Browsertyp unterschiedliche Informationen über den Nutzer gespeichert. ☐

Weiß ich nicht. ☐

C5. Welche der folgenden URLs (Internetseiten-Adressen) garantiert einen mit hoher Wahrscheinlichkeit datenabhörsicheren Zugriff auf die Internetseite der Sparkasse? W

Antwortmöglichkeiten bitte sorgfältig lesen!

http://www.sparkasse.de ☐

https://www.sparkasse.de ☒

http://www.sicher.sparkasse.de ☐

http://banking.sparkasse.de ☐

Weiß nicht ☐

Teil D: Messenger und Tools

D1. Nutzt Du einen Messenger (wie z.B. WhatsApp)?

Ja ☐

Nein ☐

D2. Welche Browser kennst Du, um durch das Internet zu surfen?

Mozilla Firefox ☐

Internet Explorer / Microsoft Edge ☐

Google Chrome ☐

Apple Safari ☐
Opera ☐
Keinen ☐
Sonstiges ☐

Sonstiges

D3. Welche Browser nutzt Du, um durch das Internet zu surfen?

Mozilla Firefox ☐
Internet Explorer / Microsoft Edge ☐
Google Chrome ☐
Apple Safari ☐
Opera ☐
Keinen ☐
Sonstiges ☐

Sonstiges

D4. Welche Browsertools kennst du?

Ghostery ☐
Adblock Plus ☐
Bug me not ☐
Firebug ☐
Flagfox ☐
Self-Destructing-Cookies ☐
NoScript ☐
Keine ☐
Sonstiges ☐

Sonstiges

D5. Welche Browsertools nutzt du?

Ghostery ☐

Adblock Plus	☐
Bug me not	☐
Firebug	☐
Flagfox	☐
Self-Destructing-Cookies	☐
NoScript	☐
Keine	☐
Keine[4]	☐
Sonstiges	☐

Sonstiges

D6. Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers?

	sehr wichtig				unwichtig	
Die Verschlüsselung bei der Übermittlung der Daten	4	3	2	1	0	RK
Die Identifikationsmöglichkeit des Gesprächspartners, das heißt zu wissen, wer mein Gegenüber ist	4	3	2	1	0	RK
Die Anzahl der Nutzer im Freundes- und Familienkreis	☐	☐	☐	☐	☐	
Die Geschwindigkeit der Übermittlung von Nachrichten und Daten	☐	☐	☐	☐	☐	

Teil E: Wissensfragen 2

E1. Sind folgende Aussagen wahr oder falsch? W

	wahr	falsch	weiß nicht
Wenn auf einer Internetseite eine Datenschutzerklärung veröffentlicht wurde, bedeutet das, dass der Anbieter der Internetseite Deine Adresse und Dein Kaufverhalten nicht der Regierung mitteilen darf.	☐	X	☐
Man muss Deine Erlaubnis einholen, wenn man ein Foto oder Video von Dir hochlädt, auf dem Du klar zu erkennen bist.	X	☐	☐
Wenn auf einer Internetseite eine Datenschutzerklärung veröffentlicht wurde, bedeutet das, dass der Anbieter der Internetseite keine Informationen über Dich mit anderen Firmen teilen darf, bis Du Deine Genehmigung gegeben hast.	X	☐	☐
Wenn eine Firma Dein Internetverhalten über mehrere Seiten verfolgen möchte, muss sie zuerst Dein Einverständnis einholen.	X	☐	☐
Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.	X	☐	☐

[4] In LimeSurvey wurde die Frage D5. nur mit Antwortmöglichkeiten, die in der Frage D4. ausgewählt wurden, angezeigt. Wurde jedoch in D4. "Keine" ausgewählt, erschien die Frage D5. erst garnicht und somit auch keine doppelte Antwortmöglichkeit "Keine".

E2. Sind folgende Aussagen wahr oder falsch? W

	wahr	falsch	weiß nicht
Die Geheimdienste (wie zum Beispiel der amerikanische Geheimdienst NSA [National Security Agency]) greifen nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.		X	
Betreiber Sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar NICHT nutzen.	X		
Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.	X		
Durch das Surfen im „Private Browsing"-Modus ist man anonym im Internet, da keine Browserinformationen gespeichert werden.		X	
Online-Shops (z.B. Amazon) werten das Nutzungsverhalten von Kunden aus und erstellen auf dieser Basis Kaufempfehlungen oder entsprechend zugeschnittene Werbung.	X		

Teil F: Risikoeinschätzung

F1. Was sind für dich Risiken im Internet? RK

	sehr hohes Risiko				sehr geringes Risiko
Die unerwünschte Weitergabe von persönlichen Daten an Dritte	X				
Das Ausspionieren meiner persönlichen Daten	X				
Das Empfangen von Spam-Mails			X		
Die Beleidigungen und Belästigungen im Internet	X				
Das Versenden unerwünschter E-Mails in meinem Namen		X			
Andere wissen, was ich mache, oder kennen meinen Aufenthaltsort	X				
Die Veröffentlichung peinlicher/intimer Chats/Fotos/…	X				

F2. Jetzt geht es um DEINE Einschätzungen zu Risiken im Umgang mit Computern und Internet. RK

	sehr hohes Risiko				sehr geringes Risiko
Wie hoch ist Deiner Ansicht nach das Risiko, dass der Computer durch das Öffnen von Mailanhängen mit einem Computervirus infiziert werden kann?	0	2	4	2	0
Wie hoch ist Deiner Ansicht nach das Risiko, dass man es nicht merkt, wenn der Rechner mit einem Computervirus infiziert ist?	4	2	2	0	0
Wie hoch ist Deiner Ansicht nach das Risiko, dass ein Computervirus von der Antivirensoftware nicht erkannt wird?	0	0	2	2	4

	sehr hohes Risiko				sehr geringes Risiko
Wie hoch ist Deiner Ansicht nach das Risiko, dass der Computer durch den Download von Dateien über Tauschbörsen (z.B. eMule, BitTorrent) mit einem Computervirus infiziert werden kann?	2	4	2	0	0
Wie hoch ist Deiner Ansicht nach das Risiko, dass der Computer beim Surfen im Internet (ohne Dateien herunterzuladen) mit einem Computervirus infiziert werden kann?	0	2	4	2	0

Teil G: Maßnahmen Datenschutz

G1. Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? ANK

	Ja	Nein	Weiß nicht
Ich nutze Pop-Up-Blocker oder Adblocker.	X		
Ich nutze eine Firewall.	X		
Ich nutze eine Verschlüsselungssoftware beim E-Mailen und Chatten.	X		
Ich aktualisiere regelmäßig meine Anti-Viren-Software.	X		
Ich nutze Anonymisierungstools. (Ein Anonymisierungstool ist eine Software, die Daten beim Surfen so verändert, dass keine Rückschlüsse auf Dich als Besucher der Internetseiten gezogen werden können.)	X		
Ich nutze Anti-Tracking-Software. (Anti-Tracking-Software ist eine Software, die ein Nachverfolgen des Besuchs von Internetseiten verhindert.)	X		

G2. Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten?

	Ja	Nein	Weiß nicht	
Ich nutze verschiedene Passwörter.	X			HK
Ich nutze sichere Geräte mit persönlichem Passwort.	X			HK
Unter der Annahme, dass ich ein Soziales Netzwerk nutze, aktualisiere ich persönliche Sicherheitseinstellungen in Sozialen Netzwerken gegenüber Grundeinstellungen.	X			HK
Ich nutze nur Seiten, bei denen ich weiß, dass sie sicher sind.	X			HK
Ich habe aktive Inhalte im Browser (z. B. Javascript, ActiveX) deaktiviert.				UK

Teil H: Eigenes Verhalten

H1. Wie sehr treffen die folgenden Aussagen auf Dich zu?

	trifft voll und ganz zu				trifft überhaupt nicht zu	
Ich suche immer erst nach Möglichkeiten, Musik im Internet kostenlos zu bekommen, bevor ich daran denke, sie zu kaufen.	4	3	2	1	0	ANK
Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.	4	3	2	1	0	HK
Ich sichere in regelmäßigen Abständen die wichtigsten Daten auf einem CD/DVD-Rohling oder einer externen Festplatte.	4	3	2	1	0	HK
Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.	0	1	2	3	4	UK
Wenn ich mir die Originalversion einer Software nicht leisten kann, suche ich nach kostenlosen und legalen Freeware-Alternativen.	4	3	2	1	0	ANK
Ich denke nicht lange darüber nach, einen E-Mail-Anhang zu öffnen – ich tue es einfach.	0	1	2	3	4	RK
Wenn ich per E-Mail oder im Chat einen Link zugesendet bekomme, klicke ich ihn meistens an, auch wenn ich mir nicht sicher bin, auf welcher Seite ich lande.	0	1	2	3	4	RK
Ich achte nicht darauf, von welchen Seiten die Dateien stammen, die ich herunterlade.	0	1	2	3	4	RK
E-Mails, bei denen ich die Vermutung habe, dass es sich um unerwünschte Nachrichten (Spam) handelt, lösche ich sofort.	4	3	2	1	0	HK
Ich ändere in regelmäßigen Abständen alle meine Passwörter.	4	3	2	1	0	HK
Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.	4	3	2	1	0	HK
Aufgrund des hohen Sicherheitsrisikos im Internet schränke ich meine Online-Zeit ein.	0	1	2	3	4	HK

Teil I: Persönliche Informationen

I1. Bist Du männlich oder weiblich?

☐ weiblich

☐ männlich

I2. Wie alt bist Du?

☐☐

I3. Welche Schulform besuchst Du?

☐ Realschule Plus

☐ Gymnasium

☐ IGS

I4. Worüber hättest Du gerne mehr Informationen?

	Ja	Unsicher	Nein
… zum Schutz meiner Daten im Internet.	☐	☐	☐
… zur rechtlichen Situation in Bezug auf den Schutz meiner Daten.	☐	☐	☐
… zu technischen Möglichkeiten des Schutzes meiner Daten.	☐	☐	☐
… zu den Gefahren beim Surfen im Internet	☐	☐	☐

I5. Hier hast Du die Möglichkeit, wenn Du möchtest, weitere Wünsche und Anregungen bezüglich dieser Studie zum Thema Datenschutz zu nennen:

Vielen Dank für die Teilnahme an der Umfrage.

Du kannst das Browserfenster nun schließen.

Berechnungsweg zur Feststellung der Kompetenznote und Beschreibung der Auswertung der bivariaten Analyse:

Aus den vorherigen Seiten ist die Codierung der Antworten ersichtlich. Mit Ausnahme der Fragen, bei denen die Antworten offensichtlich sind (z. B. Wissensfragen), traf der Autor für andere Items eine Einschätzung auf Basis der Mindestanforderungen aus dem Datenschutzkompetenzmodell. Die in Abschnitt 3.5 formulierten Datenschutzkompetenzen wurden auf die Items übertragen.

Es gibt je nach Skalen-Typ genau vier Möglichkeiten der Codierung, welcher Maßstab einem Item bzw. einer Frage zugrunde gelegt wird:

Fall[1]	Skalen-Typ	Verrechnung durch Summation: Prozentualer Anteil der Schüler, die wie folgt angekreuzt haben …	Item-Code
A	Likert 0 – 4	die Werte *3* und *4* oder nur *4* *)	D6, H1, B3/4
B	abgewandelt Likert 0 / 2 / 4	die Werte *2* und *4*	F2
C	ja / weiß nicht / nein	*ja*-Feld	G1, G2
D	Abschätzung	das angekreuzte Feld bis zum Extremum *sehr sensibel* bzw. *sehr hohes Risiko.*	A2, F1
X1	Im Fall der Dimension *Wissen* wird der prozentuale Anteil der korrekten Antworten pro Fragekomplex genommen und abschließend der Mittelwert gebildet		C, E
X2	Es wurde die Summe der Werte betrachtet, wenn mindestens eine Einstellung geändert worden ist		B1/2
*) dieser Fall, das nur *4* gewertet worden ist, tritt nur bei H1 auf. Anhand der gelb markierten Zahlen in der Auswertung (Anhang A4.9 und A.10) kann abgelesen werden, welcher Fall bei dem jeweils entsprechenden Item zutrifft.			

Tab. A4.8-1: Verrechnungstabelle deskriptive Auswertung

Für die (differenzierte) deskriptive Auswertung gilt: In den Fällen A2, F1 und F2 wird pro Frage der Mittelwert bzgl. der Frage und abschließend über alle Fragen der Mittelwert der entsprechenden Dimension berechnet.

Der prozentuale Wert der Dimensionen dient als Maßstab für die Beurteilung der entsprechenden Dimension gemäß Tabelle 4.7. In den Anhängen A4.9 und A4.10 sind in blau die entsprechenden Zahlenwerte in die Diagramme eingetragen.

[1] Im Fall der differenzierten deskriptiven Auswertung gelten nur die Fälle A, C, D, X1 und X2.

Für die Auswertung der bivariaten Analyse gilt:

Damit ein Zusammenhang zwischen den Daten hergestellt werden kann, musste für alle Fragen eine Normierung definiert werden, da nicht alle Fragen an einer 5-Likert-Skala orientiert sind. Die folgende Tabelle fasst ausgehend von Tabelle A4.8-1 die Fälle zusammen:

Fall	Codierung	Dimension	Item
A	Die Skala für die jeweilige Kompetenz ist von 4 bis 0 bzw. 0 bis 4 nummeriert (5-Likert-Skala).	RK, ANK, UK, HK	B3/4, D6, H1
B	Hier wurde für jeden Gesichtspunkt eine Stelle in der 5-Likert-Skala definiert, die für den Fall einer korrekten Einschätzung mit 4 Punkten versehen wurde; die davon direkt benachbarten Stellen erhielten jeweils 2 Punkte und alle weiteren Felder 0 Punkte. Am Ende wurde der Mittelwert der Punkte gebildet (5-Likert-Skala).	RK	F2
C	Für die entsprechende Antwort „Ja“ wurde jeweils ein Punkt vergeben und auf eine 5-Likert-Skala von 0 bis 4 normiert Für die Antwort „Ja“ gab es je einen Punkt und am Ende wurde die Summe der vier Teilitems betrachtet.[2]	ANK, HK	G1, G2
D	Hier wurde für jedes einzelne Kriterium eine Stelle in der 5-Likert-Skala definiert, an der ab dieser Stelle und abwärts betrachtet (im Sinne von *sehr sensibel/sollte nicht veröffentlicht werden* bzw. *sehr hohes Risiko*) ein Punkt vergeben wurde; d. h., dass der Schüler jeweils dann einen Punkt erhielt, wenn er das Kriterium wie eingeschätzt oder im Sinne „sensibler“ bzw. „noch höheres Risiko“ ankreuzte. Am Ende wurde die Gesamtsumme der Punkte gebildet und auf eine 5-Likert-Skala von 0 bis 4 normiert.	RK	A2, F1
X1	Pro korrekte Antwort in dem Multiple-Choice-Fragebogen ergab einen Punkt, sodass insgesamt zwischen 0 und 5 Punkte erreicht werden konnten. Abschließend wurde auf die 5-Likert-Skala normiert. Für jede richtige Antwort wurde ein Punkt vergeben und pro Wissensblock die Summe der korrekten Antworten auf die 5-Likert-Skala normiert.	W	C, E

Tab. A4.8-2a: Codierung der Items

[2] Das letzte Teilitem in diesem Frageblock zur Messung der Urteilskompetenz wurde verworfen, da die Schüler die Fragestellung nicht verstanden hatten; s. dazu auch die Anmerkung in Abschnitt 4.3.3.1.

Fall	Codierung	Dimension	Item
X2	Wer nur die erste Antwort ankreuzte (nichts geändert, da dem Anbieter Vertrauen geschenkt wird), bekam 0 Punkte; wer die Kontaktaufnahme und/oder das Auffinden ankreuzte, bekam 1 Punkt, da diese beiden Kriterien im Vergleich zu *Sichtbarkeit des Profils*, *Sichtbarkeit des Posts* und *Möglichkeit des Postens auf der Seite* als weniger kritisch eingestuft wurden; mit 2 Punkten wurde bewertet, wenn einer der Gesichtspunkte *Sichtbarkeit des Profils*, *Sichtbarkeit des Posts* und *Möglichkeit des Postens auf der Seite* angekreuzt wurde (unabhängig von der Kontaktaufnahme und/oder dem Auffinden); wenn zwei oder drei der Aspekte *Sichtbarkeit des Profils*, *Sichtbarkeit des Posts* und *Möglichkeit des Postens auf der Seite* (unabhängig von der Kontaktaufnahme und/oder dem Auffinden) angekreuzt wurden, erhielt 3 Punkte; die 4 Punkten wurden vergeben, wenn alle Gesichtspunkte *Sichtbarkeit des Profils*, *Sichtbarkeit des Posts* und *Möglichkeit des Postens auf der Seite* (unabhängig von der Kontaktaufnahme und/oder dem Auffinden) angekreuzt wurden.	UK	B1/2

Tab. A4.8-2b: Codierung der Items

Die Verrechnung der Dimensionen aus den verschiedenen Frageblöcken erfolgte nach dem folgenden Schlüssel:

Dim.	Verrechnung
W	Summierung aller Punkte der Einzelfragen aus dem Bereich Wissen und Normierung auf 100%
RK	Summierung aller Punkte aus Risikobewertungskompetenz und Normierung auf 100% (ist die Frage zur Messenger-Nutzung (D6) beantwortet worden, dann floss sie an dieser Stelle bei dem jeweiligen Schüler mit ein)
ANK	Summierung aller Punkte aus der jeweiligen Kompetenz und Normierung auf 100%
UK	
HK	

Tab. A4.8-3: Verrechnungsschlüssel der Dimensionen

Die Mittelwerte von Risikobewertungskompetenz, Auswahl- und Nutzungskompetenz, Urteilskompetenz und Handlungskompetenz wurden abschließend als (neue Variable) Datenschutzkompetenz (DK) zusammengefasst und als solche zur Dimension *Wissen* in Beziehung gesetzt. Abschließend wurden die errechneten Prozentwerte gegeneinander aufgetragen. Die graphische Auswertung befindet sich in Anhang A4.11.

ANHANG 4.9

Deskriptive Auswertung der Studie

Die folgenden Seiten umfassen die Diagramme der deskriptiven Auswertung der Studie inklusive knapper Beschreibung. Hinter der Frage steht in eckigen Klammern der Code des LimeSurvey-Fragebogens (vgl. Anhang A4.7) und die Kompetenz (kursiv geschrieben), die sich aus der Auswertung der Q-Sortierung (vgl. Anhang A4.4) ergibt.
Ferner steht in der Mehrheit der Fälle in blauer Schrift innerhalb der Diagramme der prozentuale Anteil (die Zahl ist eingerahmt), der für die Bewertung des Items bzw. der Kompetenz relevant ist; zudem sind die in die Berechnungen eingeflossenen Zahlen gelb markiert. In vielen Fällen ist dies die Summe einzelner Werte. Ist der prozentuale Anteil direkt aus dem Diagramm ersichtlich, dann ist er nicht separat aufgeführt.

Welche Sozialen Netzwerke[1] nutzt du? [A1]

Hier war eine Mehrfachauswahl möglich.

Eindeutiger Favorit ist *YouTube*, gefolgt von *SnapChat*, *Google+* und *Instagram*. Die restlichen Sozialen Netzwerke sind eher uninteressant.
(Bemerkenswert ist, dass von den vier Favoriten nur *Google+* ein Soziales Netzwerk ist. Gerade *YouTube* entspricht nicht den Vorstellungen eines solchen.)

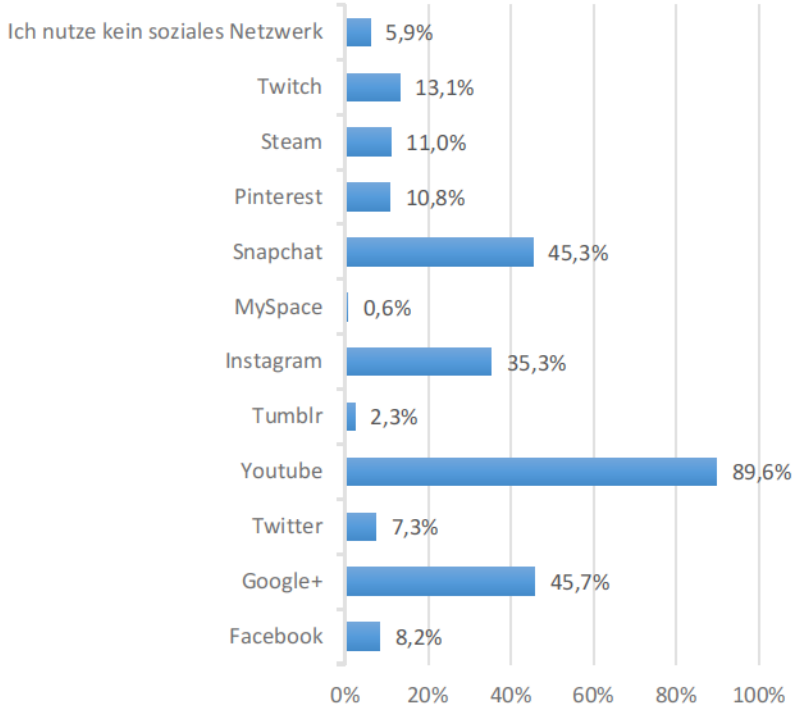


Abb. A4.9-1

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]
(Fortsetzung nächste Seite)

Die persönliche Einschätzung zur Sensibilität personenbezogener Daten ist ein Maß für die Risikobewertungskompetenz.
Weniger kritisch werden Angaben wie Spitznamen, Lieblingsorte, eigene Erlebnisse und Religion gesehen, während Interessen und Hobbies und Lieblingsfilme u. Ä. als unkritisch eingestuft werden.

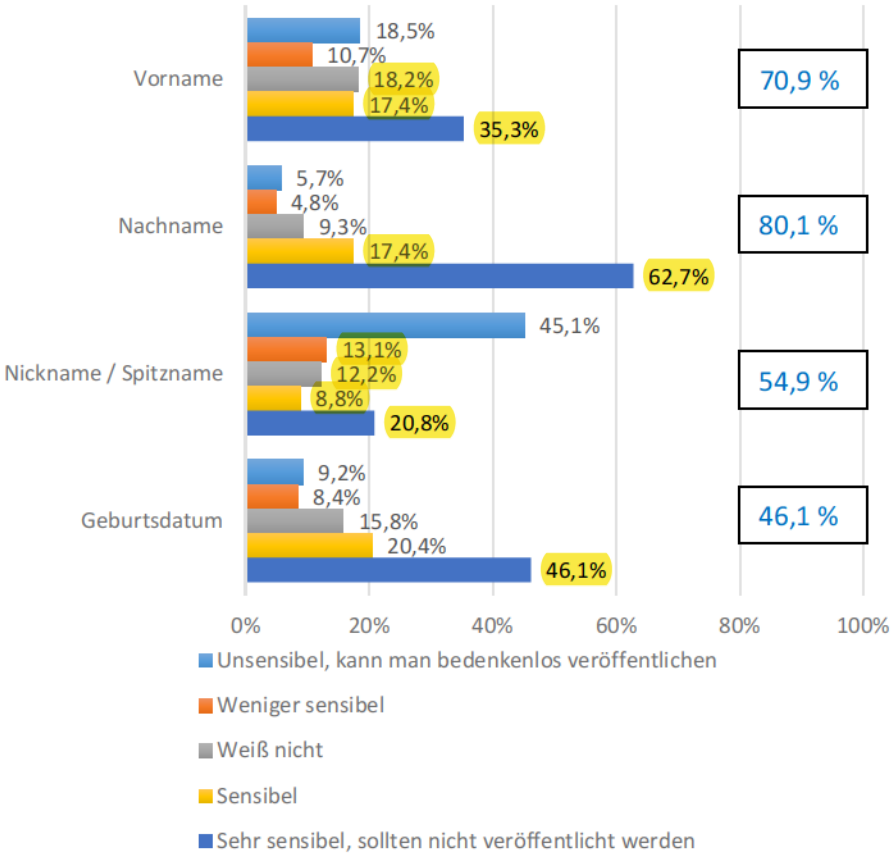


Abb. A4.9-2a

[1] Zur Auswahl der Sozialen Netzwerke bei dieser Fragestellung s. Anhang A4.17.

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*] (Fortsetzung)

Hingegen sind Angaben wie Nachname, Geburtsdatum, Adresse, Telefonnummer, Kontakte, aber auch eigene Gedanken, Gefühle und Sorgen sehr sensible Daten.

Durchschnittswert der Risikobewertungskompetenz dieser Frage beträgt 66,5 %.

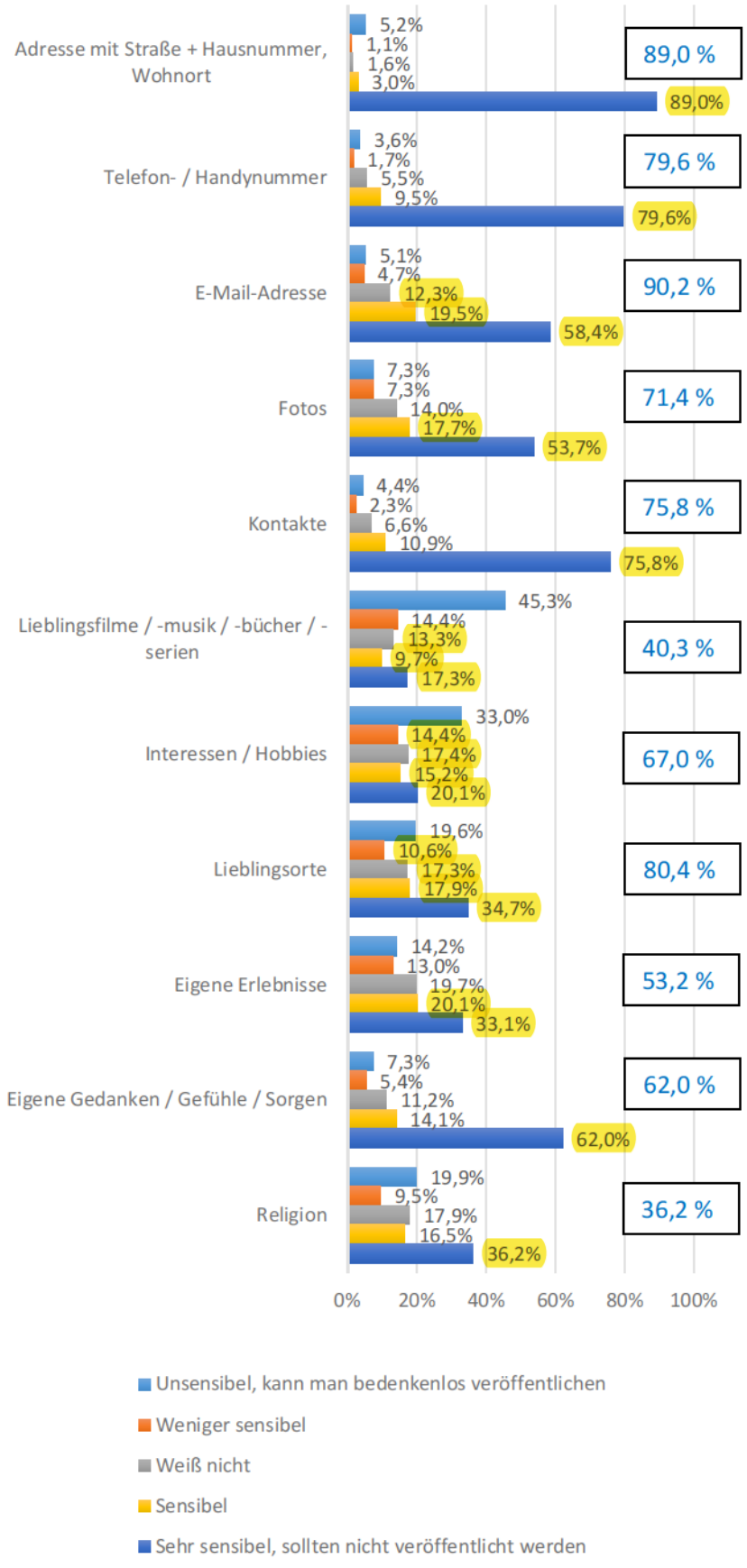


Abb. A4.9-2b

Hast du die Privatsphären-einstellungen im Sozialen Netzwerk geändert bzw. würdest Du sie ändern? [B1+B2; *UK*]

Mehr als die Hälfte nimmt keine Änderungen in den Grundeinstellungen eines Sozialen Netzwerks vor und vertraut den Einstellungen der Anbieter. Ein Fünftel der Schüler nimmt eine Änderung und rund 1/4 nimmt zwei oder mehr Änderungen vor.

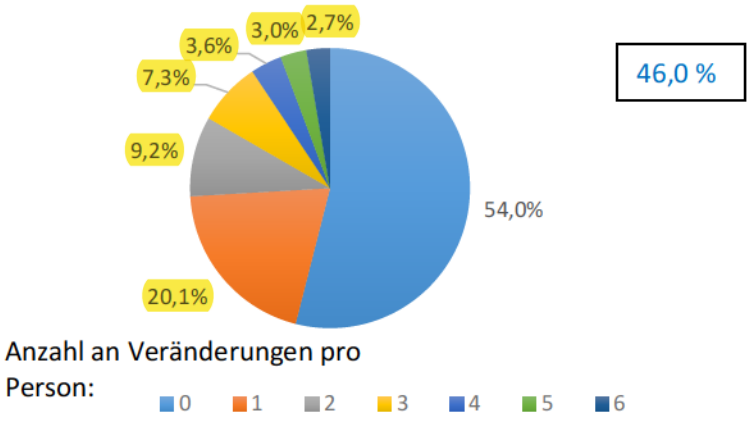


Abb. A4.9-3

Hast du die Privatsphären-einstellungen im Sozialen Netzwerk geändert bzw. würdest Du sie ändern? Wenn ja, welche? [B1+B2; *UK*]

Hier war eine Mehrfachauswahl möglich, wenn man etwas ändert.

Wegen des Vertrauens in den Anbieter wird i. d. R. nichts geändert.
Die Änderungen betreffen v. a. die Möglichkeit der Einschränkung der Kontaktaufnahme, Auffindbarkeit zur eigenen Person und die Sichtbarkeit des eigenen Profils im Sozialen Netzwerk (jeweils ca. 20 %). Von rund 15 % wird die Sichtbarkeit eigener Posts und des eigenen Profils außerhalb des Sozialen Netzwerks eingeschränkt. Und gut 10 % begrenzen die Post-Möglichkeiten Anderer auf der eigenen Seite.

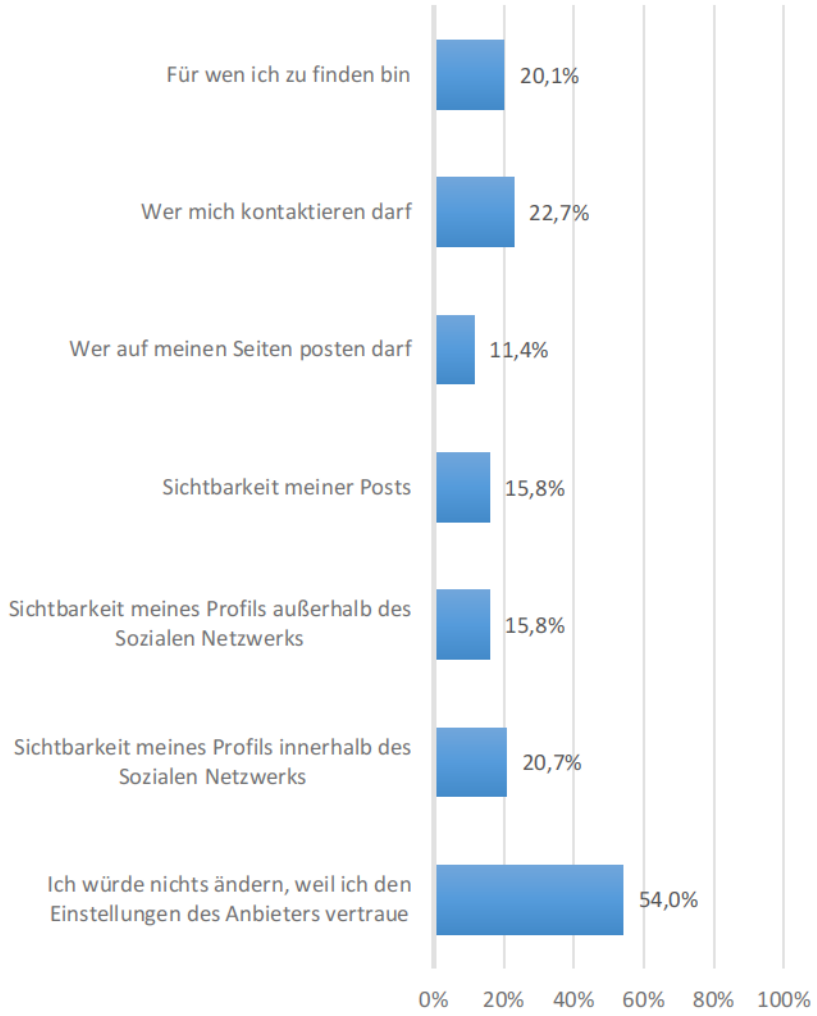


Abb. A4.9-4

Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [B3+B4; *HK*, *UK*]

Informationen, die ins Internet gestellt werden, und die Möglichkeit der Selbstbestimmung, wer etwas über einen erfährt, ist den Probanden extrem wichtig (rund 70 bzw. 75 % der Jugendlichen). Nur 1/3 der Befragten denkt nicht darüber nach, wer gepostete Inhalte später sehen kann.

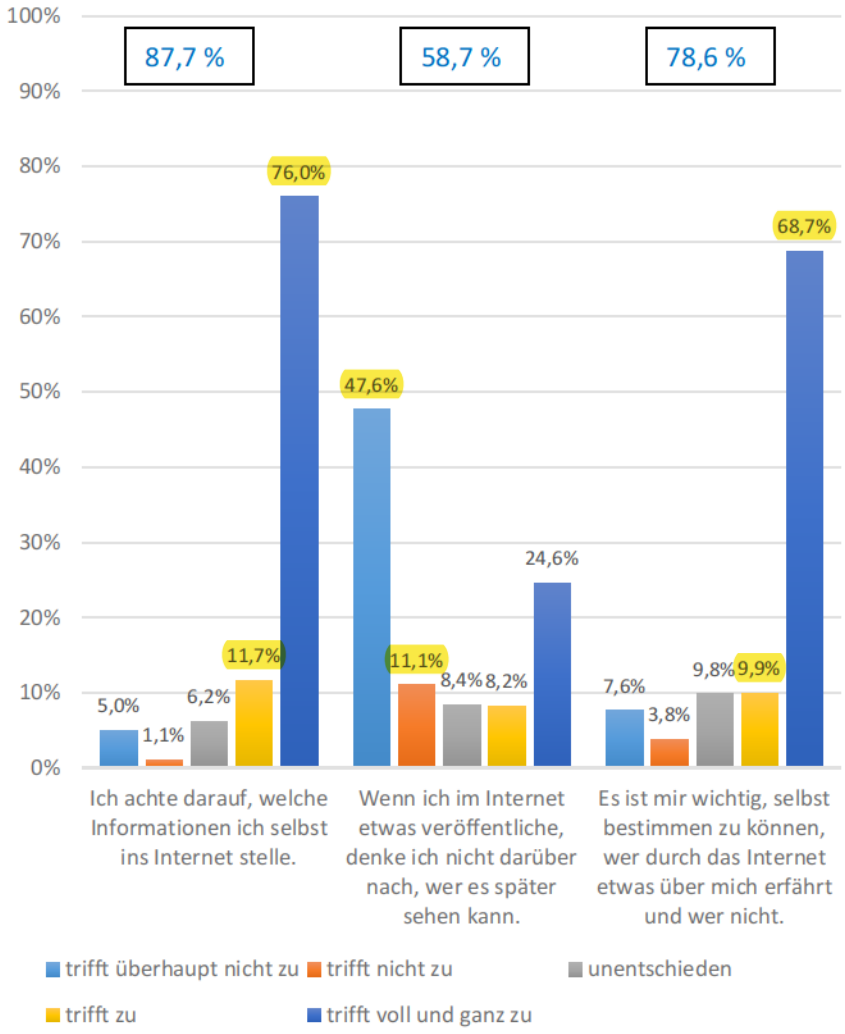


Abb. A4.9-5

Bei den Fragen im ersten Wissensteil [C1 – C5; *W*] sah das Ergebnis aller abgegebenen Fragen im Schnitt folgendermaßen aus:

Der Anteil bezieht sich auf alle gegebenen Antworten. Rund 1/5 der vorgegebenen Antworten sind richtig, während mehr als die Hälfte *weiß ich nicht* lautet.

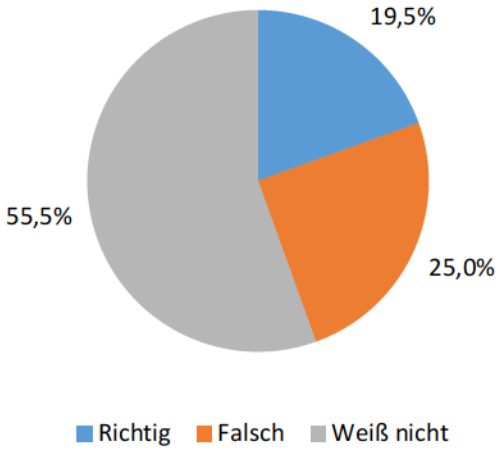
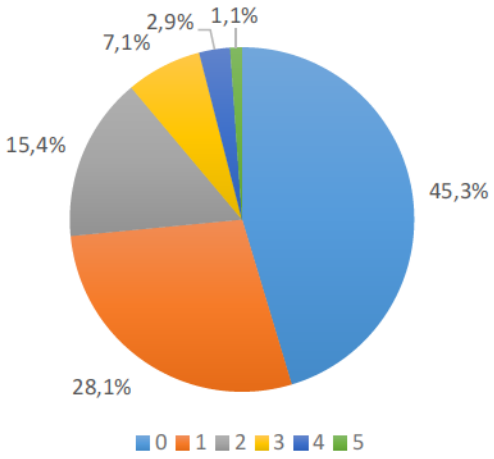


Abb. A4.9-6

Anzahl an richtiger Antworten im ersten Wissensteil [C1 – C5; *W*] pro Person:

In diesem Fall wurde *Weiß nicht* als falsch bewertet. Der Anteil bezieht sich auf die Schüler.

Gut 2/5 der Teilnehmer gibt keine richtige Antwort oder weiß es nicht. Immerhin bei rund einem Viertel ist es noch eine korrekte Antwort unter allen. (Die Ratewahrscheinlichkeit für die jeweils korrekte Antwort der Multiple-Choice-Aufgaben beträgt unter der Annahme, dass *weiß nicht* nicht geraten wurde, 1/4.)



In diesem Fall wurde "Weiß nicht" als Falsch bewertet!

Abb. A4.9-7

Bekannte Browser bei den Schülern: [D2]

Hier war eine Mehrfachauswahl möglich.

Chrome und *Firefox* sind sehr bekannt; rund 40 % kennen *Microsoft Edge und Apple Safari*.
Die Nutzung keines Browsers (6,5 %) verwundert.

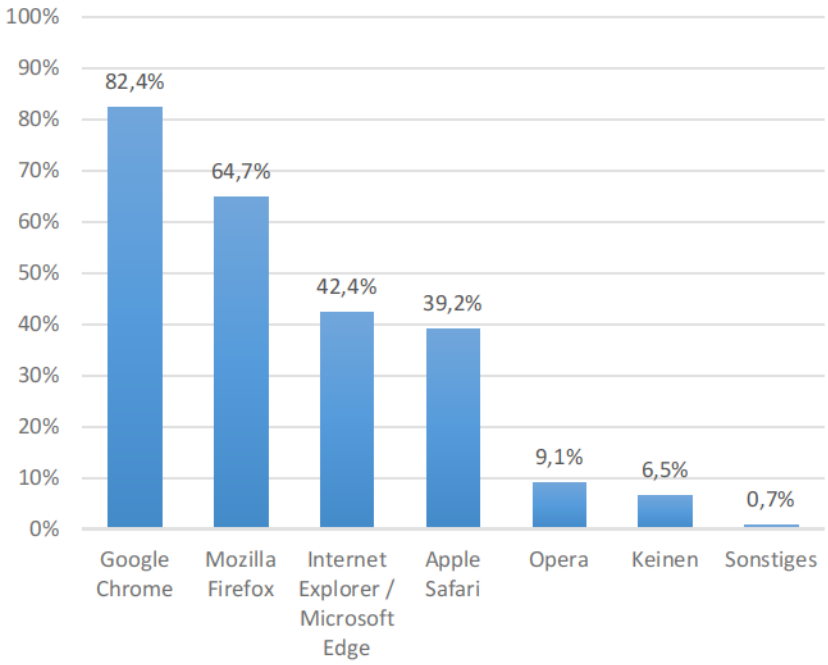


Abb. A4.9-8

Anzahl bekannter Browser pro Person: [D2]

Im Schnitt kennen die Schüler zwei bis drei Browser, sodass sie zum besseren Schutz auf Alternativen ausweichen können.

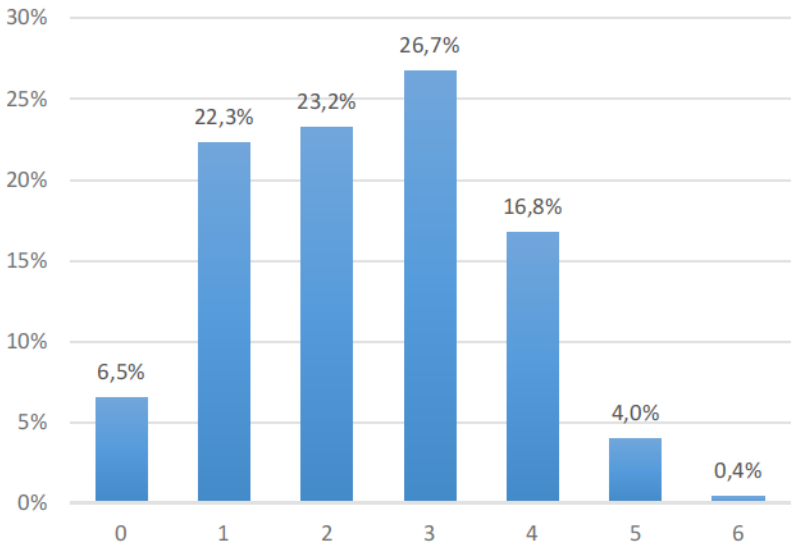


Abb. A4.9-9

Durch Schüler genutzte Browser: [D3]

Hier war eine Mehrfachauswahl möglich.

Ein ähnliches Bild wie die Antwort in Abbildung 4.9-8, jedoch ist *Microsoft Edge* weit abgeschlagen (17 %).

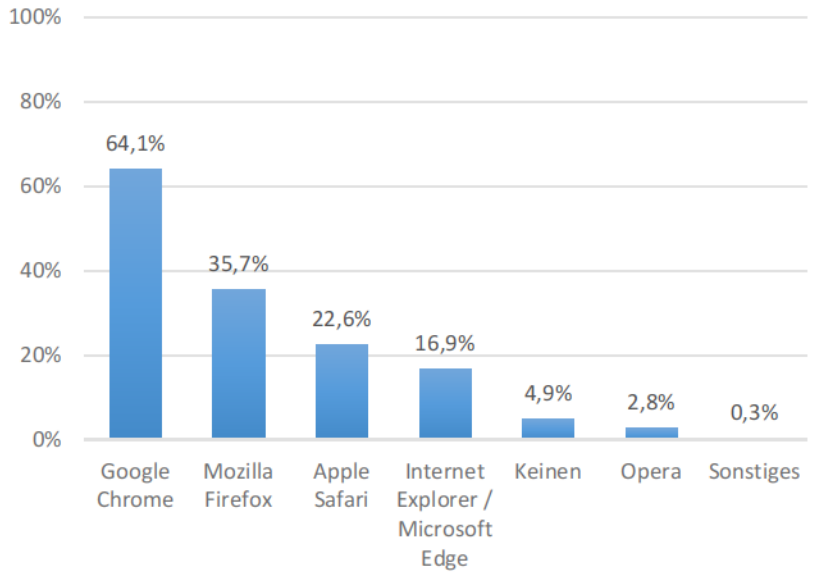


Abb. A4.9-10

Bekannte Browsertools bei den Schülerinnen und Schülern: [D4]

Hier war eine Mehrfachauswahl möglich.

Gut 80 % der Schüler kennen keine Tools, um ihren Browser sicherer zu machen. Ein Werbeblocker (11 %) und *Firebug* (6 %) sind noch die am meisten gekannten Werkzeuge.

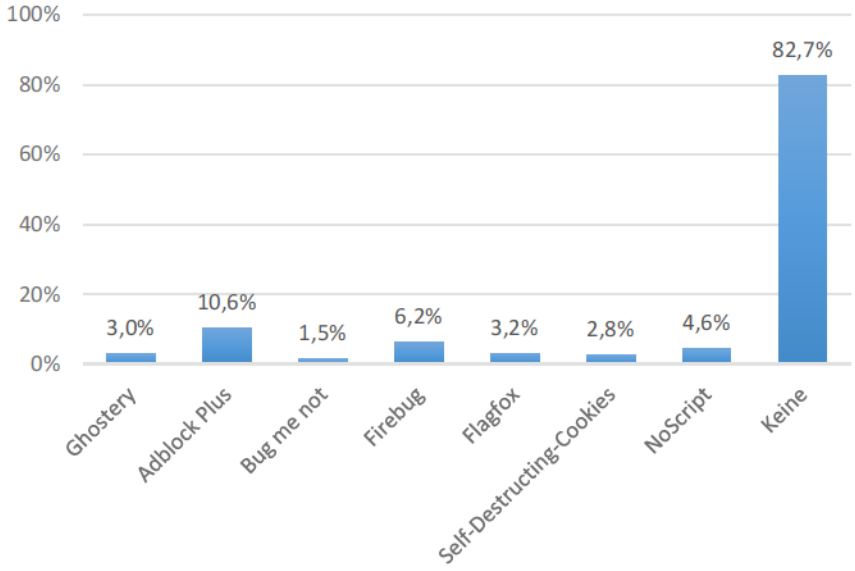


Abb. A4.9-11

Anzahl bekannter Browsertools pro Person: [D4]

Mehr als 80 % der Befragten kennen keine Browsertools und 10 % nutzen immerhin ein Tool.

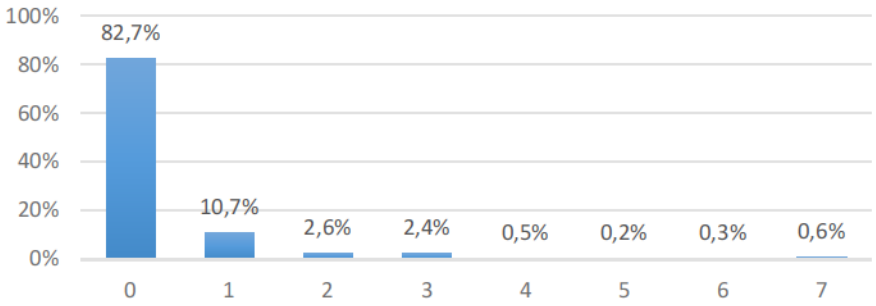


Abb. A4.9-12

Durch Schüler genutzte Browsertools:
[D5]

Diese Frage wurde nur von den 172 Schülern beantwortet, denen Browsertools bekannt waren. Hier war eine Mehrfachauswahl möglich. Es kann davon ausgegangen werden, dass nur die Tools genutzt werden, die den Schülern auch bekannt sind.

Adblock Plus (30 %) und *Firebug* (12 %) sind die Meistgenutzten; *NoScript* ist mit 9 % vertreten.

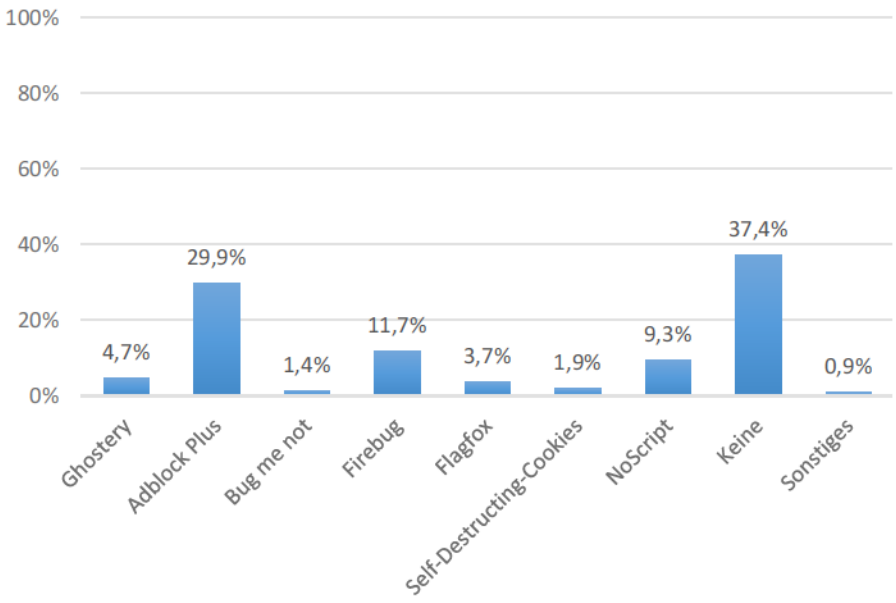


Abb. A4.9-13

Wie wichtig ist Dir jeweils einer der unten stehenden Aspekte bei der Nutzung eines Messengers? [D6; *RK*]

Eine verschlüsselte Kommunikation und die Identifikationsmöglichkeit des jeweiligen Gegenübers sind einer sehr klaren Mehrheit wichtig bzw. sehr wichtig (85 %). Die Anzahl der Nutzer und die Übertragungsgeschwindigkeit spielen eine untergeordnete Rolle, wobei – im Vergleich – für eine knappe Mehrheit dies schon von Bedeutung ist.

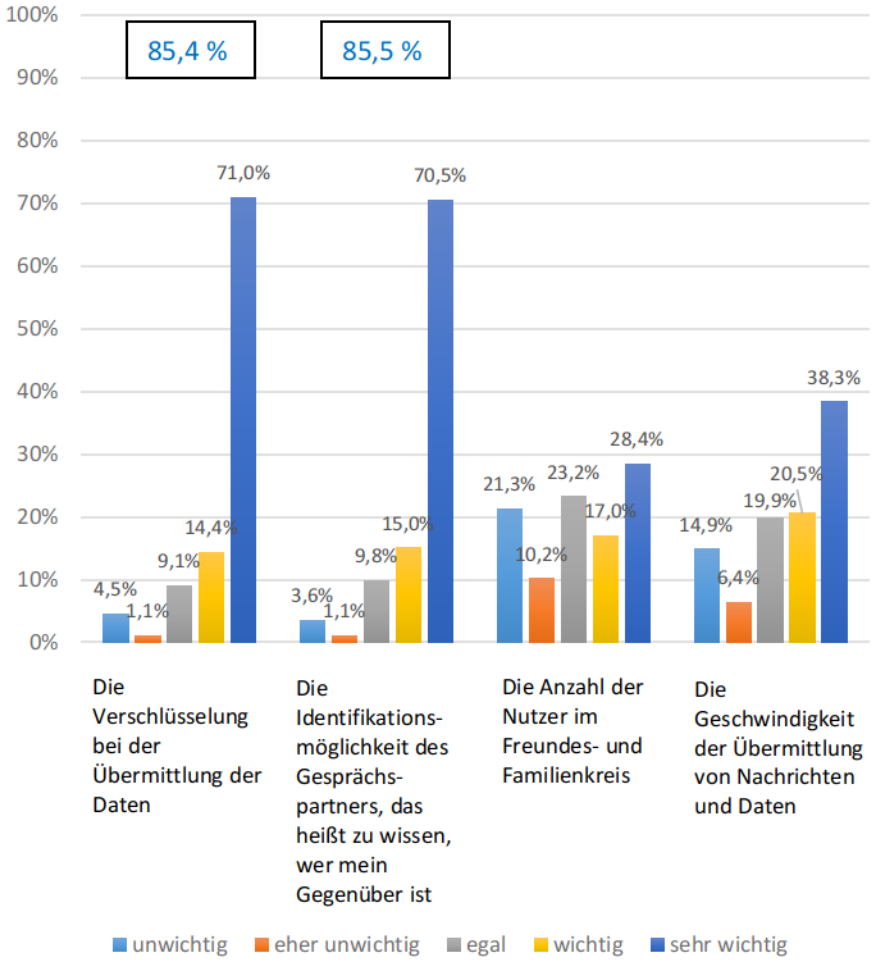


Abb. A4.9-14

Bei den Fragen im zweiten Wissensteil [E1+E2; *W*] sah das Ergebnis aller abgegebener Antworten im Schnitt folgendermaßen aus:

Der Anteil bezieht sich auf alle gegebenen Antworten. Während knapp die Hälfte der vorgegebenen Antworten *weiß ich nicht* lautet, können 35 % als korrekt verbucht werden.

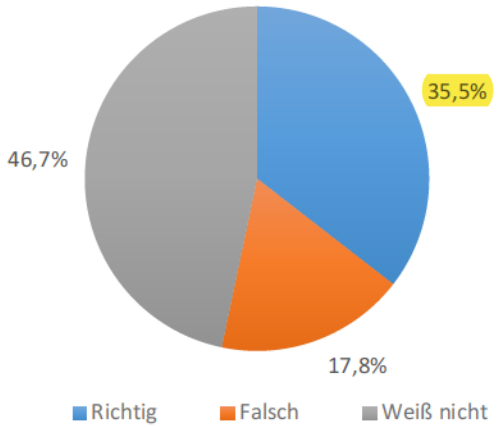


Abb. A4.9-15

Anzahl an richtiger Antworten im zweiten Wissensteil [E1+E2; *W*] pro Person:

In diesem Fall wurde *Weiß nicht* als falsch bewertet. Der Anteil bezieht sich auf die Schüler.

Im Schnitt sind zwei bis vier (von zehn) Fragen bei knapp 50 % der Schüler korrekt beantwortet, wobei ca. 1/3 der Befragten noch mehr richtige Antworten geben kann.
Knapp 20 % der Schüler beantworten keine oder nur eine Frage richtig.

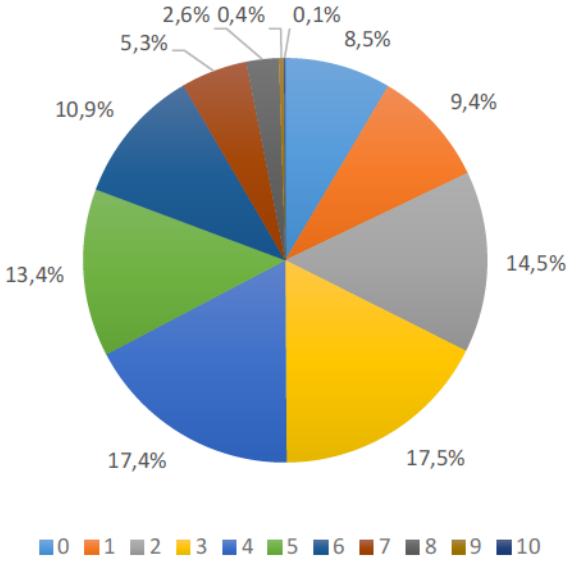


Abb. A4.9-16

Was sind für dich Risiken im Internet? [F1; *RK*]

Zwischen 53 und 65 % der Schüler stufen die vorgelegten Fälle als (ernsthafte) Risiken im Internet ein. Nur der Empfang von Spam-Mails wird von 1/3 der Schüler als sehr hohes Risiko eingestuft.

Durchschnittswert der Risikobewertungskompetenz dieser Frage beträgt 65,4 %.

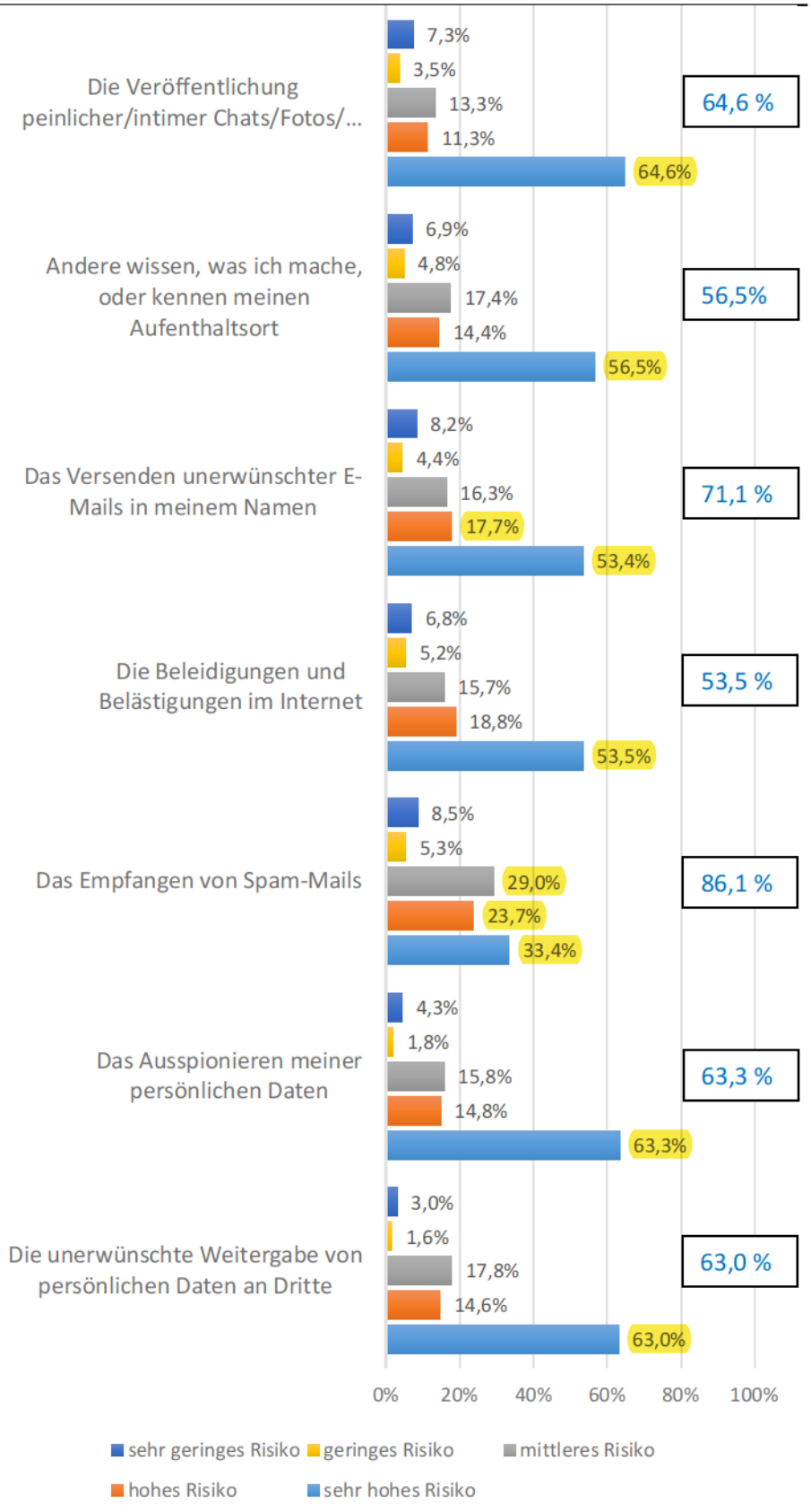
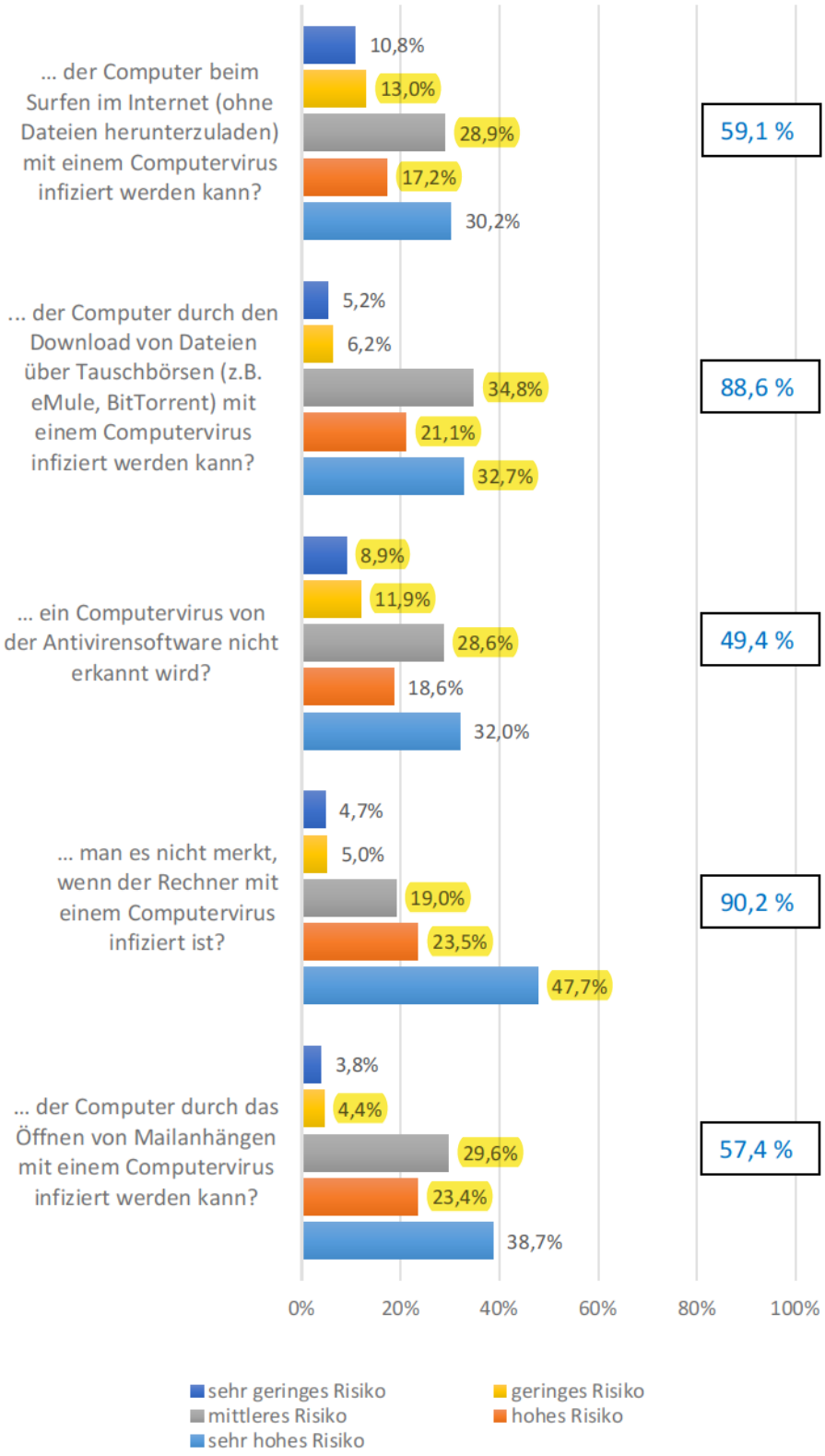


Abb. A4.9-17

Wie hoch ist Deiner Ansicht nach das Risiko, dass … [F2; *RK*]

Im Schnitt sind es zwischen knapp 50 % und 70 % der Jugendlichen, die in den gefragten Fällen ein hohes Risiko sehen, sonst schätzt knapp 1/3 es als mittleres Risiko ein, wobei hierzu auch diejenigen aufgrund des Ankreuzverhaltens gezählt werden, die im Sinne von *weiß nicht* geantwortet haben.[2] Im Fall der unbemerkten Infektion mit einem Virus fällt mit knapp 50 % ein sehr hohes Risiko durch ein klares Votum ins Auge.

Durchschnittswert der Risikobewertungskompetenz dieser Frage beträgt 68,9 %.



Fasst meine beide Fragen des Blocks F zusammen, dann ergibt sich ein Wert von 67,2 %.

Abb. A4.9-18

[2] Siehe dazu den Einleitungstext zur Umfrage im Anhang A4.7 („Solltest Du Dir mit Deiner Antwort unsicher sein, dann wähle in diesem Fall das Feld aus der Mitte aus.“)

Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? [G1; *ANK*]
Ich nutze…

Mit Ausnahme von Anti-Viren-Software weiß die Mehrheit der Befragten nicht, ob eine entsprechende Software auf dem Gerät installiert ist. Die Anti-Viren-Software wird von knapp 50 % eingesetzt. *AdBlocker*, Anonymisierungstools und Anti-Tracking-Software kommen kaum zum Einsatz. Bei 1/4 der Befragten ist die Firewall aktiviert und 30 % nutzen eine Verschlüsselungssoftware.

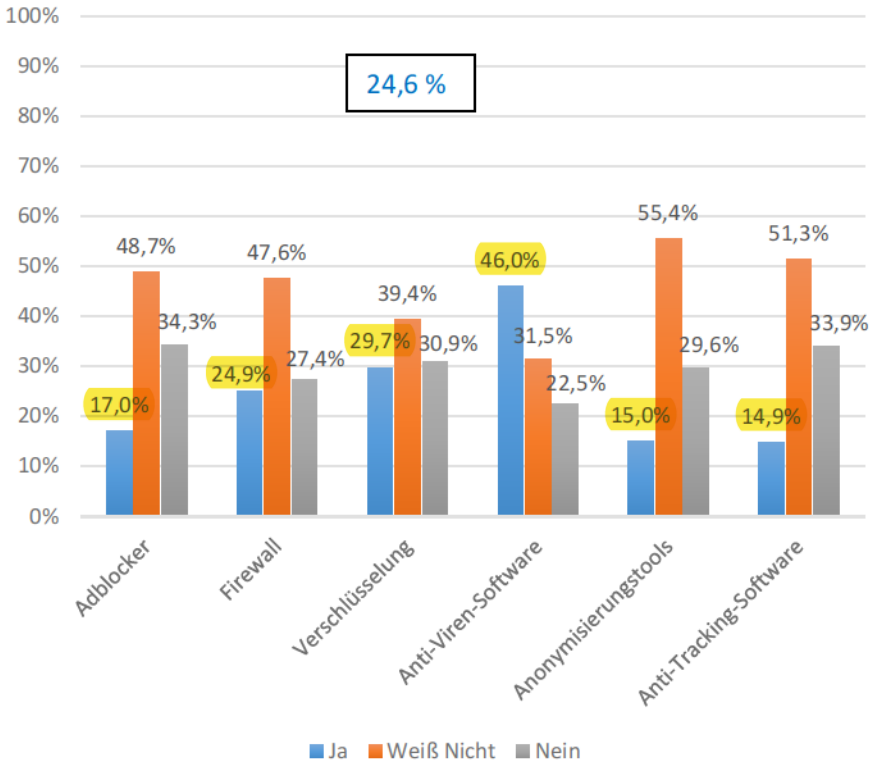


Abb. A4.9-19

Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? [G2; *HK*, *UK*]
Ich …

Die Nutzung sicherer Geräte mit Passwörtern, gefolgt von der Nutzung verschiedener Passwörter und dem Besuch sicherer Seiten werden von deutlich mehr als 50 % der Jugendlichen angegeben. Mit der Tatsache, Sicherheitseinstellungen in Sozialen Netzwerken zu aktualisieren und aktive Inhalte zu deaktivieren, kann eine deutliche Mehrheit nichts anfangen. Die Urteilskompetenz ist nicht messbar, da das letzte Item nicht verstanden worden ist.

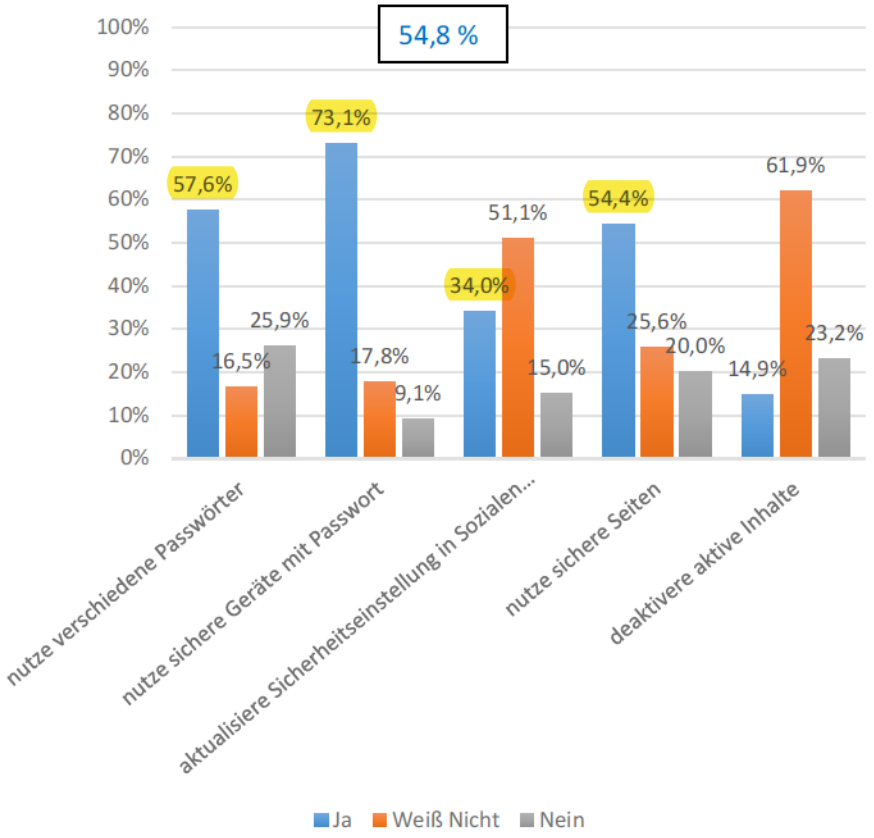


Abb. A4.9-20

Wie sehr treffen folgende Aussagen auf dich zu? (negativ) [H1; *RK, UK, ANK*]

Aus den Daten lässt sich ablesen:

[RK]: Knapp 50 % achtet darauf, woher die Dateien stammen, klickt nicht ohne Überlegung auf einen zugesandten Link oder öffnet Dateianhänge von E-Mails. Aber knapp 30 % weiß auch nicht, ob sie es tun.

[UK]: Webebanner werden von der Mehrheit nicht ohne Überlegung angeklickt und 1/4 der Befragten weiß nicht, ob sie es tun – wie im Fall der Items zur RK.

[ANK][3]: Gut 50 % der Jugendlichen nutzt die Möglichkeit kostenloser Musik aus dem Netz und gut 20 % ist sich nicht schlüssig.

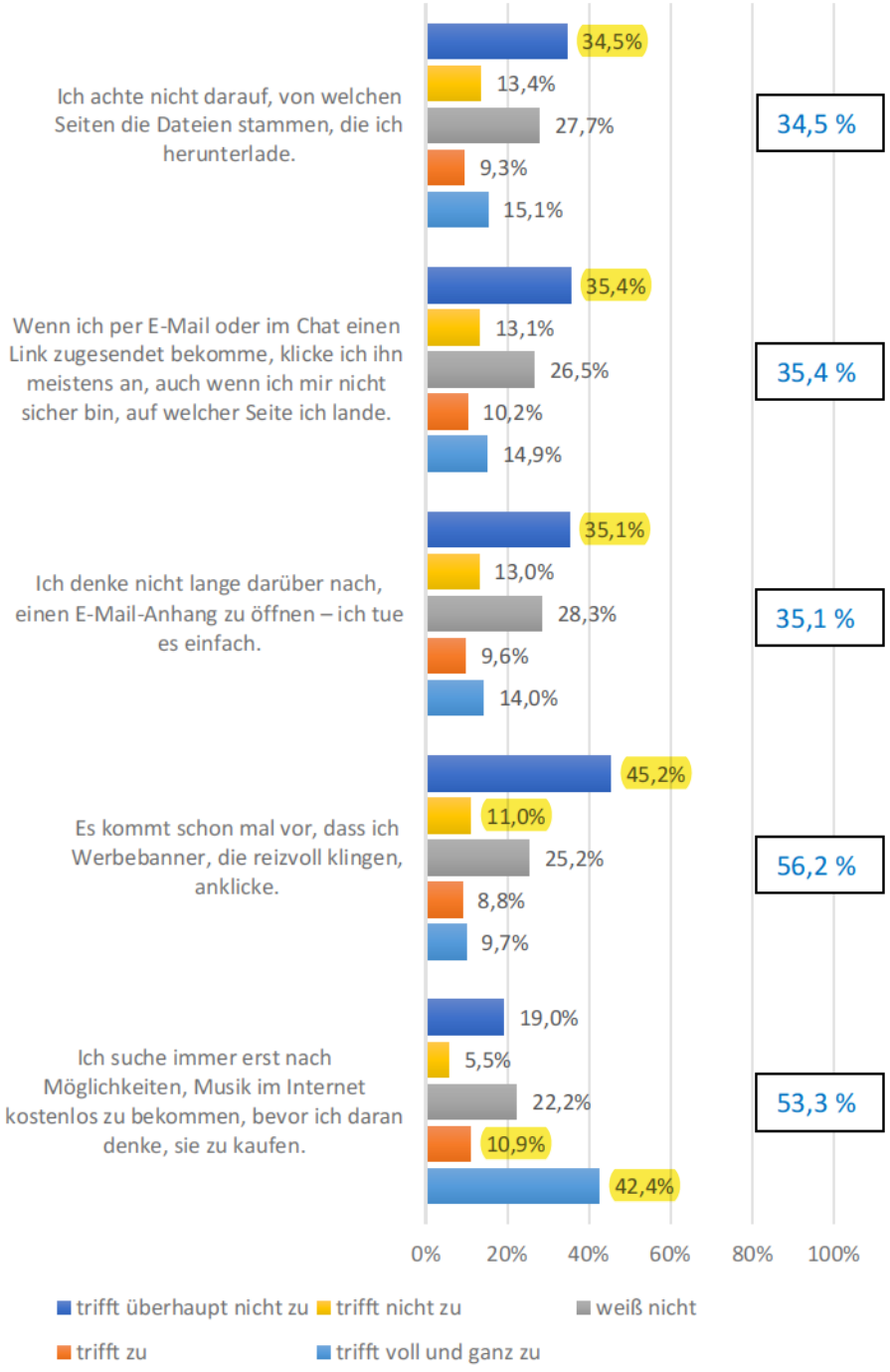


Abb. A4.9-21

[3] Bei dieser Bewertung wird angenommen, dass der kostenlose Download der Musik aus legalen Quellen erfolgt. Da dies aber im Item nicht explizit erwähnt wird, ist die Bewertung mit Vorsicht zu sehen.

Wie sehr treffen folgende Aussagen auf dich zu? (positiv) [H1; *HK*, *ANK*]

Aus den Daten lässt sich ablesen:

[HK]: Alle drei Fälle (*ich tue es – ich weiß nicht – ich tue es nicht*) sind ausgeglichen.

[HK]: Rund 45 % der Jugendlichen achten auf die Aktualisierung der Software, aber 35 % wissen es auch nicht.

[HK]: Gut 50 % der Schüler ändern ihr Passwort nicht und 22 % wissen es nicht, ob sie es tun.

[HK]: Vermuteter Spam wird von knapp 60 % sofort gelöscht, aber 25 % wissen es nicht.

[ANK]: Knapp 40 % sucht nicht nach Freeware-Software statt teurer Kaufsoftware; 32 % wissen es nicht.

[HK]: Nur 30 % sichert seine Daten regelmäßig, während gut 30 % es gar nicht tun.

[HK]: Einen regelmäßigen Virenscan der Festplatte machen 40 %, während 28 % es unterlassen.

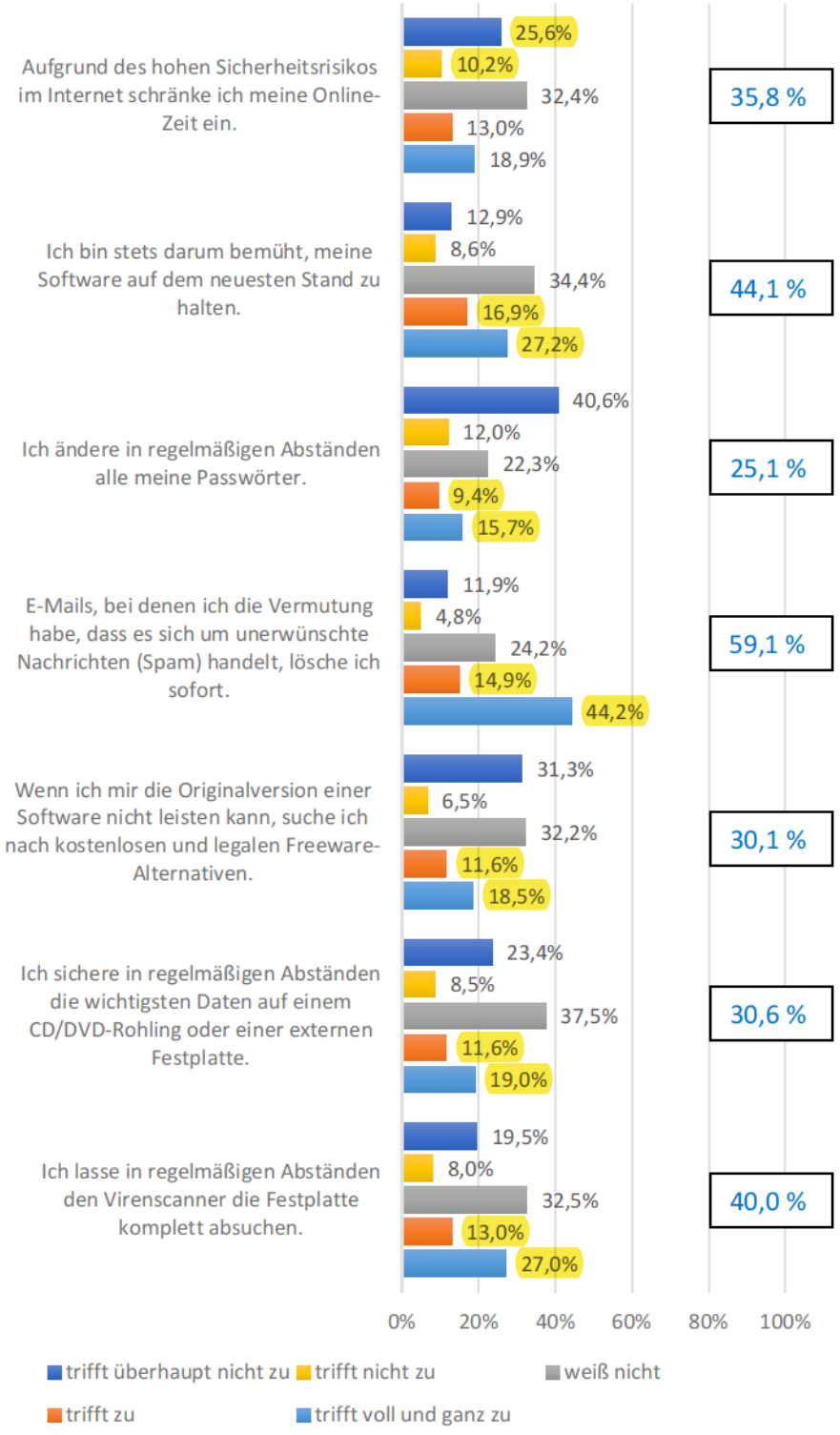


Abb. A4.9-22

Verteilung der Geschlechter:

Es liegt eine gleichmäßige Geschlechterverteilung vor.

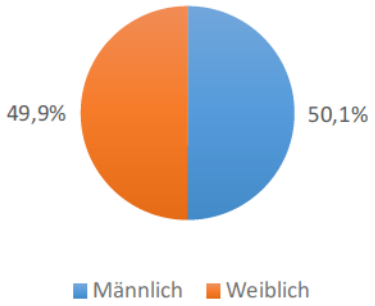


Abb. A4.9-23

Verteilung Alters:

Insbesondere Schüler im Alter von 11 bis 12 Jahren haben an der Studie teil-genommen.

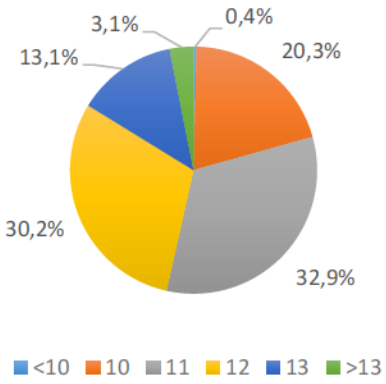


Abb. A4.9-24

Verteilung Schulart:

Drei Viertel der Teilnehmer besuchen ein Gymnasium, der andere Anteil verteilt sich auf Realschule Plus und ein geringer Anteil von knapp 10 % auf die IGS.

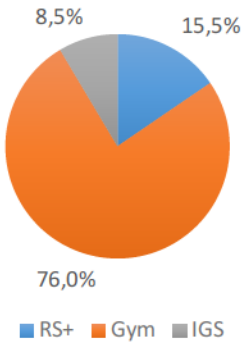


Abb. A4.9-25

Interesse an weiteren Informationen zu:

Das hohe Interesse gilt überwiegend dem Schutz von Daten und Gefahren beim Surfen. Rund 50 % wünschen weitere Informationen zu technischen Möglichkeiten und zur rechtlichen Situation.

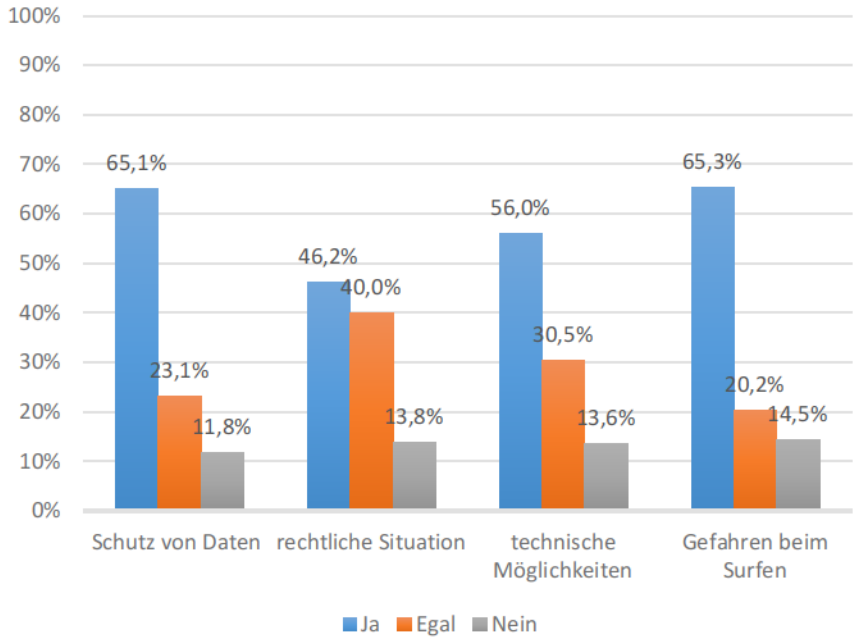


Abb. A4.9-26

ANHANG 4.10

Differenzierte deskriptive Auswertung der Studie

Die folgenden Seiten umfassen die Diagramme der differenzierten deskriptiven Auswertung der Studie inklusive einer Beschreibung. Hinter der Frage steht in eckigen Klammern der Code des LimeSurvey-Fragebogens (vgl. Anhang A4.7) und die Kompetenz (kursiv geschrieben), die sich in der Regel aus der Auswertung der Q-Sortierung (vgl. Anhang A4.4) ergibt.
Ferner steht in der Mehrheit der Fälle in blauer Schrift innerhalb der Diagramme der prozentuale Anteil (die Zahlen sind eingerahmt), die für die Bewertung des Items bzw. der Kompetenz relevant sind; zudem sind die in die Berechnungen eingeflossenen Zahlen gelb markiert. In vielen Fällen ist dies die Summe einzelner Werte. Ist der prozentuale Anteil direkt aus dem Diagramm ersichtlich, dann ist er nicht separat aufgeführt.

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Während die jüngeren Schüler den Vornamen als sehr sensibel ansehen (jeweils rund 40 %), sind es gut 25 % der älteren. Rund 20 % der Schüler – unabhängig vom Alter – können es nicht einschätzen, wie sensibel die Information ist. Ein deutlich geschlechterspezifischer Unterschied kann nicht festgestellt werden, wobei die jüngeren Teilnehmer vorsichtiger als die älteren sind.

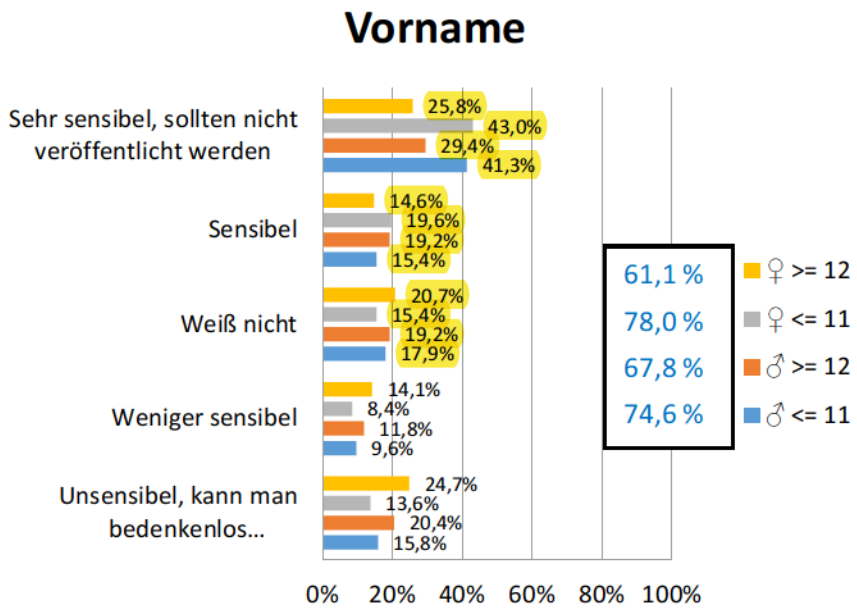


Abb. A4.10-1

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Unabhängig von Alter und Geschlecht wird der Nachname als höchst sensibel eingestuft. Der Anteil der Befragten, die unschlüssig sind, liegt zwischen 6 % (jüngere Mädchen) und 14 % (ältere Mädchen), wobei der Wert bei den Jungen unabhängig vom Alter 10 % beträgt. Insgesamt sind es rund 80 %, die mit dieser Information vorsichtig sind. Geschlechterspezifische Unterschiede sind kaum feststellbar, wobei die jüngeren Mädchen am vorsichtigen von allen sind.

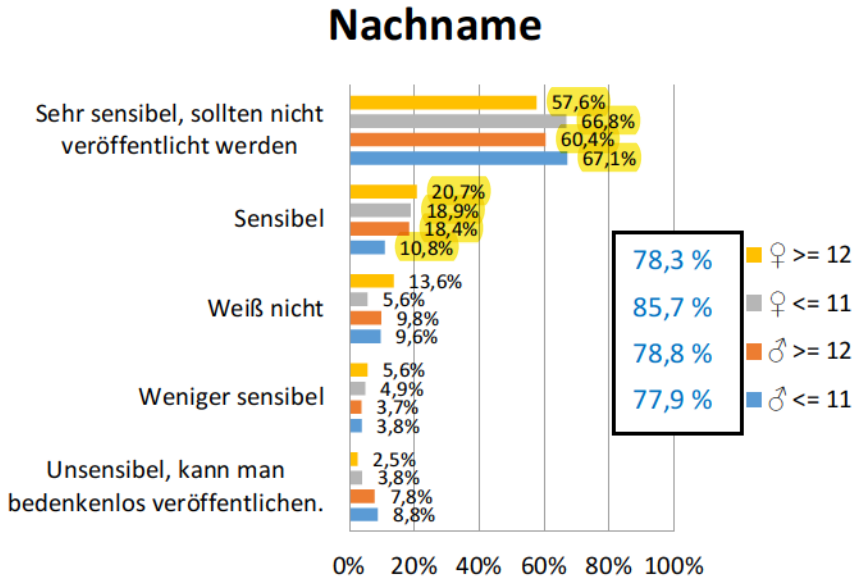


Abb. A4.10-2

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

In der Bekanntgabe des Spitznamens sehen die Älteren mit gut der Hälfte und die Jüngeren mit rund 40 % keine Gefahr, wobei die Jüngeren mit je rund 1/4 der Befragten dies als sehr sensibel einstufen. Die Jüngeren sind in dieser Bekanntgabe eher vorsichtiger. Geschlechterspezifische Unterschiede sind nicht feststellbar.

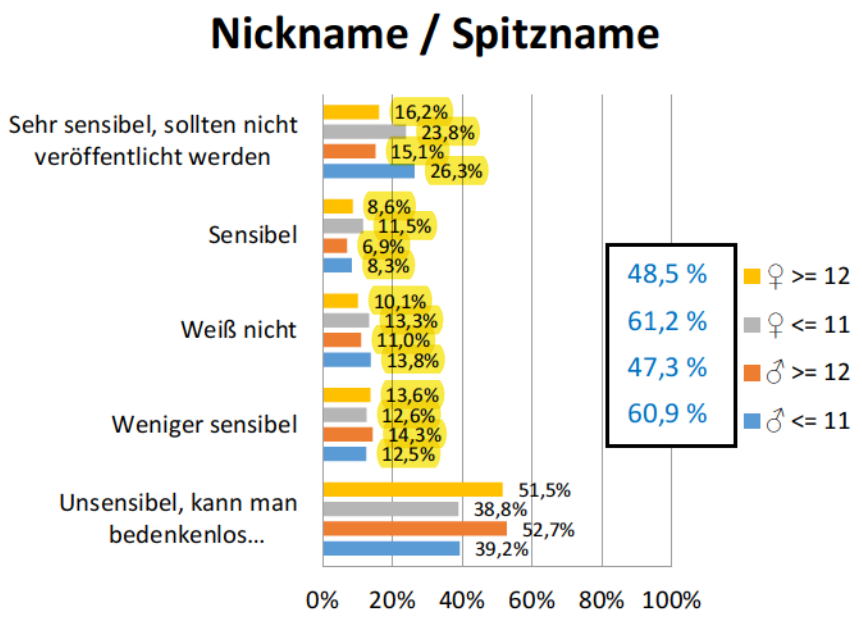


Abb. A4.10-3

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Gut die Hälfte der Jüngeren, und mit 10 % bzw. 15 % weniger die Älteren, sehen das Geburtsdatum als äußerst sensibel an, wobei die Jungen in der jeweiligen Altersgruppe sensibler als die Mädchen sind. In den anderen Fällen liegt das Feld relativ nahe beieinander, wobei die Gruppe der älteren Mädchen das Datum für unsensibler als die anderen Gruppen hält.

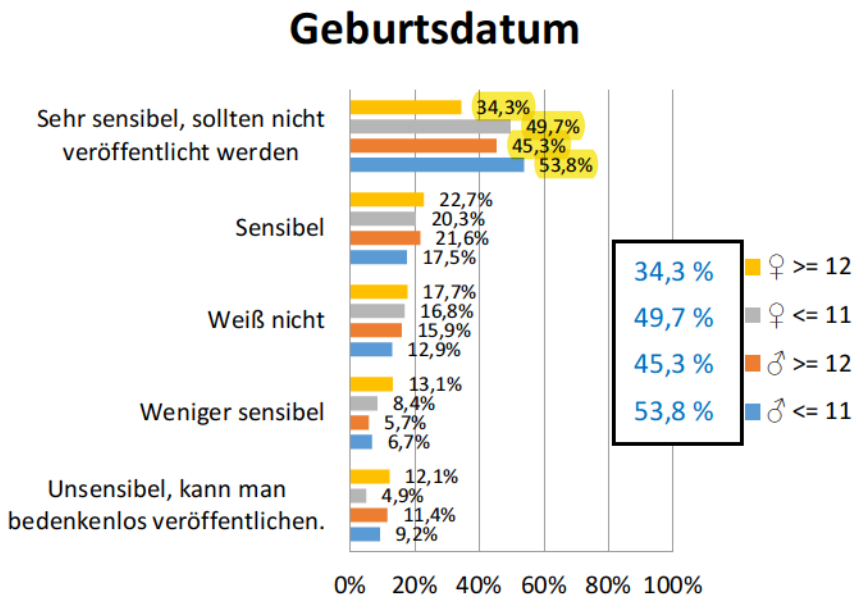


Abb. A4.10-4

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Die Mädchen sehen in der Adresse ein eindeutig sehr sensibles Datum (mit deutlich über 90 %), während die Jungen – gerade die Jüngeren mit nur 80 % – es weniger kritisch einstufen. Die jüngeren Jungen sind mit 8 % auch der größte Anteil derer, die es für unsensibel halten. Unsicher sind sich kaum welche. Insgesamt sehen die Jungen es etwas lockerer als die Mädchen.

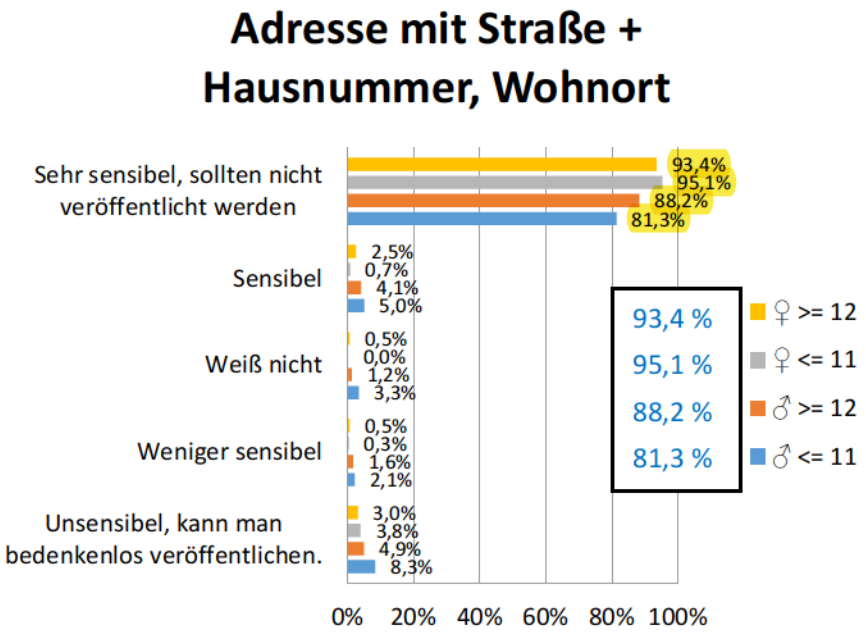


Abb. A4.10-5

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Für die Telefonnummer ergibt sich ein ähnliches Bild wie für die Adresse, jedoch sind die Älteren mit 76 % bzw. 86 % eher vorsichtig als die Jüngeren mit rund 70 %. Der Anteil der Unschlüssigen ist hier wieder größer, wobei die Jüngeren es schwerer einschätzen können. Ebenfalls sind auch hier die Mädchen wieder vorsichtiger als die Jungen.

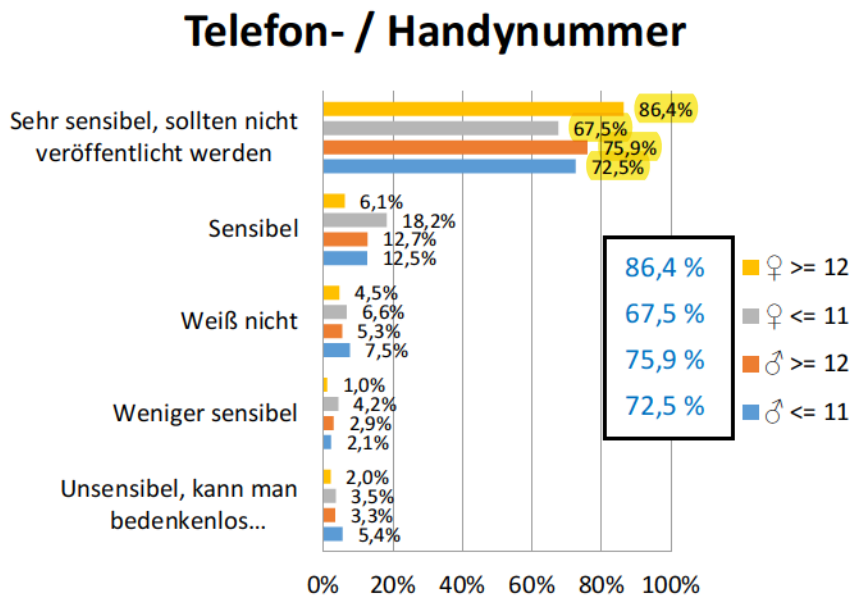


Abb. A4.10-6

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Mehrheitlich (mit rund 90 %) wird die E-Mail-Adresse als sensibel gesehen, wobei aber auch knapp 1/4 der älteren Jungen es nicht einschätzen können. Etwas vorsichtiger mit dieser Information sind die Mädchen als die Jungen, und auch die Jüngeren gegenüber den Älteren.

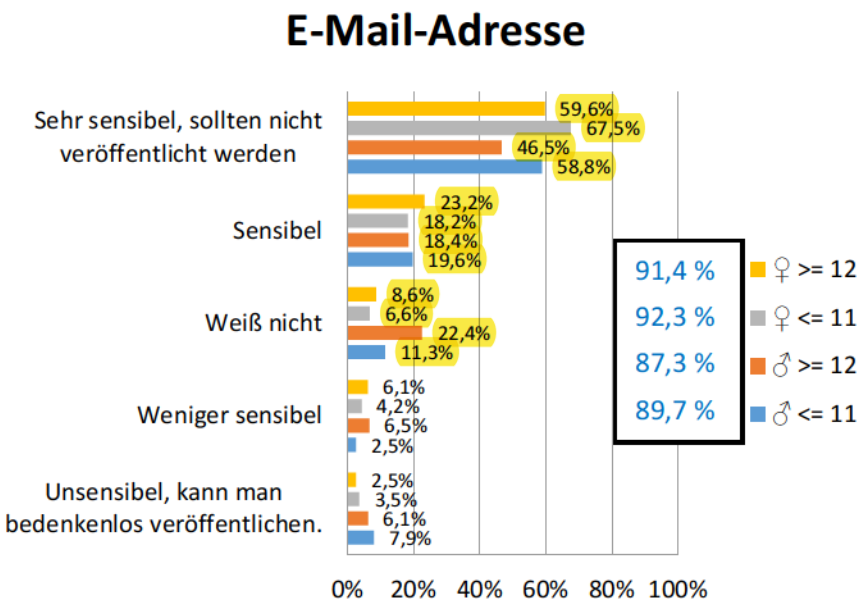


Abb. A4.10-7

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Gerade die Jüngeren sehen mit deutlich mehr als die Hälfte der Befragten Fotos für sehr kritisch an, während die Älteren es etwas lockerer sehen. Insgesamt wird es eher als sensibel betrachtet, wobei wieder die älteren Jungen sich mit einer Einschätzung schwertun. Insgesamt sind innerhalb der Altersgruppe kaum geschlechterspezifische Unterschiede diagnostizierbar.

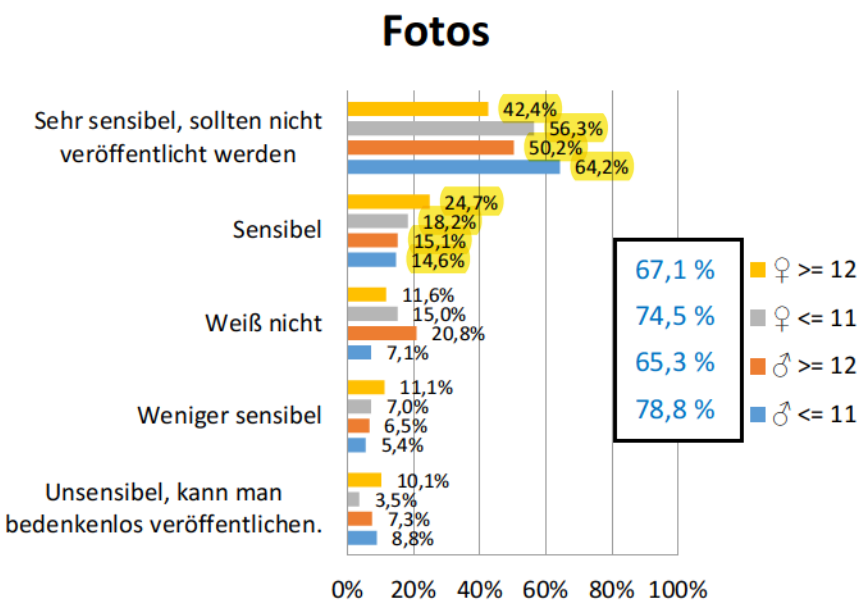


Abb. A4.10-8

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Veröffentlichte Kontakte halten die Mädchen für sensibler als Jungen, wobei aber die Mehrheit Kontakte als klar sensibles Datum einstuft. Altersspezifisch kann in der Geschlechtergruppe kein großer Unterschied festgestellt werden.

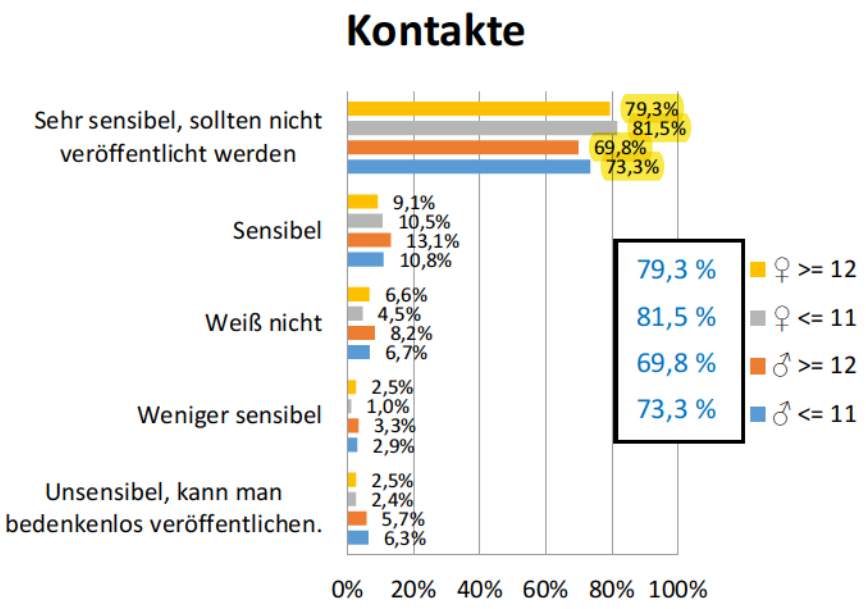


Abb. A4.10-9

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Mit 44 % halten die älteren Schüler – unabhängig vom Geschlecht – Lieblingsfilme usw. für unsensibel. Jedoch sind die Jüngeren kritischer und die jüngeren Mädchen halten es eher für sensibel (64 %). Der Anteil der Unentschlossenen liegt zwischen 17 % und 20 %.

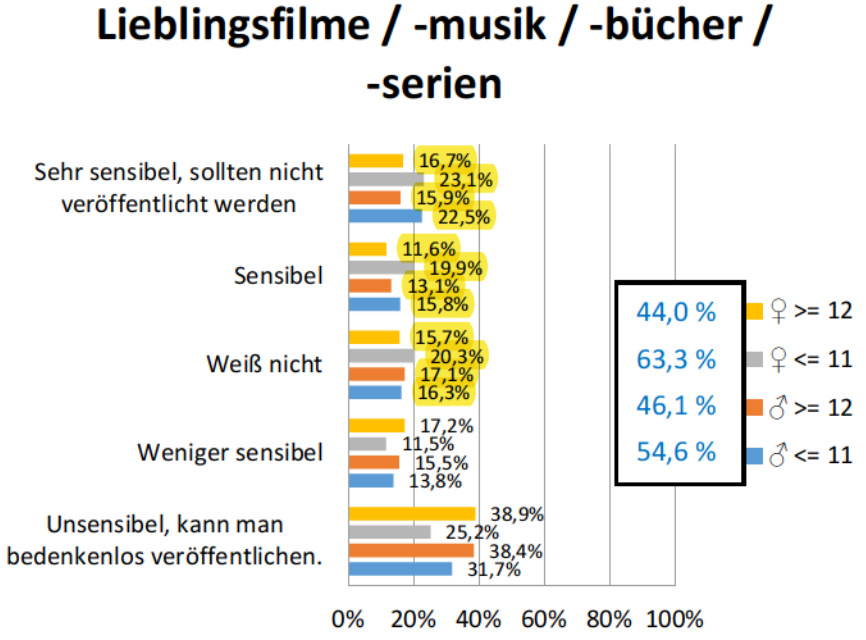


Abb. A4.10-10

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Mit knapp 50 % werden – unabhängig von Altersklasse und Geschlecht – die Interessen als unsensibel angesehen, wobei die älteren Mädchen noch am unkritischsten mit gut 50 % sind. Die Jüngeren, insb. die jüngeren Mädchen, sind eher etwas vorsichtiger als die Älteren.

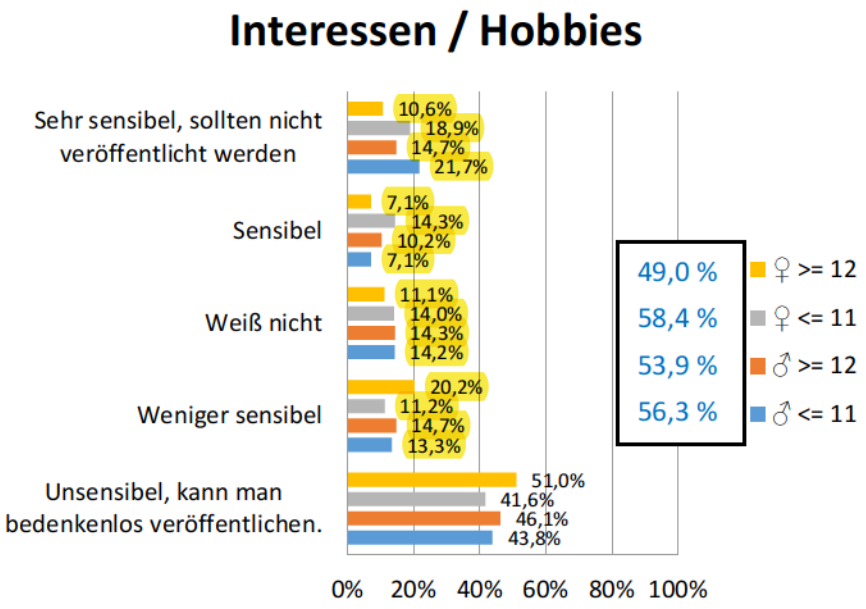


Abb. A4.10-11

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Rund die Hälfte hält die Angabe von Lieblingsorten für sehr sensibel bzw. sensibel, wobei die Jüngeren kritischer sind. Unabhängig von Alter und Geschlecht sind sich rund 20 % unsicher. Rund 1/3 steht der Angabe eher unkritisch gegenüber. Ein geschlechterspezifischer Unterschied kann nicht ausgemacht werden.

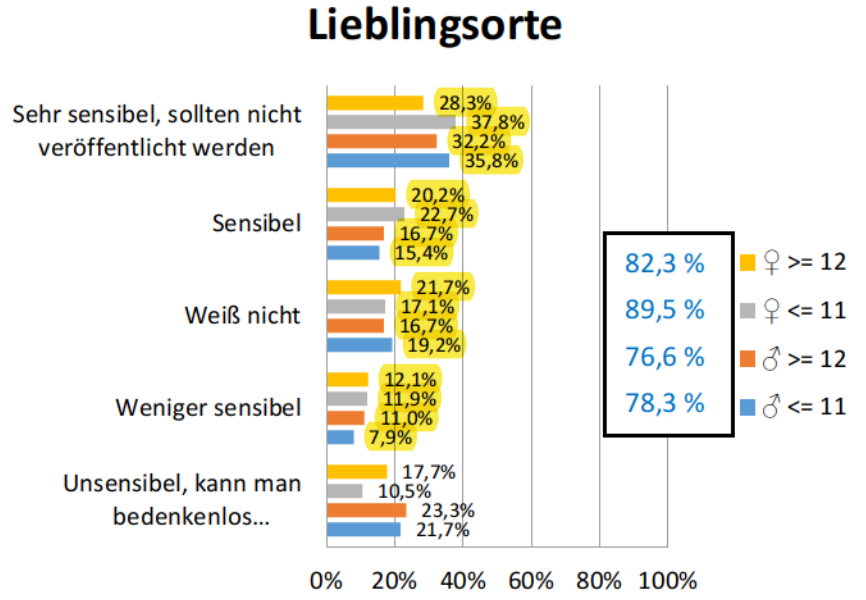


Abb. A4.10-12

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Während die Älteren unabhängig vom Geschlecht mit knapp der Hälfte die Sensibilität erkennen, sind die Jüngeren, v. a. die Mädchen, vorsichtiger, in dem was sie mitteilen.

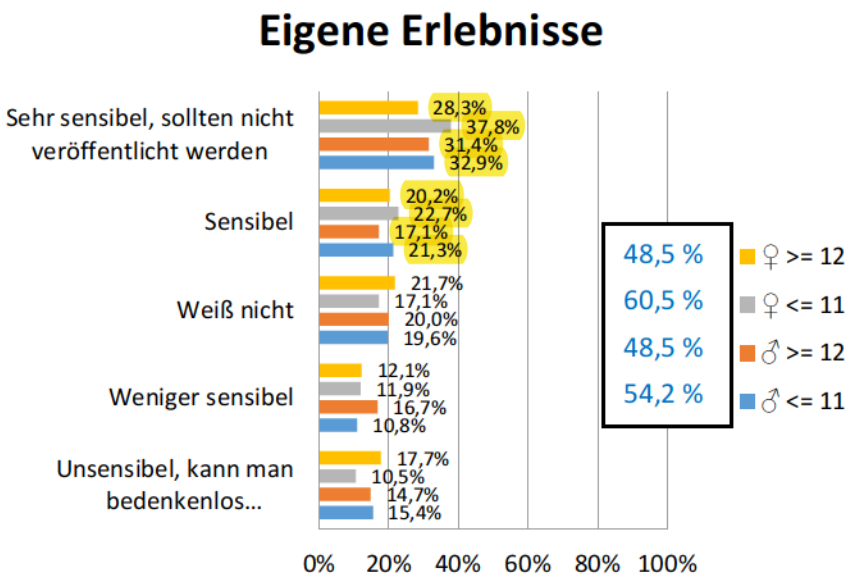


Abb. A4.10-13

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Dass eigene Gedanken usw. deutlich sensibler als Lieblingsorte und eigene Erlebnisse sind, bestätigen rund 80 % der Schüler, wobei die Jüngeren deutlich vorsichtiger sind. Bemerkenswert ist, dass die Mädchen mitteilungsbedürftiger als die Jungen sind, was deutlicher in der Gruppe der Älteren statt der Jüngeren auszumachen ist.

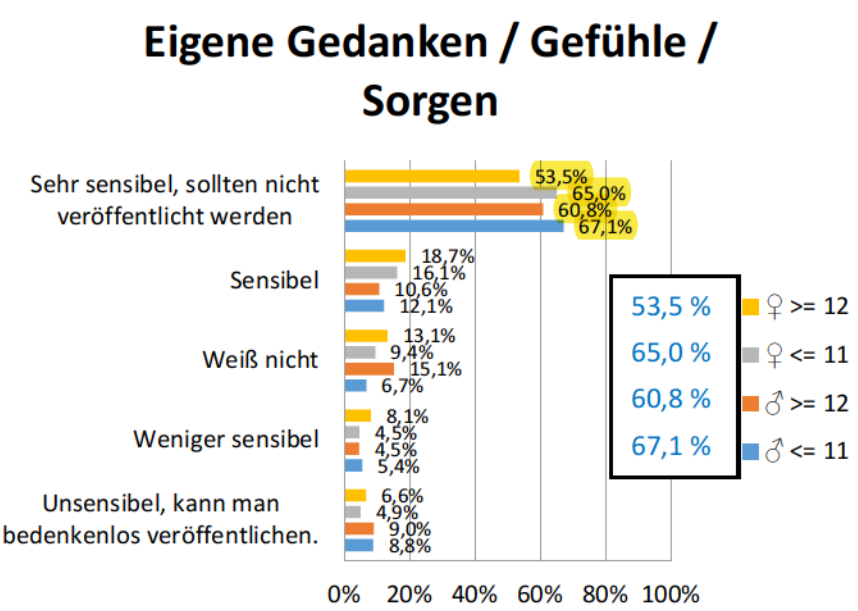


Abb. A4.10-14

Wie sensibel sind folgende Daten, um sie in Sozialen Netzwerken NICHT zu veröffentlichen? [A2; *RK*]

Die Angabe der Religion halten mit deutlichem Abstand die jüngeren Jungen für sehr kritisch (46 %), während die anderen Klassen die Sensibilität der Angabe mit rund 1/3 einstufen. Jeder Fünfte ist sich unsicher und rund 1/3 hält die Religion für ein weniger sensibles bzw. unsensibles Datum. Insgesamt sind die Jungen vorsichtiger als die Mädchen.

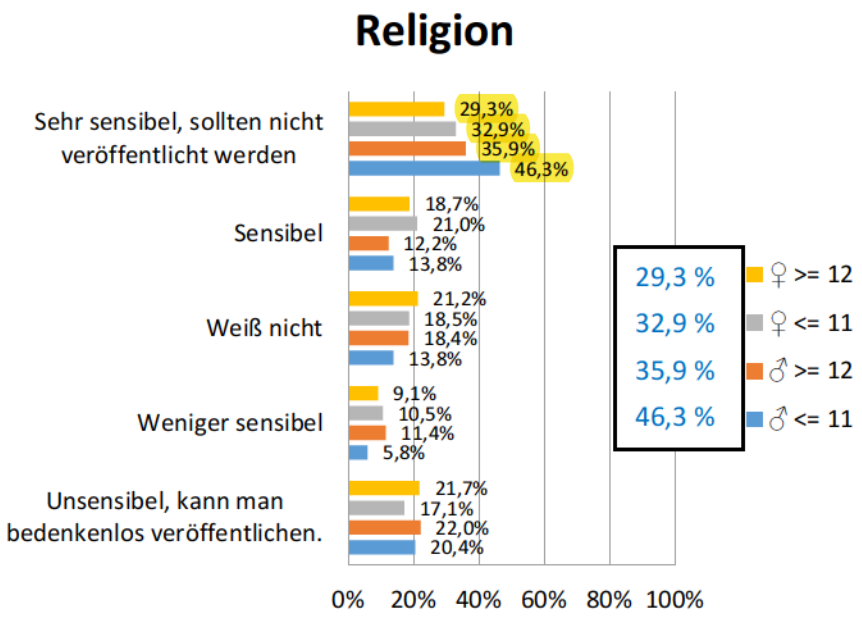


Abb. A4.10-15

Zusammenfassung zu Frage A2:

Die Antworten auf die erste Frage nach der Sensibilität von Daten zur Veröffentlichung in Sozialen Netzwerken lassen kein eindeutiges Bild oder keine eindeutige Tendenz in Bezug auf Alter oder Geschlecht erkennen. Je nach Item sind die Einschätzungen unterschiedlich. Ganz grob lässt sich aber erkennen, dass die Gruppe der Mädchen einerseits und die Gruppe der jüngeren Probanden andererseits bei der Angabe von persönlichen Daten eher zurückhaltender und vorsichtiger sind.

Hast Du die Privatsphäreeinstellungen im Sozialen Netzwerk geändert bzw. würdest Du sie ändern?
[B1/B2; *UK*]

Keine Änderungen nehmen eher die jüngeren Probanden – 63 % bei den Jungen und 56 % bei den Mädchen – vor als bei den älteren (54 % die Jungen und 41 % die Mädchen). Vergleicht man die Geschlechter miteinander, so vertrauen die Jungen den Anbietern eher als die Mädchen, die deutlich vorsichtiger sind. Diese Differenz zwischen den Geschlechtern ist bei den Älteren mit rund 13 % größer als bei den Jüngeren (8 %).

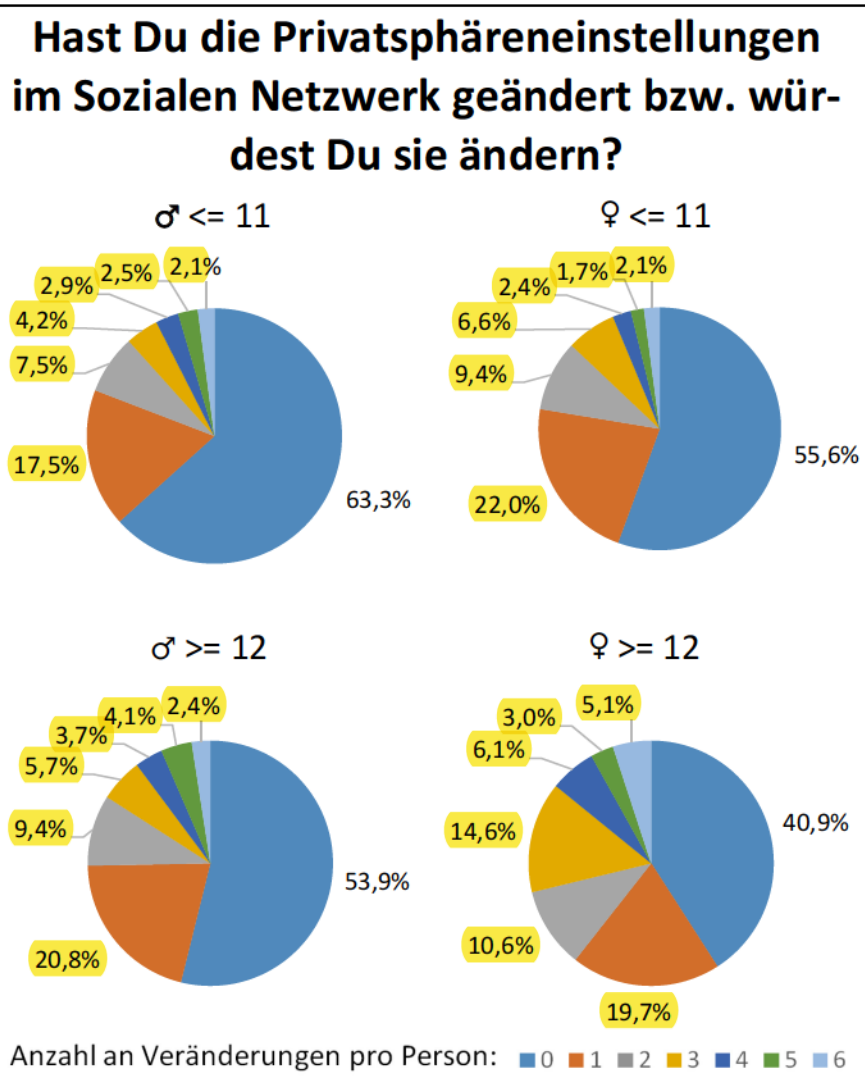


Abb. A4.10-16

Hast du die Privatsphäreneinstellungen im Sozialen Netzwerk geändert bzw. würdest Du sie ändern? Wenn ja, welche?
[B1+B2; *UK*]

Während die jüngeren Schülerinnen und Schüler eher nichts ändern und auch die Jungen dazu tendieren, dem Anbieter zu vertrauen, sind es insbesondere die älteren Mädchen mit gut 2/3, die Änderungen in den Einstellungen vornehmen.
Rund 1/4 der älteren Jungen und knapp 20 % der älteren Mädchen achten auf die Sichtbarkeit des eigenen Profils innerhalb des Netzwerks, während die anderen Gruppen diesen Aspekt weniger deutlich bewerten. Sichtbarkeit außerhalb des Netzwerks und die Sichtbarkeit von Posts liegt bei rund 15 %. Die Tatsache, Anderen das Posten auf der eigenen Seite zu ermöglichen, wird von den Älteren eher eingestellt als von den Jüngeren. Die Kontaktaufnahme durch Andere wird stärker von den Mädchen kontrolliert als die Möglichkeit, im Netz gefunden zu werden, wobei sie sich von den Jungen etwas kritischer abheben.

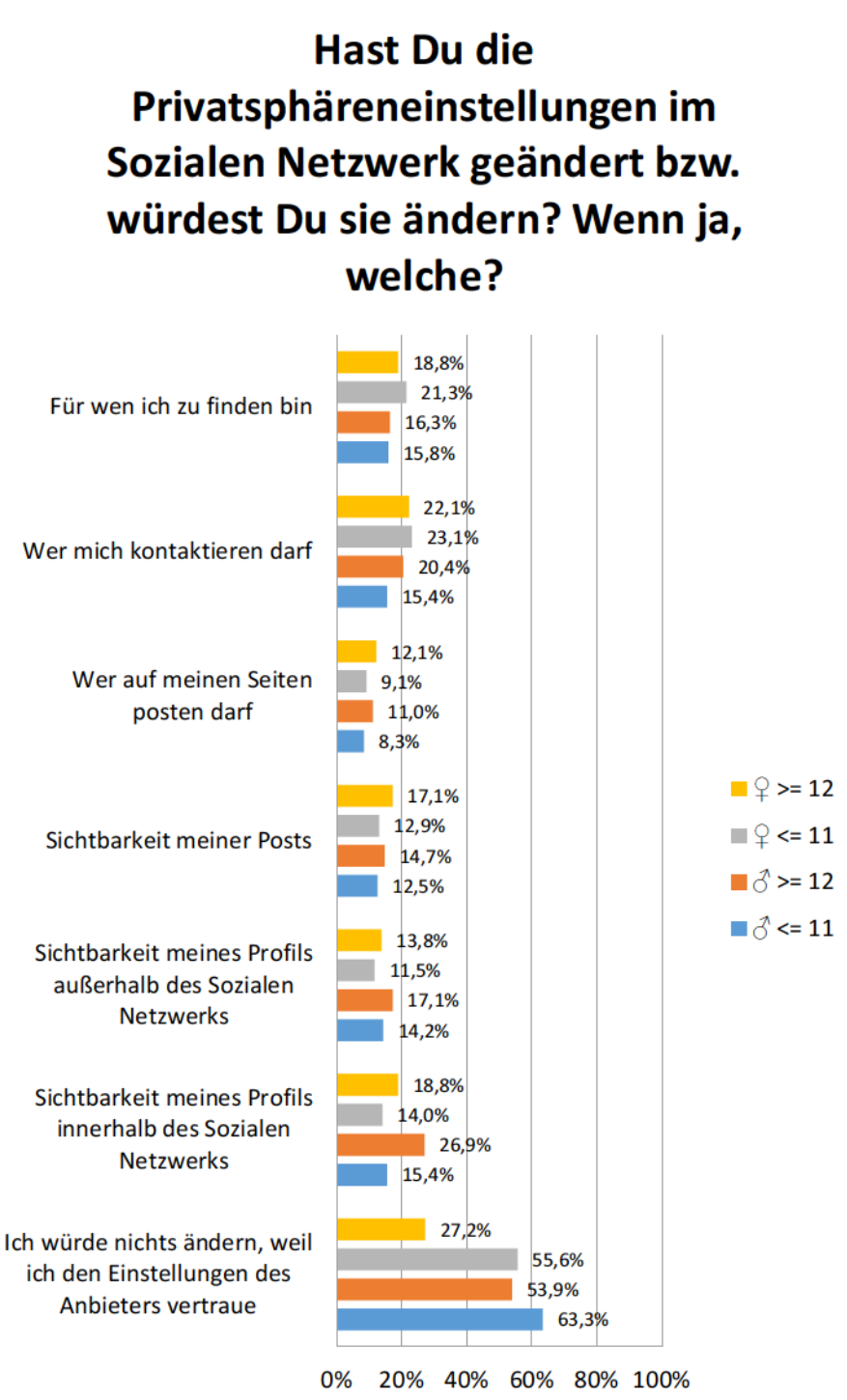


Abb. A4.10-17

Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [B3/4(a); *HK*]

Gut 90 % der Mädchen und rund 83 % der Jungen zeigen das erwünschte Verhalten, wobei die jüngeren Mädchen noch ein wenig vorsichtiger als die älteren sind; bei den Jungen ist es genau umgekehrt. Nur für einen verschwindend geringen Teil von rund 7 % bei den Jungen und 3 % bei den Mädchen tritt Desinteresse ein. Immerhin 5 % sind unentschieden, wobei der Anteil der Jungen über dem der Mädchen liegt.

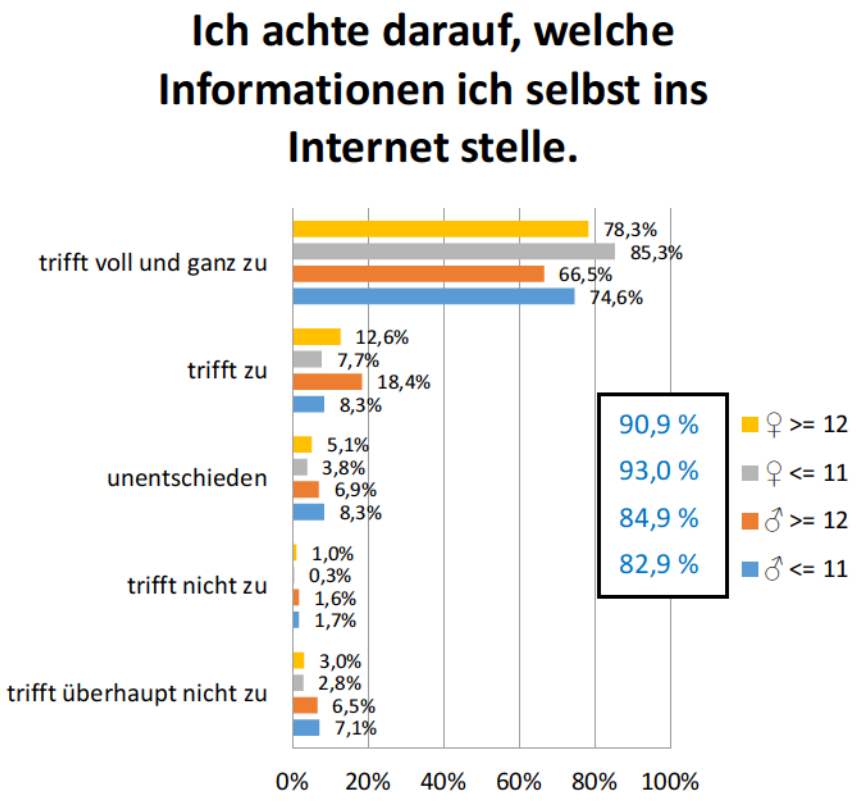


Abb. A4.10-18

Jetzt geht es um Informationen, die andere über Dich im Internet finden können. Wie sehr treffen die folgenden Aussagen auf Dich persönlich zu? [B3/4(c); U*K*]

Rund 85 % der Mädchen, aber nur 71 % der Jungen ist das Bestimmungsrecht wichtig. Unentschieden sind rund 10 %, hier v. a. eher die Jungen. Während der Mädchenanteil mit knapp 5 % das unerwünschte Verhalten zeigt, sind die Jungen mit einem rund dreifachen Anteil (im Vergleich zu den Mädchen) hier unvorsichtiger. Während bei den Jungen das Alter keine Rolle spielt, sind die jüngeren Mädchen vorsichtiger als die älteren Mädchen.

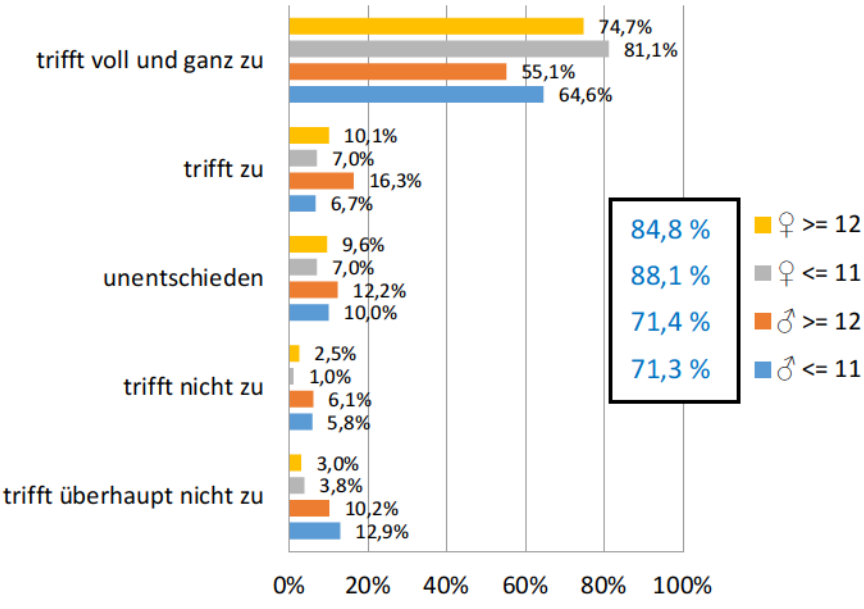


Abb. A4.10-19

Die älteren Jungen verteilen sich relativ gleichmäßig auf richtige, falsche Antworten und Ahnungslosigkeit. Insbesondere die Mädchen wissen die Begriffe nicht einzuordnen, wobei die jüngeren Schülerinnen stärker als die älteren davon betroffen sind. Auch bei den Jungen ist das Wissen der Älteren größer als das der Jüngeren. Wenn Antworten gegeben werden, dann ist der Anteil der falschen Antworten höher als der Anteil der korrekten Antworten mit Ausnahme bei den älteren Jungen. Insgesamt sind die Jungen besser als die Mädchen und die älteren Teilnehmer besser als die jüngeren.

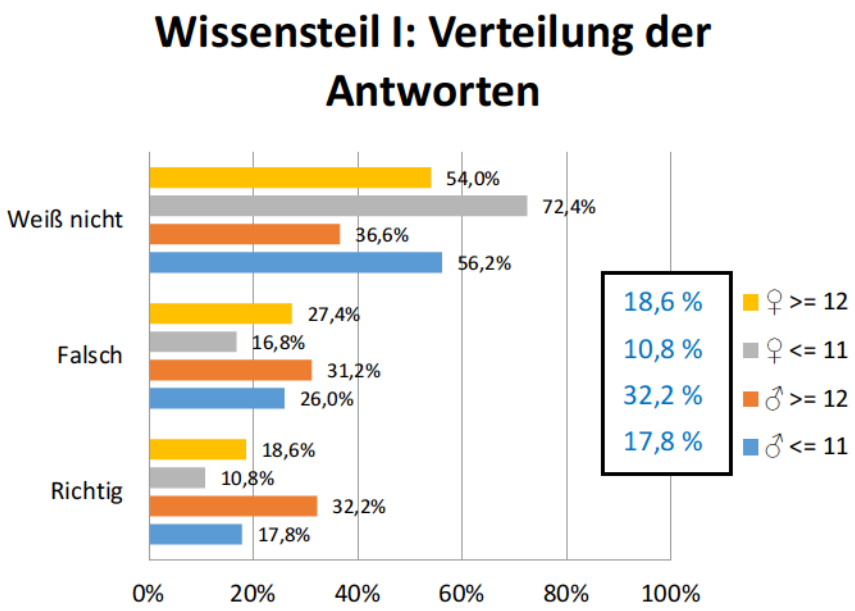


Abb. A4.10-20

Im Gegensatz zu Abbildung A4.10-20, in der der prozentuale Anteil aller gegebenen Antworten dargestellt ist, ist in dieser Abbildung der sich auf die Schüler beziehende Anteil zu sehen.
Vor allem die jüngeren Teilnehmer (Mädchen 58 %, Jungen 50 %) können keine Frage korrekt beantworten. Bei den Älteren ist der Wert der Mädchen etwas geringer (46 %). Eine richtige Antwort wird unabhängig von Alter und Geschlecht von rund 30 % gegeben. Mit 1/4 hebt der Wert für zwei korrekte Antworten bei den älteren Jungen von den Anderen (im Schnitt 10 % bis 13 %) deutlich ab. Bei einer größeren Anzahl an korrekten Antworten nimmt die Anzahl in allen Fällen immer weiter ab, wobei aber immer die älteren Jungen die Spitze der Gruppe bilden. Der Gesamteindruck aus Abbildung A4.10-20 wird bestätigt.

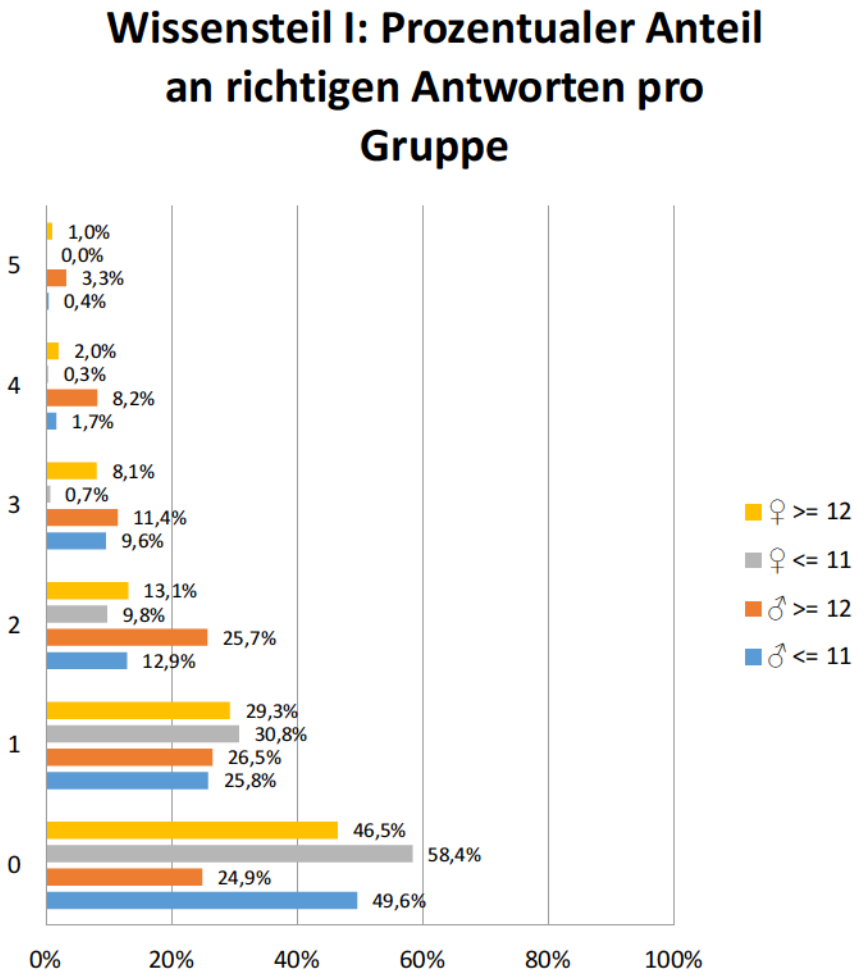


Abb. A4.10-21

Bei der Einordnung von Aussagen schneiden die älteren Schüler (jeweils über 40 %) deutlich besser als die jüngeren ab, wobei aber in dieser Altersklasse die Jungen einen kleinen Vorsprung gegenüber den Mädchen haben. Insgesamt nimmt der Anteil der Ahnungslosen gegenüber den Fachbegriffsfragen ab (Ausnahme die älteren Jungen), der bei den Jüngeren aber um die 50 % liegt. Im Bereich der falschen Antworten sind die Älteren mit rund 20 % ungefähr gleich auf, die jüngeren Jungen bei rund 18 %, während es bei den jüngeren Mädchen 12 % sind.

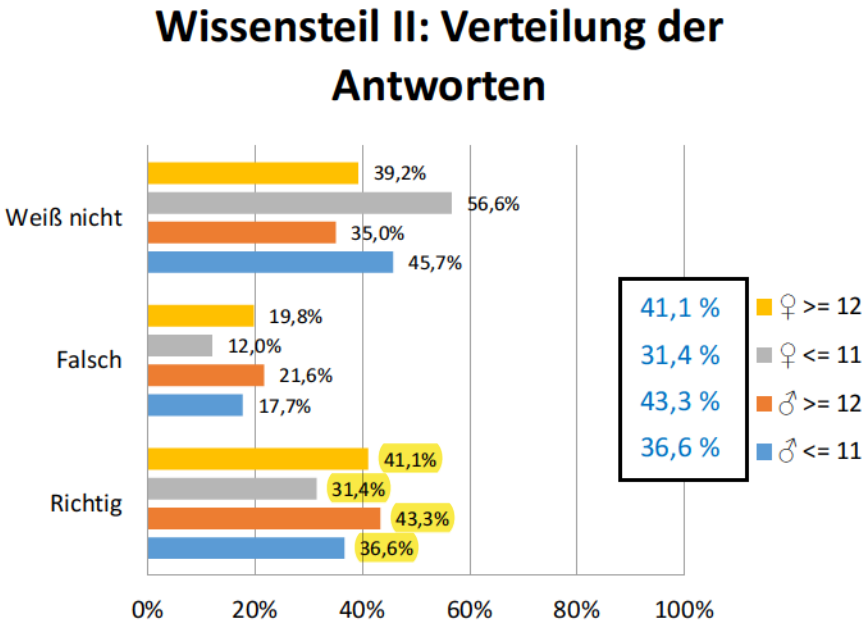


Abb. A4.10-22

Im Gegensatz zu Abbildung A4.10-22, in der der prozentuale Anteil aller gegebenen Antworten dargestellt ist, ist in dieser Abbildung der sich auf die Schüler beziehende Anteil zu sehen.
Betrachtet man den Anteil an korrekten Antworten, so werden im Schnitt zwei bis drei gegeben. Wiederum ist auffällig, dass ab drei korrekten Antworten die älteren Schüler besser als die jüngeren abschneiden. Ein deutlich geschlechterspezifischer Unterschied ist nicht auszumachen, wobei im unteren Teil (eine oder zwei korrekte Antworten) die Mädchen besser abschneiden. Nur falsche Antworten geben 4 % mehr älteren Jungen statt älteren Mädchen ab.

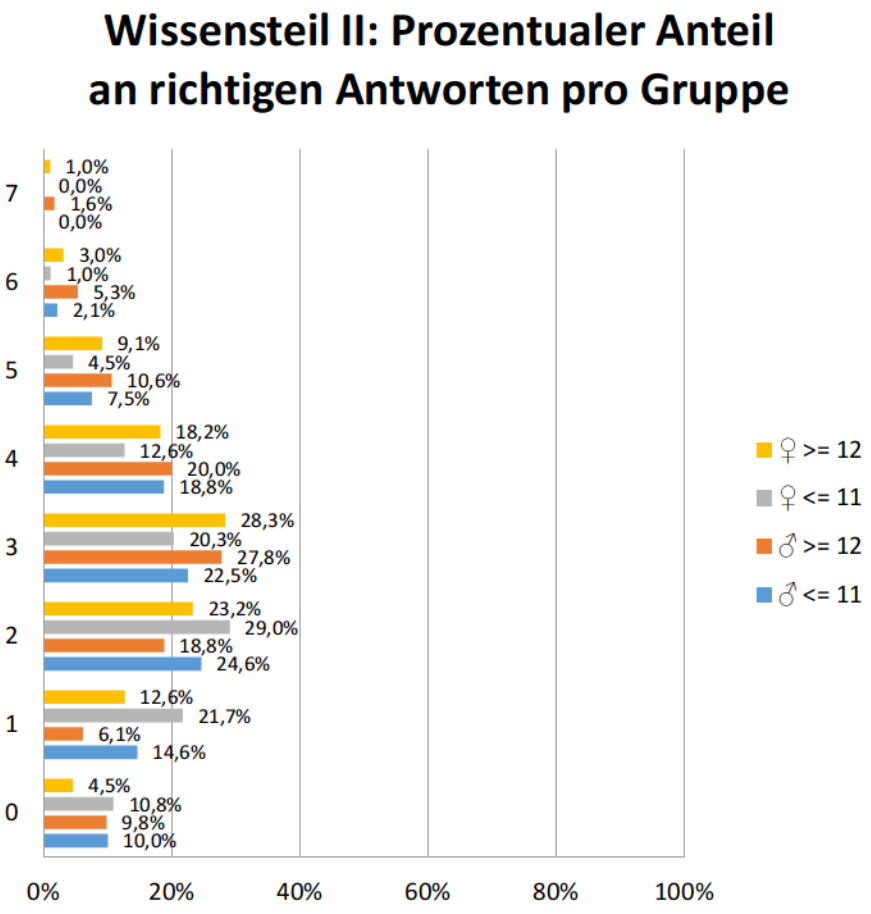


Abb. A4.10-23

Was sind für dich Risiken im Internet? [F1; *RK*]

Die unerwünschte Weitergabe persönlicher Daten wird alters- und geschlechtsunabhängig von einer deutlichen Mehrheit (zwischen 57 % und 68 %) als sehr hohes Risiko eingestuft, wobei jedoch bei den Mädchen die Differenz der Altersklassen deutlich ist (rund 10 %) und die jungen Mädchen es riskanter ansehen, während die Jungen beieinander liegen. Mit jeweils rund 20 % wird es von allen als mittleres Risiko eingestuft.

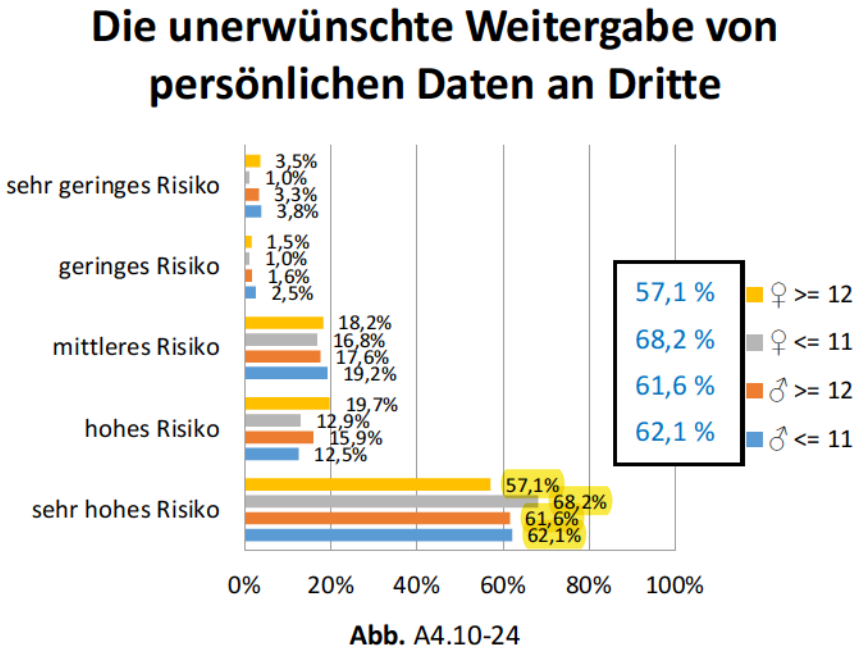


Abb. A4.10-24

Was sind für dich Risiken im Internet? [F1; *RK*]

Ein ähnliches Bild wie die Weitergabe persönlicher Daten gilt auch für das Ausspionieren persönlicher Daten, jedoch die Gruppe der jüngeren Jungen ist hier gleichauf mit der Gruppe der jüngeren Mädchen und hebt sich damit von den älteren Jungen ab.

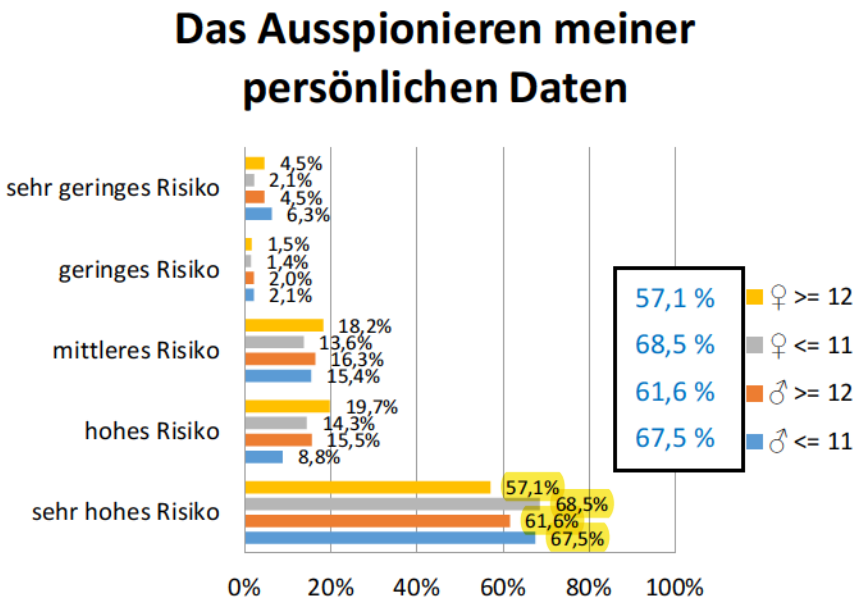


Abb. A4.10-25

Was sind für dich Risiken im Internet? [F1; *RK*]

Für rund 28% der Älteren und 37 % der Jüngeren stellt der Empfang von Spam-Mails ein sehr hohes Risiko dar, wobei insbesondere die jüngeren Teilnehmer – und hier die Mädchen – es riskanter beurteilen. Ebenfalls rund 30 % sehen es als mittleres Risiko an und nur rund 10 % bei den Jungen und nur rund 5 % bei den Mädchen kaum ein Risiko dahinter erkennen. Ältere Jungen sehen somit ein vergleichsweises schwächeres Risiko in den Spam-Mails als die Mädchen und die Jüngeren sind risikobewusster.

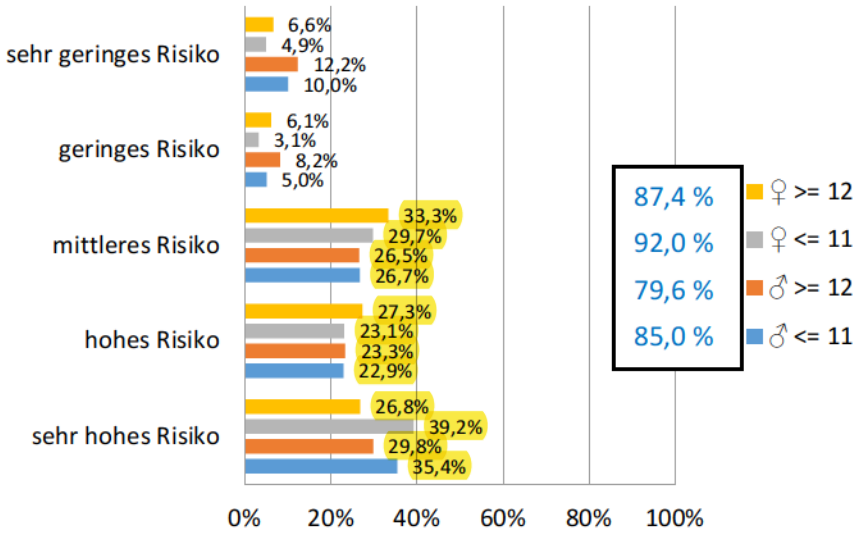


Abb. A4.10-26

Was sind für dich Risiken im Internet? [F1; *RK*]

Hinter Beleidigungen und Belästigungen nehmen rund die Hälfte ein Risiko wahr, wobei die Jüngeren und hier insb. die Mädchen es stärker einschätzen. Als hohes und mittleres Risiko wird es jeweils – unabhängig von Alter und Geschlecht – mit je rund 20 % eingeschätzt. Nur 10 % der älteren Jungen sehen ein geringes Risiko in den Beleidigungen und Belästigungen. Insgesamt finden die Jüngeren es riskanter als die Älteren, und auch die Mädchen sehen ein höheres Risiko als die Jungen.

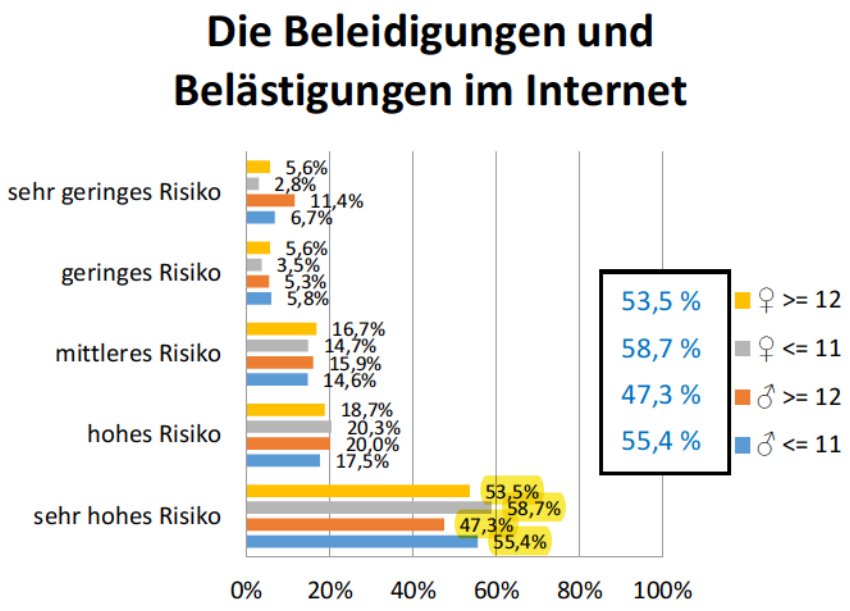


Abb. A4.10-27

Was sind für dich Risiken im Internet? [F1; *RK*]

Ein ähnliches Bild wie die persönliche Weitergabe und das Ausspionieren persönlicher Daten gilt für den Versand unerwünschter E-Mails im eigenen Namen. Zwischen 64 % und 75 % der Teilnehmer sehen ein Risiko darin, wobei die Jungen altersunabhängig gleich auf sind, sind die jüngeren Mädchen zwar mit den Jungen gleich, übertreffen um 10 % aber die älteren Mädchen. Diese sehen mit 23 % ein mittleres Risiko in dem Mailversand.

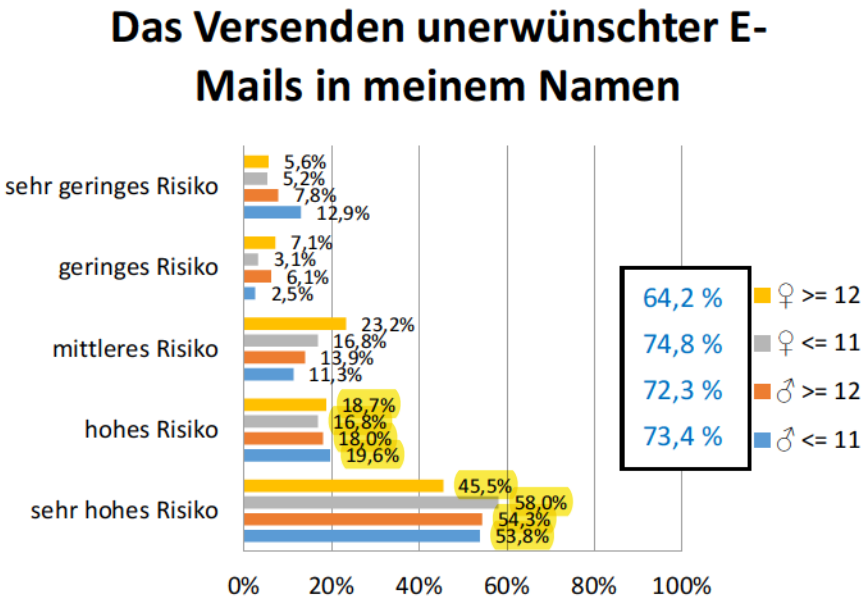


Abb. A4.10-28

Was sind für dich Risiken im Internet? [F1; *RK*]

Während der Anteil der jüngeren Teilnehmer in dem Wissen über Tätigkeit oder Aufenthaltsort das Risiko etwas höher als bei den älteren einschätzt, so sieht insgesamt rund die Hälfte und auch etwas mehr der Schüler in der Tatsache ein sehr hohes Risiko. Als hohes oder mittleres Risiko wird es im Verhältnis eher von den älteren als den jüngeren Teilnehmern wahrgenommen. Bei den Älteren sind auch hier die Jungen vorsichtiger als die Mädchen.

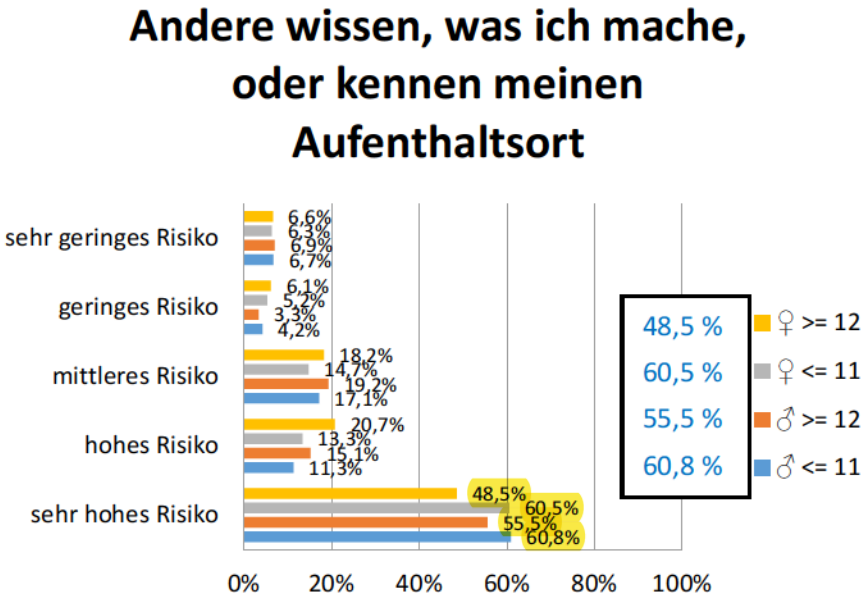


Abb. A4.10-29

Was sind für dich Risiken im Internet? [F1; *RK*]

Insbesondere die Jüngeren, und hier vorrangig die Mädchen, sehen in der Veröffentlichung peinlicher Fotos usw. ein sehr hohes Risiko, wobei insgesamt gut 60 % darin ein Problem wahrnehmen. Ein hohes und mittleres Risiko wird mit rund 15 % verstärkt von den älteren statt den jüngeren Teilnehmern gesehen. Geschlechterspezifische Unterschiede sind nicht deutlich messbar.

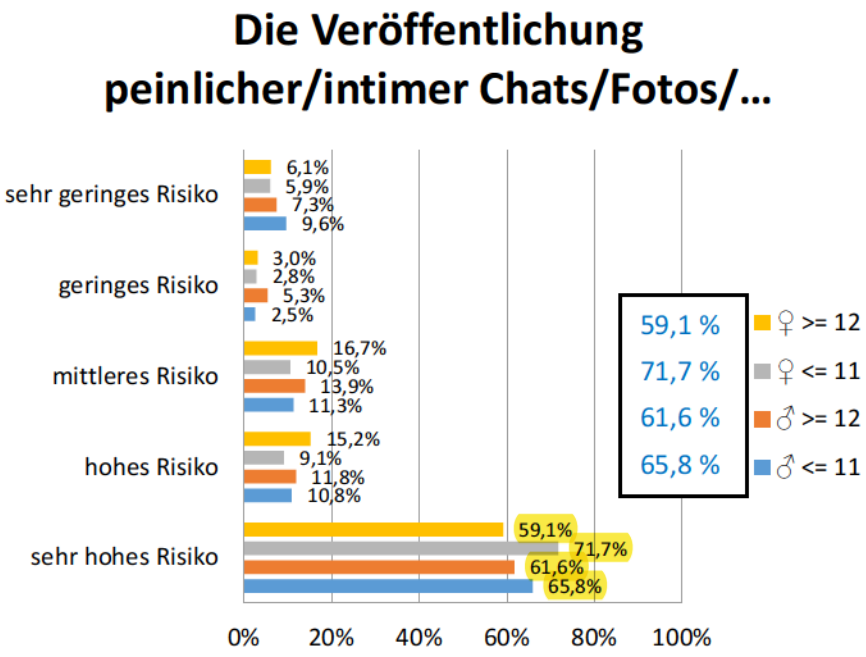


Abb. A4.10-30

Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? [G1; *ANK*]
Ich nutze …

Die Nutzung eines Adblockers wird vor allem von den Älteren und hier den Jungen genannt, wobei die älteren Mädchen und jüngeren Jungen ungefähr gleich auf sind. Die deutliche Mehrheit (mit z. T. über 50 %) von Mädchen und den jüngeren Jungen wissen von der Nutzung nichts. Auch der Anteil der älteren Jungen, die es nicht wissen, ist größer als der Anteil derer, die ihn nutzen. Während rund 40 % der älteren Jungen wissen, dass sie ihn nicht nutzen, ist der Anteil der anderen Nichtnutzer bei allen rund 30 %. Insgesamt sind es v. a. die Älteren und unter den Geschlechtern v. a. die Jungen, die einen Adblocker nutzen.

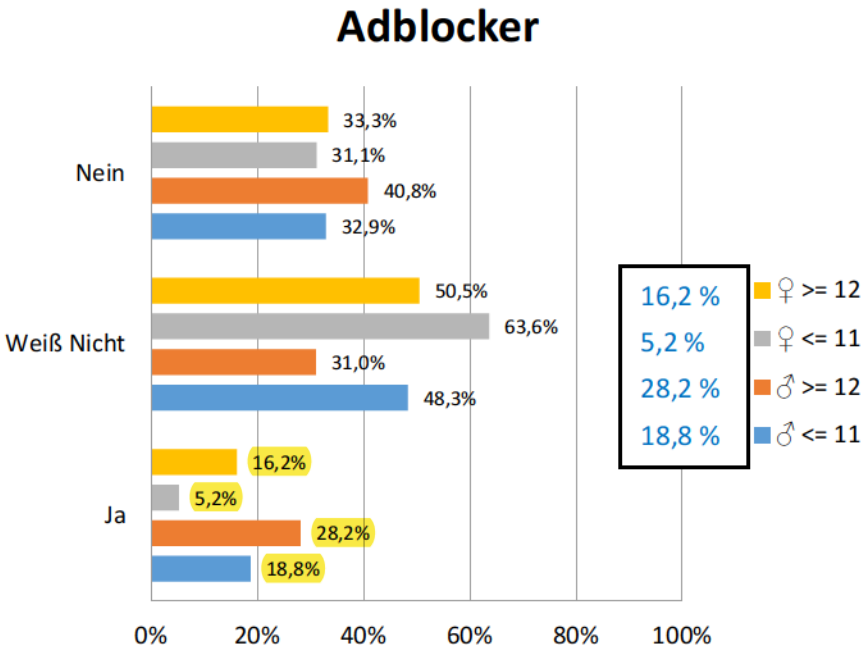


Abb. A4.10-31

Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? [G1; *ANK*]
Ich nutze …

Während ungefähr der Anteil derer, die nicht wissen, ob sie eine Firewall einsetzen, ähnlich dem zu Adblocker ist, wissen mit deutlichem Abstand knapp die Hälfte der älteren Jungen, dass sie eine Firewall nutzen. Auch die jüngeren Jungen setzen sie mit 27 % – und damit höher als die älteren Mädchen (18 %) – ein. Bei den Mädchen ist der Einsatz ähnlich wie beim Adblocker. Der Anteil der Nichtnutzer beträgt bei den Mädchen rund 30 % und bei den Jungen rund 25 %. Insgesamt setzen mehr Jungen die Firewall als die Mädchen ein und innerhalb der Geschlechtergruppen die Älteren mehr als die Jüngeren.

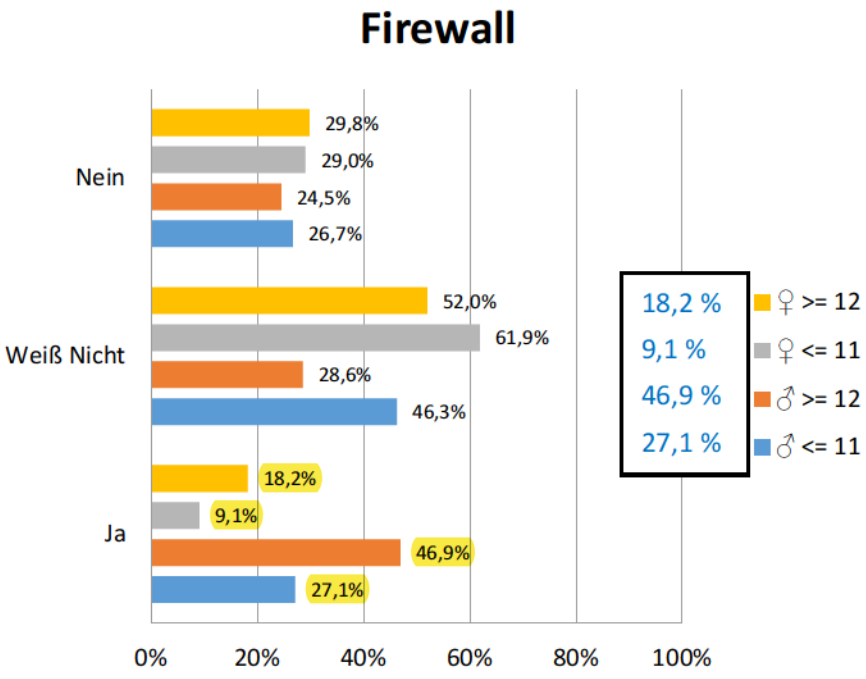


Abb. A4.10-32

Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? [G1; *ANK*]
Ich nutze …

Unabhängig von Alter und Geschlecht nutzen rund 30 % eine Verschlüsselungssoftware, wobei der Anteil der älteren Mädchen höher ist. Während die Mehrheit von der Nutzung nichts weiß, ist der Anteil der jüngeren Mädchen deutlich höher als in den anderen Gruppen. Dass keine Verschlüsselung angewandt wird, wissen mit deutlicher Mehrheit von gut 40 % die älteren Jungen. In diesem Fall sind die Mädchen vorsichtiger und nutzen Verschlüsselung gegenüber den Jungen. Im Altersvergleich sind die älteren Mädchen etwas stärker vertreten.

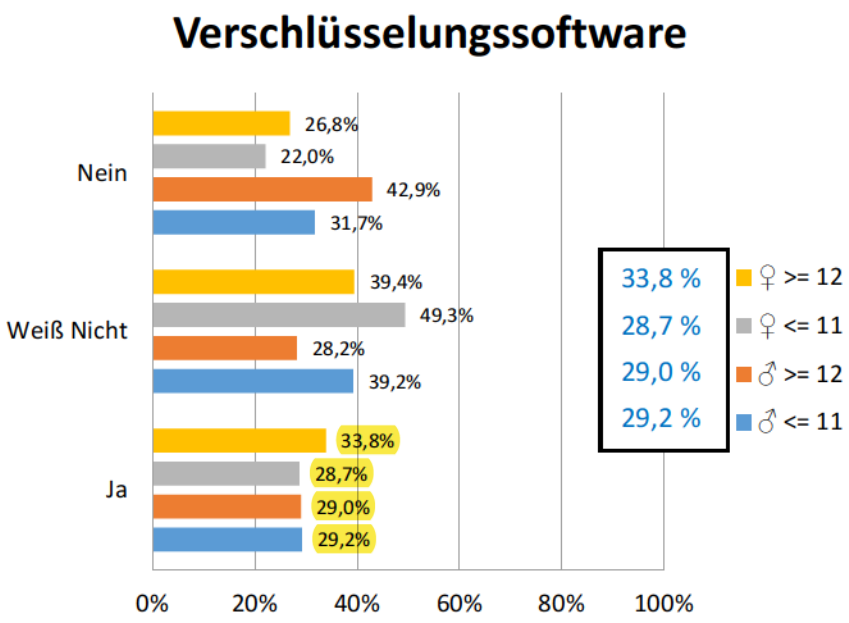


Abb. A4.10-33

Welche technischen Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? [G1; *ANK*]
Ich aktualisiere regelmäßig meine …

Die Aktualisierung von Anti-Viren-Software wird v. a. von den älteren Jungen bestätigt (60 %), während die älteren Mädchen und die jüngeren Jungen mit rund 45 % ungefähr gleich auf sind. Dementsprechend ist die Gruppe der jüngeren Mädchen auch die größte, die nicht weiß, ob sie die Anti-Viren-Software aktualisiert. Rund 20 % über alle Gruppen hinweg aktualisiert die Anti-Viren-Software nicht. Insgesamt achten die Jungen deutlicher als die Mädchen auf die Aktualität der Software. Im Vergleich zu den anderen Fällen ist dieser Anteil höher.

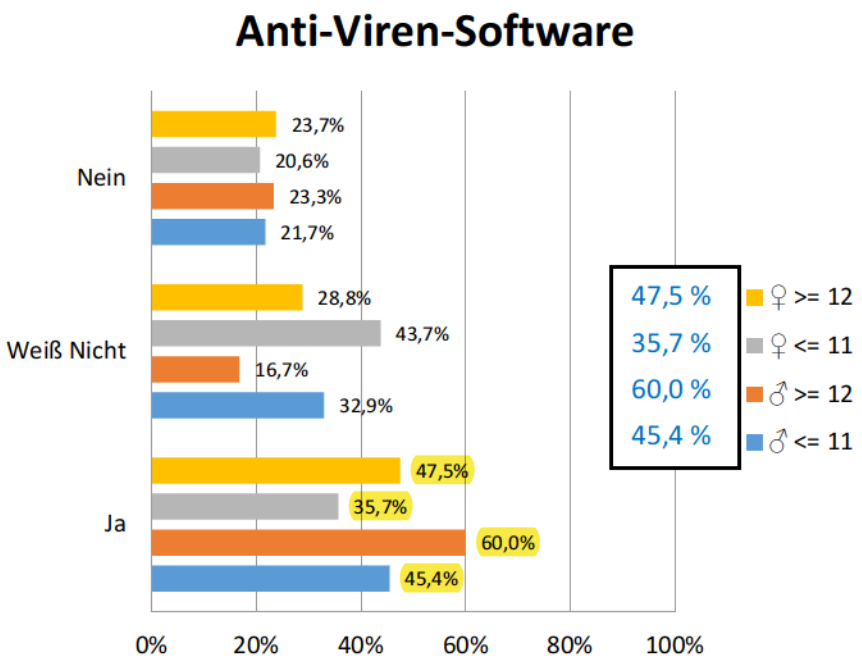


Abb. A4.10-34

Wie sehr treffen folgende Aussagen auf dich zu? (negativ) [H1; *UK*]

Ein unüberlegtes Anklicken eines Werbebanners kommt unabhängig von Alter und Geschlecht für 60 % der älteren und rund 54 % der jüngeren Teilnehmer nicht infrage. Mit rund 25 % wissen es die Teilnehmer nicht. Knapp 20 % der Befragten sind unvorsichtig. Insgesamt kann bei diesem Item kein deutlicher alters- oder geschlechtsspezifischer Unterschied festgestellt werden, wobei nur die Älteren etwas vorsichtiger sind.

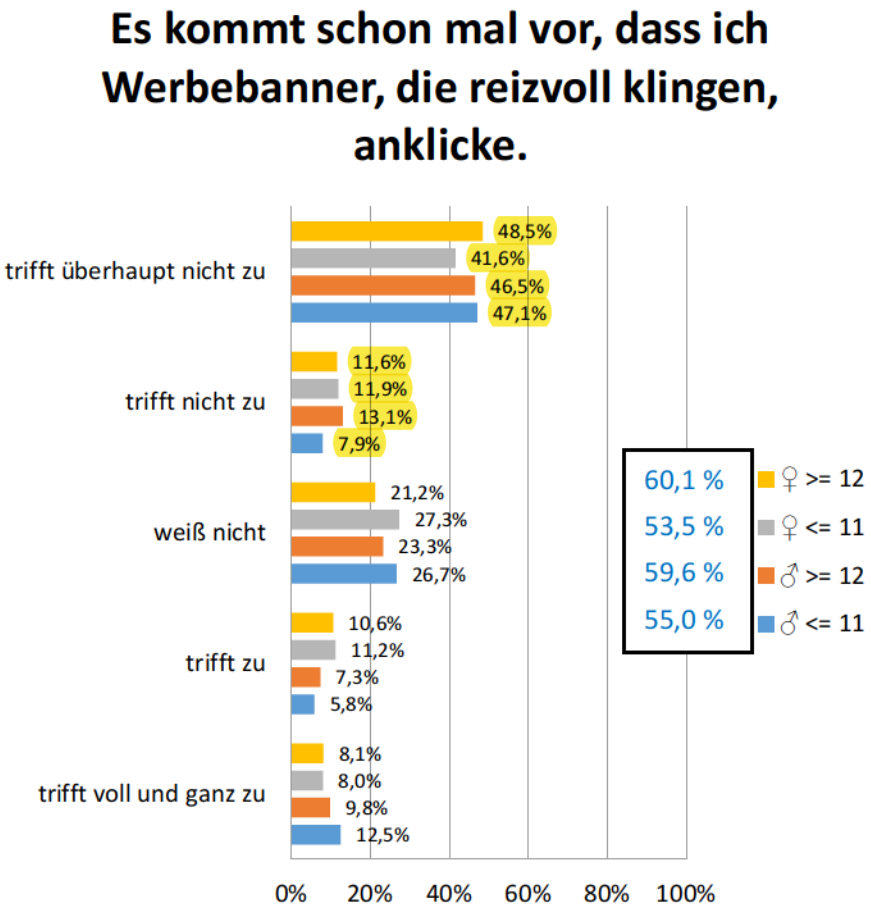


Abb. A4.10-35

Wie sehr treffen folgende Aussagen auf dich zu? (negativ) [H1; *HK*]

Rund 57 % der älteren und zwischen 58 % und 66 % der jüngeren Schüler löschen Spam-Nachrichten sofort, wobei insbesondere die jüngeren Mädchen so reagieren. Rund 25 % ist sich nicht sicher, während weniger als 20 % dies unterlassen (Ausnahme die jüngeren Mädchen nur rund 10 % Anteil). Alters- oder geschlechterspezifische Unterschiede sind nur bei den Jüngeren und dort innerhalb des Geschlechts diagnostizierbar.

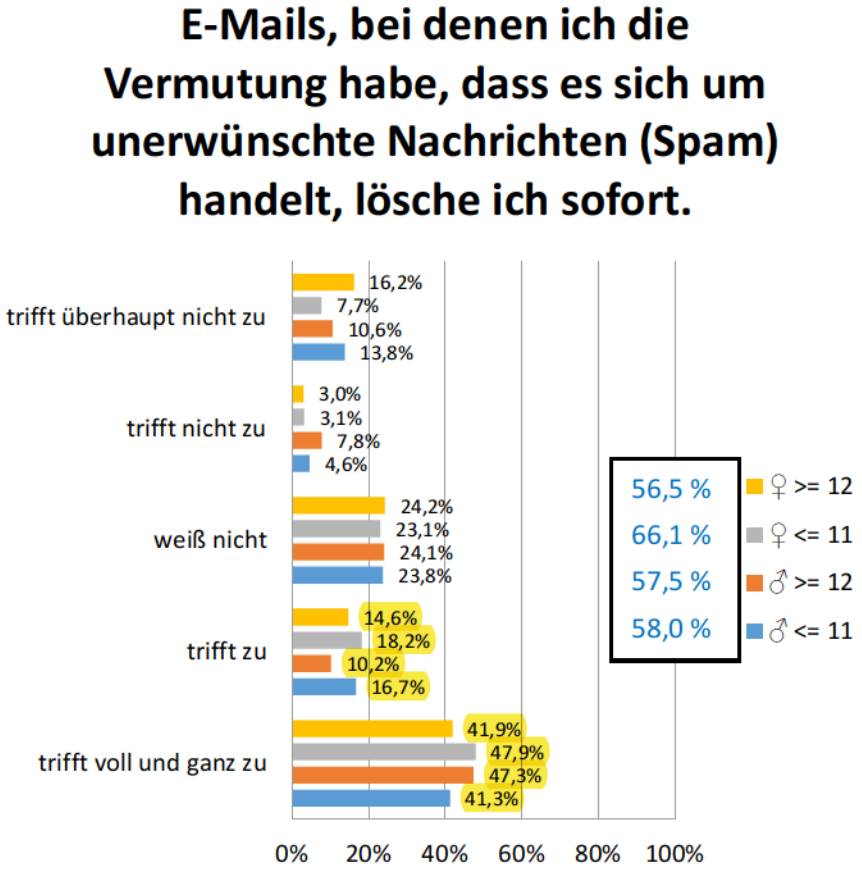


Abb. A4.10-36

Wie sehr treffen folgende Aussagen auf dich zu? (negativ) [H1; *HK*]

Knapp 60 % der Schüler (Ausnahme sind die jüngeren Mädchen mit ca. 44 %) ändern ihre Passwörter nicht in regelmäßigen Abständen. Dies tun nur gut 20 % bzw. bei den jüngeren Mädchen gut 30 %. Etwa 20 % wissen nicht, ob sie es tun. Zwischen Alter und Geschlecht sind keine nennenswerten Unterschiede außer im Fall der jüngeren Teilnehmer beim Geschlecht auszumachen. Wieder sind es die jüngeren Mädchen, die deutlich vorsichtiger als die anderen Gruppen sind.

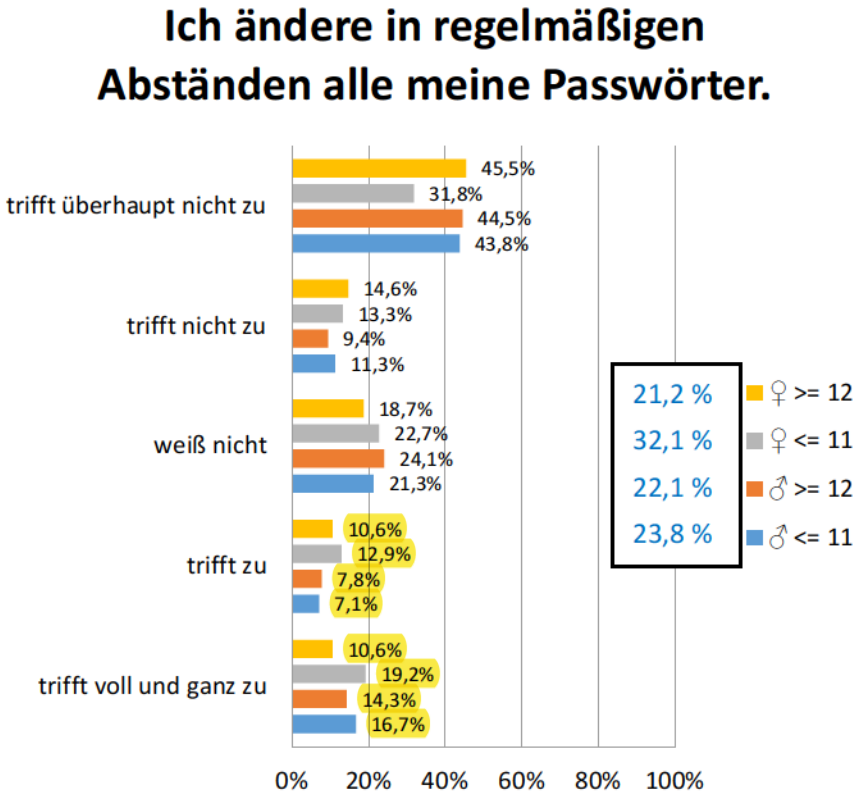


Abb. A4.10-37

Wie sehr treffen folgende Aussagen auf dich zu? (negativ) [H1; *HK*]

Ein deutlicher Anteil von rund 38 % der Mädchen und rund 30 % der Jungen wissen nicht, ob sie ihre Software auf dem neuesten Stand halten. Unter der Jungen sind es unabhängig vom Alter rund 50 %, die es tun, und unter den Mädchen 40 % bei den Älteren, aber nur 36 % bei den Jüngeren. Unter 20 % der Jungen, aber gut über 20 % der Mädchen kümmern sich nicht um eine Software-Aktualisierung. Insgesamt kann man erkennen, dass eher die Jungen statt die Mädchen darauf bedacht sind, wobei es bei den Mädchen v. a. Unwissenheit zu sein scheint.

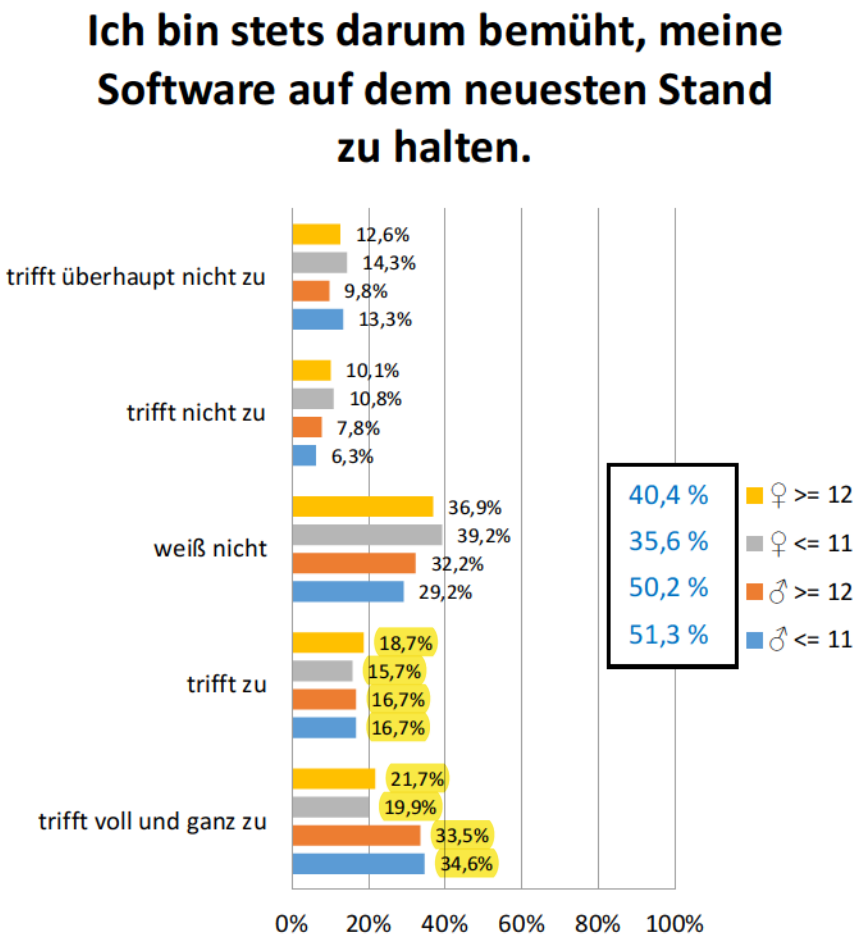


Abb. A4.10-38

Aufgrund der Datenlage kann folgendes Fazit gezogen werden:

1. Es sind keine großen oder deutlichen Unterschiede zwischen den Geschlechtern und dem Alter diagnostizierbar.
2. Die Mädchen sind eher vorsichtig und bedachter in dem, was sie tun, und hier v. a. die jüngeren. Die Jungen kann man eher als „riskanter“ bezeichnen, wobei auch sie dennoch überlegt handeln. Die älteren Teilnehmer sehen den Umgang mit persönlichen Daten eher lockerer als die jüngeren.
3. Bei den technischen Fragestellungen sind die Jungen überlegen und die Mädchen scheinen eher hilflos zu sein.
4. Insgesamt ergibt sich ein Bild der Besorgtheit um die persönlichen Daten.
5. Es lassen sich folgende prozentuale Anteile errechnen:

Gruppe	W	RK	ANK	UK	HK
Mädchen >=12	29,9%	62,4%	28,9%	68,0%	52,3%
Mädchen <= 11	21,1%	70,4%	19,7%	62,0%	56,7%
Jungen <= 12	37,8%	63,0%	41,0%	59,0%	53,7%
Jungen <= 12	27,2%	67,7%	30,1%	54,3%	54,0%

Tab. A4.10-1: Prozentuale Verteilung

Dementsprechend ergeben sich folgende Noten:

Gruppe	W	RK	ANK	UK	HK
Mädchen >=12	5	4	5	3	4
Mädchen <= 11	5	3	5	4	4
Jungen <= 12	5	4	5	4	4
Jungen <= 12	5	3	5	4	4

Tab. A4.10-2: Notenvergabe

ANHANG 4.11

Korrelative Auswertung der Studie

Die folgenden Seiten umfassen die Diagramme der bivariaten Analyse der Studie inklusive knapper Anmerkungen und stellen die Abhängigkeiten zwischen den einzelnen Dimensionen (Subkompetenzen) des Datenschutzkompetenzmodells dar.

Zusammenhang zwischen *Wissen* und *Risikobewertungskompetenz*[1]

Die *Risikobewertungskompetenz* variiert ohne erkennbaren Zusammenhang zu *Wissen* zwischen knapp 40 % und 100 %. Dies wird bestätigt durch r = 0,009 [2], d. h. es liegt keine Korrelation vor.

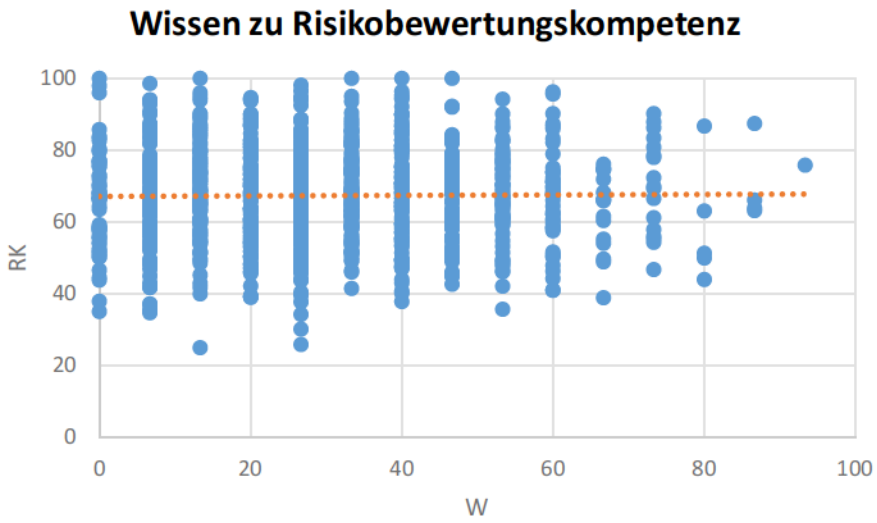


Abb. A4.11-1

Zusammenhang zwischen *Wissen* und *Auswahl- und Nutzungskompetenz*

Die *Auswahl- und Nutzungskompetenz* variiert stark zu *Wissen*, wobei eine schwache bis mittlere Korrelation vorliegt, wie r = 0,168 bestätigt. Die Regressionsgerade lässt vermuten, dass mit steigendem *Wissen* auch die *Auswahl- und Nutzungskompetenz* wächst (und umgekehrt), was sich damit erklären lässt, dass Wissen eine zielsichere Auswahl z. B. an Softwareprodukten zulässt.

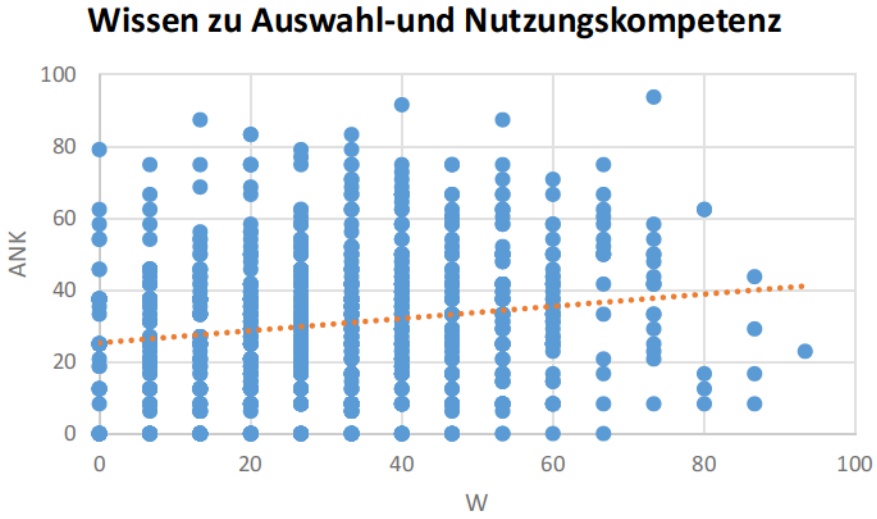


Abb. A4.11-2

[1] Die rot gepunktete Gerade ist die Regressionsgerade.
[2] r beschreibt den Korrelationskoeffizient.

Zusammenhang zwischen *Wissen* und *Urteilskompetenz*

Die *Urteilskompetenz* variiert bei 0 % *Wissen* zwischen 0 % und 90 % als auch bei 80 % *Wissen* zwischen 20 % und 100 %. Es liegt eine schwache bis mittlere Korrelation vor (r = 0,154). Die Regressionsgerade spricht jedoch dafür, dass mehr *Wissen* auch mehr *Urteilskompetenz* verspricht (und umgekehrt), wobei die Streuung jedoch viel zu groß ist.

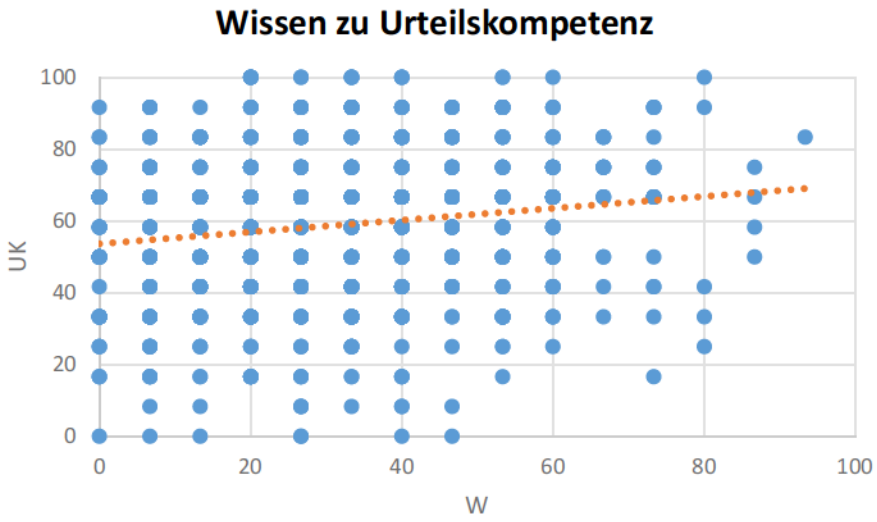


Abb. A4.11-3

Zusammenhang zwischen *Wissen* und *Handlungskompetenz*

Die *Handlungskompetenz* variiert ohne erkennbaren Zusammenhang zu *Wissen* zwischen 20 % und 100 %. Der Korrelationskoeffizient mit r = 0,254 spricht für einen mittleren Effekt. Die Regressionsgerade zeigt jedoch, dass ein höherer Anteil an Wissen auch eine bessere Handlungskompetenz vermuten lässt (und umgekehrt).

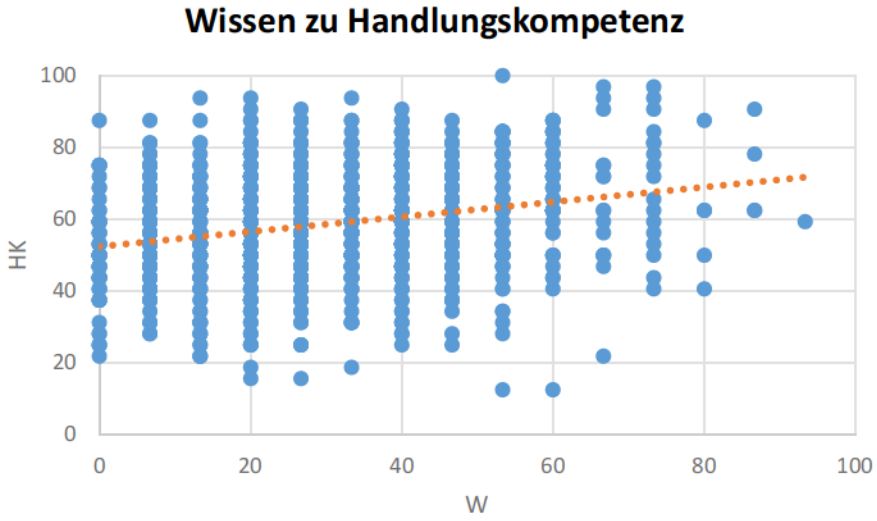


Abb. A4.11-4

Zusammenhang zwischen *Wissen* und der abschließenden *Datenschutzkompetenz*

Die *Datenschutzkompetenz* korreliert zu *Wissen*, was an der ansteigenden Regressionsgerade erkennbar ist: mehr Wissen führt zu einer höheren Datenschutzkompetenz (und umgekehrt). Die Werte sind noch breit gestreut, jedoch liegt der Korrelationskoeffizient bei r = 0,266, also liegt ein mittlerer Effekt vor. Dies lässt sich damit begründen, dass *Wissen* für eine ausreichende *Datenschutzkompetenz* notwendig ist.

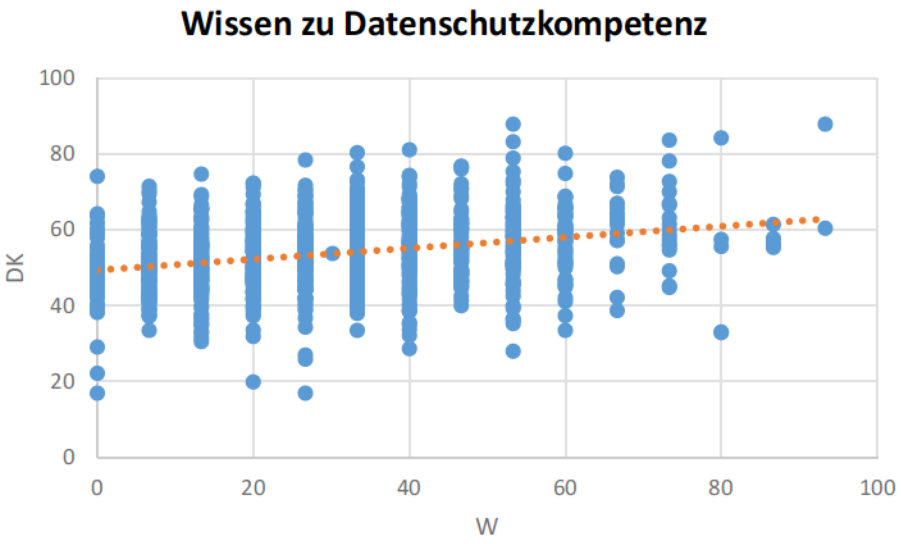


Abb. A4.11-5

Zusammenhang zwischen *Risikobewertungskompetenz* und *Auswahl- und Nutzungskompetenz*

Diese Datenwolke lässt keinen Zusammenhang und nur eine schwach-negative Korrelation (r = -0,111) erkennen. Je höher die *Risikobewertungskompetenz* desto niedriger die *Auswahl- und Nutzungskompetenz*.

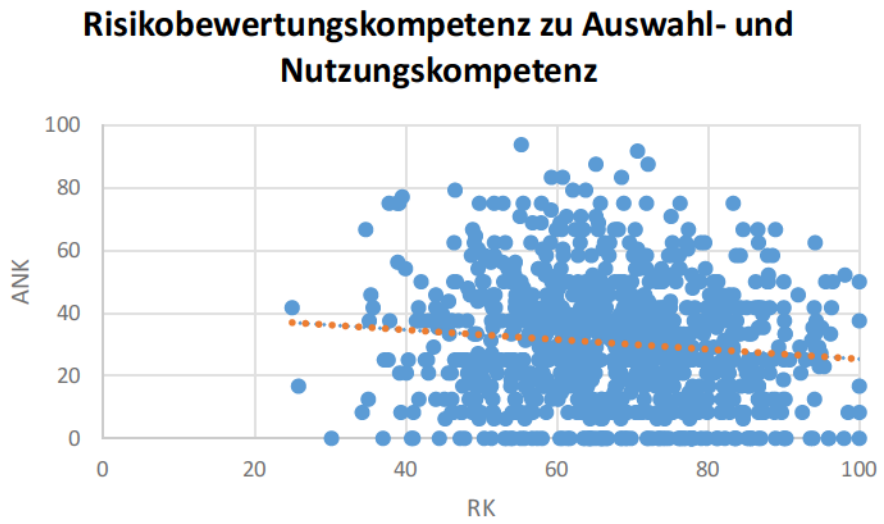


Abb. A4.11-6

Zusammenhang zwischen *Risikobewertungskompetenz* und *Urteilskompetenz*

Diese Datenwolke lässt keinen Zusammenhang und nur eine schwache bis mittlere Korrelation (r = 0,238) erkennen. Die steigende Regressionsgerade besagt, dass mit wachsender *Risikobewertungskompetenz* auch die *Urteilskompetenz* zunimmt (und umgekehrt).

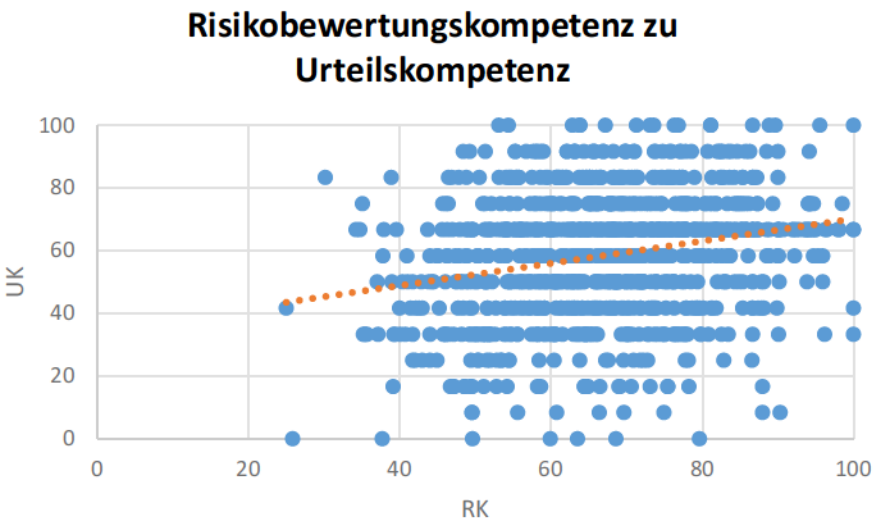


Abb. A4.11-7

Zusammenhang zwischen *Risikobewertungskompetenz* und *Handlungskompetenz*

Diese Datenwolke lässt keinen Zusammenhang und nur eine sehr schwache Korrelation (r = 0,088) erkennen. Je höher die *Risikobewertungskompetenz* desto höher die *Handlungskompetenz* (und umgekehrt).

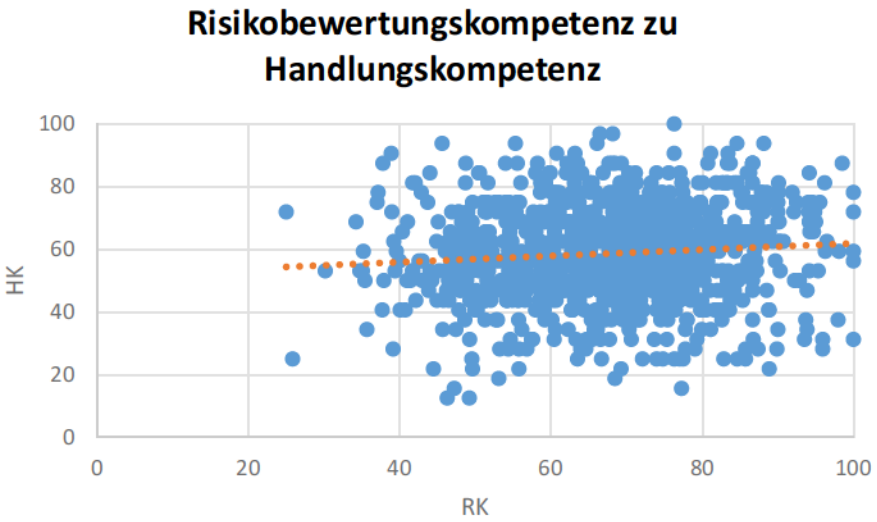


Abb. A4.11-8

Zusammenhang zwischen *Auswahl- und Nutzungskompetenz* und *Urteilskompetenz*

Die *Auswahl- und Nutzungskompetenz* korreliert sehr schwach zur *Urteilskompetenz* (r = -0,072). Je höher die *Urteilskompetenz* desto niedriger die *Auswahl- und Nutzungskompetenz* (und umgekehrt).

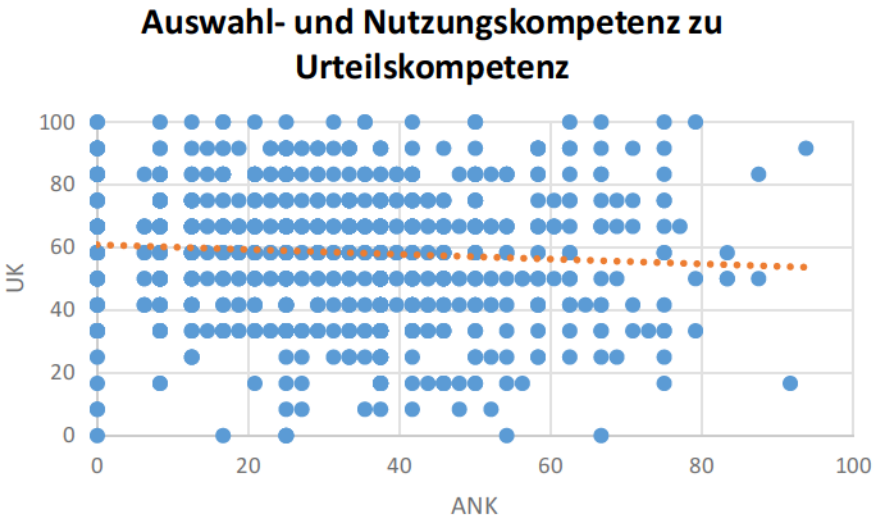


Abb. A4.11-9

Zusammenhang zwischen *Auswahl- und Nutzungskompetenz* und *Handlungskompetenz*

Trotz einer starken Streuung ist eine Tendenz zu verzeichnen, dass eine höhere *Auswahl- und Nutzungskompetenz* auch eine höhere *Handlungskompetenz* impliziert (und umgekehrt). Von einem mittleren Effekt kann bei r = 0,333 gesprochen werden.

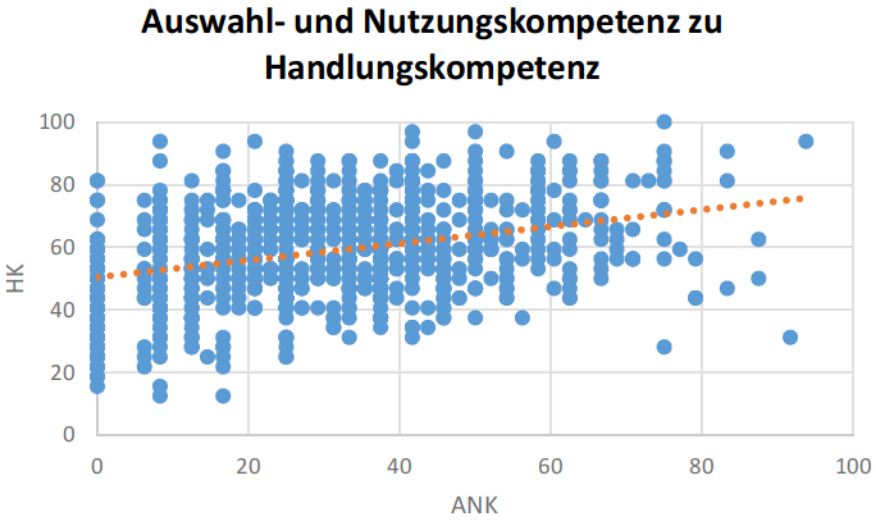


Abb. A4.11-10

Zusammenhang zwischen *Urteilskompetenz* und *Handlungskompetenz*

Mit einem Wert von r = 0,102 kann von einer schwachen Korrelation gesprochen werden, wenn auch kein deutlicher Zusammenhang erkennbar ist. Je höher die *Urteilskompetenz* desto höher die *Handlungskompetenz* (und umgekehrt).

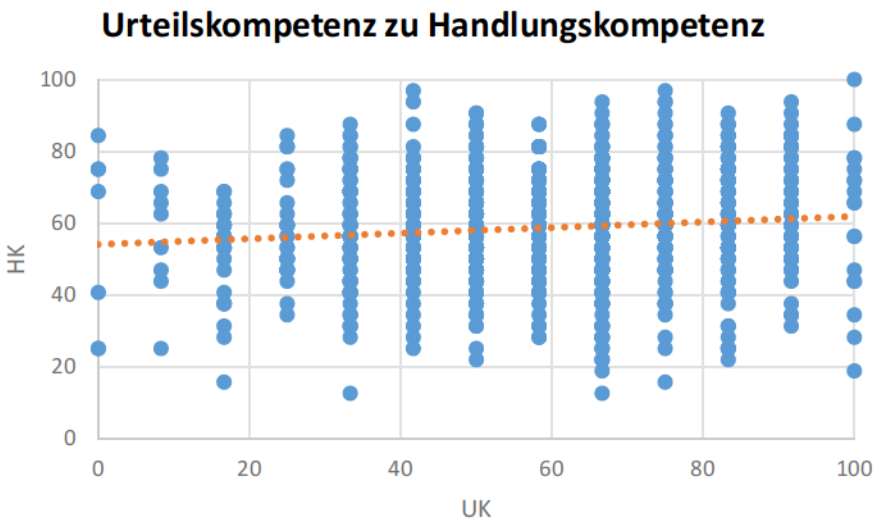


Abb. A4.11-11

ANHANG 4.12

Fragebogen der Vorbefragung

Die folgenden Seiten umfassen den schriftlichen Fragebogen für die erste Erhebung im Sommer 2016.

UNIVERSITÄT KOBLENZ · LANDAU

Universität Koblenz-Landau FDI Fachdidaktik Informatik

Fragebogen Vorbefragung „Datenschutz bei Jugendlichen“

I.	Nr.		Geschlecht	m / w	Alter	

II.	Welchen Gerätetyp nutzt Du für den Internetzugang?		
Handy/Smartphone	Computer/Laptop	Tablet-PC	Spielekonsole
Fernseher	MP3-Player u. ä.	E-Book-Reader	Sonstiges

Interner Code: 1. Zahl steht für Studie, 2. Zahl steht für die Seitenzahl

III.	Wozu nutzt Du das Internet? [4/133]		
zum Chatten	zum Mailen	für Soziale Netzwerke	zum Twittern
um Videos zu schauen	für Musikvideos	zum Fernsehen	für Online-Games
für Online-Shopping	um Musik zu hören	für Wikipedia	für Nachrichtenportale
für Newsgroups/Foren	für Mediatheken	für Bezahldienste	für Versteigerungen
für Diskussionsforen	für Weblogs	für die Schule	für Instant-Messaging
zur Information über Musik, Mode, u. ä		für Bilder-Plattformen	für Partnerbörse
für Online-Banking	um mich treiben zu lassen		

IV.	Auf welcher Weise bist Du im Netz? [6/29]		
Konsumierend	Partizipierend	produzierend	Nicht-Nutzer

V.	Wie häufig nutzt Du das Internet? [4/62] BEACHTE! Auch die Nutzung von Messengern ist eine Internetnutzung				
(a)	< 1 h/Tag	1 – 2 h/Tag	2 – 4 h/Tag	> 4 h/Tag	
(b)	täglich	mehrmals/Woche	ein paar Mal/Monat	seltener	nie

VI.	Was sind Deine Motive für die Internetnutzung? [6/38]		
Unterhaltung	Beziehungspflege	Information	Zugehörigkeitsgefühl
Knüpfen neuer Kontakte		Selbstdarstellung	Realitätsflucht

VII.	Was benutzt Du? Kreuze an!			
Messenger	Soziale Netzwerke	Browser	Browser-Tools	Apps
○ WhatsApp ○ Snapchat ○ Telegram ○ Threema ○ BlackBerry Messenger ○ Hangout ○ Xabber ○ ChatOn ○ Skype ○ Instagram ○ SMS ○	○ Facebook (FB) ○ Google+ ○ Twitter ○ YouTube ○ Tumblr ○ Instagram ○ MySpace ○ LinkedIn ○ ○ ○ ○ ○	○ Mozilla Firefox ○ Microsoft Internet Explorer ○ Google Chrome ○ Opera ○ Apple Safari ○ ○ ○ ○ ○	○ Ghostery ○ Adblock Plus ○ Bug me not ○ Firebug ○ Flagfox ○ Self-Destructing-Cookies ○ ○ ○ ○ ○	○ Antiviren-Software ○ Clean Master ○ My Permissions Datenschutz ○ ○ ○ ○ ○ ○ ○

UNIVERSITÄT KOBLENZ · LANDAU

Universität Koblenz-Landau FDI Fachdidaktik Informatik

VIII.	Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich persönlich bei den folgenden Punkten? [3/110]						
1 = sehr kompetent; 2 = kompetent; 3 = unentschieden; 4 = inkompetent; 5 = sehr inkompetent; 6 = weiß nicht							
1	Informationen im Internet recherchieren können	1	2	3	4	5	6
2	Sich mit anderen im Internet vernetzen können	1	2	3	4	5	6
3	Die eigene Person im Internet angemessen darstellen können	1	2	3	4	5	6
4	Die eigene Privatsphäre im Internet gut schützen können	1	2	3	4	5	6
5	Gewalttätigen, rassistischen und pornografischen Inhalten ausweichen können	1	2	3	4	5	6
6	Konsequenzen des eigenen Hochladens im digitalen Raum abschätzen können	1	2	3	4	5	6
7	Zwischen privaten und öffentlichen Räumen im Internet unterscheiden können	1	2	3	4	5	6
8	Vertrauenswürdigkeit von Informationsquellen im Internet einschätzen können	1	2	3	4	5	6
9	Das Internet und digitale Medien zu kreativen Betätigungen und der Gestaltung eigener Inhalte nutzen können	1	2	3	4	5	6

IX.	Welche Internetseiten nutzt Du am liebsten bzw. auf welchen Seiten gehst Du am häufigsten? [3/73]	

X.	Wie wichtig ist Dir jeweils einer der u. s. Aspekte bei der Nutzung eines Messengers?						
1 = sehr wichtig; 2 = wichtig; 3 = unentschieden; 4 = unwichtig; 5 = sehr unwichtig; 6 = weiß nicht							
1	Verschlüsselung bei der Übermittlung	1	2	3	4	5	6
2	Provider kann verschlüsselte Mitteilungen lesen	1	2	3	4	5	6
3	Identifikationsmöglichkeiten des Gesprächspartners	1	2	3	4	5	6
4	Veröffentlichung des Programmcodes zwecks Verifikation	1	2	3	4	5	6
5	Schnelligkeit der Übermittlung	1	2	3	4	5	6
6	Zusatz wie Stickers, Sprachnachrichten, Telefonieren, ...	1	2	3	4	5	6
7	Das Sicherheitsdesign ist öffentlich dokumentiert	1	2	3	4	5	6
8	Zertifizierung des Programmcodes	1	2	3	4	5	6
9	Nutzerzahlen	1	2	3	4	5	6
10	Anzahl der Dateiformate, die weitergeleitet werden können	1	2	3	4	5	6
11	Sicherheit der Nachricht bei Diebstahl des Schlüssels	1	2	3	4	5	6

UNIVERSITÄT KOBLENZ · LANDAU

Universität Koblenz-Landau FDI Fachdidaktik Informatik

XI.	Welche Informationen würdest Du über Dich im Internet veröffentlichen? [4/119, 6/30, 6/40]			
Vorname	Nachname	Nickname/Spitzname	Geburtstag	Ausbildung/Beruf
E-Mail-Adresse	Post-Adresse	Fotos (inkl. Porträt)	Private Kontakte	Berufl. Kontakte
Beziehungsstatus	Lieblingsfilme/-serien/-bücher/-musik		Interesse/Hobby	Instant-Messenger
Handy-Nummer	Telefon-Nummer	Politische Einstellung	Sexuelle Orientierung	
Eigene Erlebnisse	Eigene Gedanken	Eigene Gefühle	Eigene Sorgen/Ängste	
Religion				

XII.1	Mit wem teilst Du die Informationen in Sozialen Netzwerken? [6/43]		
nur Nutzer selbst	ausgewählte Kontakte	alle Kontakte	Kontakte + deren Freunde
alle Mitglieder	Öffentliches Netz		
XII.2	Mit wem teilst Du die Informationen auf anderen Plattformen? [6/43]		
nur Nutzer selbst	ausgewählte Kontakte	alle Kontakte	Kontakte + deren Freunde
alle Mitglieder	Öffentliches Netz		

XIII.1	Einstellungen Privatsphäre in Sozialen Netzwerken [1/30f]		
Hast Du an den Einstellungen zur Privatsphäre in dem von Dir am meisten genutzten Sozialen Netzwerks aktiv etwas geändert?		Ja	Nein
XIII.2	Welche Einstellungen hast Du verändert?		
Sichtbarkeit des Profils	Sichtbarkeit der Posts	Wer auf meine Seite posten darf	
Wer mich kontaktieren darf	Für wen ich zu finden bin		

XIV.	Datensicherheit in Communities/Messenger: Ich fühle mich … [5/41]						
1 = sehr sicher; 2 = sicher; 3 = unentschieden; 4 = weniger sicher; 5 = gar nicht sicher; 6 = weiß nicht							
1	bei WhatsApp	1	2	3	4	5	6
2	bei Facebook	1	2	3	4	5	6
3		1	2	3	4	5	6
4		1	2	3	4	5	6
5		1	2	3	4	5	6
6		1	2	3	4	5	6
7		1	2	3	4	5	6
8		1	2	3	4	5	6
9		1	2	3	4	5	6

XV.	Wie sehr vertraust Du … [4/104;4/157]						
1 = vertraue ich blind; 2 = vertraue ich; 3 = bin ich skeptisch; 4 = vertraue ich nur wenig; 5 = vertraue ich überhaupt nicht; 6 = weiß nicht							
1	WhatsApp	1	2	3	4	5	6
2	Facebook	1	2	3	4	5	6
3		1	2	3	4	5	6
4		1	2	3	4	5	6
5		1	2	3	4	5	6
6		1	2	3	4	5	6
7		1	2	3	4	5	6
8		1	2	3	4	5	6
9		1	2	3	4	5	6

UNIVERSITÄT KOBLENZ · LANDAU

Universität Koblenz-Landau FDI Fachdidaktik Informatik

XVI.	Was glaubst Du, wie sicher persönliche Daten im Internet sind? [4/143]				
sehr sicher	sicher	unentschieden	weniger sicher	gar nicht sicher	weiß nicht

XVII.	Welche Aussagen treffen für Dich zu? [4/31;142//beide letzten Fragen 1/21]						
1 = volle Zustimmung bis 5 = keine Zustimmung; 6 = weiß nicht							
1	Ich bin gut über die Möglichkeiten des Schutzes meiner Daten im Internet informiert.	1	2	3	4	5	6
2	Ich interessiere mich für die neuesten Möglichkeiten zum Schutz meiner Privatsphäre im Internet.	1	2	3	4	5	6
3	Ich bin mir sicher, dass meine persönlichen Daten im Internet noch nicht missbraucht wurden.	1	2	3	4	5	6
4	Aufgrund des hohen Sicherheitsrisikos im Internet schränke ich meine Online-Zeit ein.	1	2	3	4	5	6
5	Ich achte darauf, welche Informationen ich selbst über mich ins Internet stelle.	1	2	3	4	5	6
6	Ich achte darauf, welche Informationen über mich im Internet sichtbar sind.	1	2	3	4	5	6

XVIII.	Was sind für Dich Risiken im Internet? [4/107ff;126f;145f]		
1	Infizierung des Computers mit Schadprogrammen	Ja	Nein
2	Unerwünschte Weitergabe von persönlichen Daten an Dritte	Ja	Nein
3	Ausspionieren meiner persönlichen Daten	Ja	Nein
4	Belästigung durch Spam-Mails	Ja	Nein
5	Betrug beim Online-Einkauf/Online-Auktion	Ja	Nein
6	Nutzung meiner Daten für Werbezwecke	Ja	Nein
7	Beleidigung oder Belästigung im Internet	Ja	Nein
8	Betrug beim Online-Banking	Ja	Nein
9	Versendung unerwünschter E-Mails in meinem Namen	Ja	Nein
10	Mobbing/Stalking	Ja	Nein
11	Andere wissen, was ich tue, oder kennen meinen Aufenthaltsort	Ja	Nein
12	Fake-Profile	Ja	Nein
13	Verlust oder Löschung persönlicher Daten	Ja	Nein
14	Veröffentlichung peinlicher/intimer Chats/Fotos/...	Ja	Nein

XIX.	Zähle Malware auf!	

UNIVERSITÄT KOBLENZ · LANDAU

Universität Koblenz-Landau FDI Fachdidaktik Informatik

XX.	Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten? [4/152]		
1	Nutze Virenscanner	Ja	Nein
2	Nutze Firewall	Ja	Nein
3	Nutze sichere Geräte mit persönlichem Passwort	Ja	Nein
4	Aktualisiere persönliche Sicherheitseinstellungen in Sozialen Netzwerken gegenüber Grundeinstellungen	Ja	Nein
5	Nutze nur Seiten, bei denen ich weiß, dass sie sicher sind	Ja	Nein
6	Gebe keine persönlichen Daten in Sozialen Netzwerken preis	Ja	Nein
7	Gebe keine persönlichen Daten beim Mailen preis	Ja	Nein
8	Gebe keine persönlichen Daten beim Online-Shopping preis	Ja	Nein
9	Gebe keine persönlichen Daten beim Online-Banking preis	Ja	Nein
10	Gebe keine persönlichen Daten beim Chatten preis	Ja	Nein
11	Nutze Pop-Up-Blocker oder Adblocker	Ja	Nein
12	Nutze verschiedene Passwörter	Ja	Nein
13	Lade keine Dateien hoch	Ja	Nein
14	Lade keine Dateien herunter	Ja	Nein
15	Ändere häufig das Passwort	Ja	Nein
16	Mache bewusst falsche/irreführende persönliche Angaben	Ja	Nein
17		Ja	Nein
18		Ja	Nein
19		Ja	Nein
20		Ja	Nein

XXI.	Hast Du schon einmal folgende Strategien genutzt? [2/15]		
1	Opting-Out-Strategien		
1a	Aufgehört bestimmte Webseiten zu besuchen	Ja	Nein
1b	Aus Sicherheitsbedenken einen Online-Einkauf unterlassen	Ja	Nein
1c	Eine Online-Registrierung nicht durchgeführt, um Daten nicht angeben zu müssen	Ja	Nein
1d	Einen Online-Dienst nicht genutzt, um eigene Daten nicht für kommerzielle Zwecke herzugeben	Ja	Nein
2	Behaviorale Datenschutzmaßnahmen		
2a	Ein Pseudonym bei der Anmeldung benutzt	Ja	Nein
2b	Eine falsche E-Mail-Adresse bei der Anmeldung angeben	Ja	Nein
2c	Im Internetbrowser die Cookies und den Cache gelöscht	Ja	Nein
3	Software-Lösungen		
3a	Eine Verschlüsselungssoftware benutzt	Ja	Nein
3b	Anti-Viren-Software regelmäßig geupdatet	Ja	Nein
3c	Nutzung von Anti-Malware-Programmen	Ja	Nein
3d	Nutzung von Anonymisierungstools	Ja	Nein
3e	Nutzung von Anti-Tracking-Software	Ja	Nein
4	Rechtliche Maßnahmen		
4a	Anbieter gebeten, persönliche Daten zu löschen	Ja	Nein
4b	Anbieter gebeten, persönliche Daten nicht weiterzugeben	Ja	Nein

UNIVERSITÄT KOBLENZ · LANDAU

Universität Koblenz-Landau FDI Fachdidaktik Informatik

XXII.	Stimmen die folgenden Aussagen? [2/6]		
1	Die Betreiber Sozialer Netzwerke sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk überhaupt nicht nutzen.	Ja	Nein
2	Die NSA greift nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.	Ja	Nein
3	Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.	Ja	Nein
4	In der EU ist es gesetzlich erlaubt, dass anonymisierte Nutzerdaten für Marktforschungszwecke weitergeleitet werden dürfen.	Ja	Nein
5	Die Nachverfolgung der eigenen Internetnutzung kann durch regelmäßiges Löschen der Browserinformationen erschwert werden.	Ja	Nein
6	Unternehmen kombinieren Daten, die auf verschiedenen Webseiten hinterlassen werden, und stellen daraus Nutzerprofile zusammen.	Ja	Nein

XXIII.	Welche Deiner Rechte und Deiner Pflichten in Bezug auf Datenschutz sind Dir (bereits) bekannt?

UNIVERSITÄT KOBLENZ · LANDAU

Universität Koblenz-Landau FDI Fachdidaktik Informatik

XXIV.	Worüber hättest Du gerne mehr Informationen? [3/130]		
… zum Schutz meiner Daten im Internet		Ja	Nein
… zur rechtlichen Situation		Ja	Nein
… zu technischen Möglichkeiten		Ja	Nein
… zu den Gefahren beim Surfen im Internet		Ja	Nein
…			

Datenschutz in der Schule behandelt? Ja / Nein

In welchem Fach? _____

Verbraucherbildung in der Schule? Ja / Nein

Informatikunterricht oder AG Informatik? Ja / Nein

UNIVERSITÄT KOBLENZ · LANDAU

Universität Koblenz-Landau FDI Fachdidaktik Informatik

Diese Seite enthält die Quellen, aus den die Fragen entnommen worden sind, und lag den Schülern nicht vor:

[1] BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Hg.) (2014): Jung und vernetzt. Kinder und Jugendliche in der digitalen Welt. Berlin. Online verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Jung-und-vernetzt-Kinder-und-Jugendliche-in-der-digitalen-Gesellschaft.html, zuletzt geprüft am 01.07.2018.

[2] Masur, Philipp K.; Teutsch, Doris; Trepte, Sabine (2017): Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). In: *Diagnostica* 63 (4), S. 256–268.

[3] Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (Hg.) (2015): DIVSI U9-Studie. Kinder in der digitalen Welt. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Hamburg. Online verfügbar unter www.divsi.de/wp-content/uploads/2015/06/U9-Studie-DIVSI-web.pdf, zuletzt geprüft am 08.06.2018.

[4] Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (Hg.) (2014): DIVSI U25-Studie. Kinder, Jugendliche und junge Erwachsene in der digitalen Welt. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Hamburg. Online verfügbar unter www.divsi.de/wp-content/uploads/2014/02/DIVSI-U25-Studie.pdf, zuletzt geprüft am 01.07.2018.

[5] Feierabend, Sabine; Plankenhorn, Theresa; Rathgeb, Thomas (2015): JIM-Studie 2015. Jugend, Information, (Multi-)Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland. Hg. v. Medienpädagogischer Forschungsverbund Südwest. Stuttgart. Online verfügbar unter www.mpfs.de/fileadmin/files/Studien/JIM/2015/JIM_Studie_2015.pdf, zuletzt geprüft am 02.07.2018.

[6] Schenk, Michael; Niemann, Julia; Reinmann, Gabi; Schnurr, Jan-Mathis; Jandt, Silke; Roßnagel, Alexander (2012): Gläserne Freunde? Kompaktversion zur LfM-Studie „Digitale Privatsphäre. Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen“. Manuskriptfassung. Hg. v. Landesanstalt für Medien Nordrhein-Westfalen (LfM). Düsseldorf. Online verfügbar unter https://www.lfm-nrw.de/fileadmin/lfm-nrw/Forschung/Kompaktstudie-Glaeserne-Freunde.pdf, zuletzt geprüft am 26.07.2015.

ANHANG 4.13

Auswertung des Fragebogens der Vorbefragung

Die folgenden Seiten umfassen die deskriptive Auswertung der Erhebung vom Sommer 2016.

Verteilung zwischen Geschlechtern

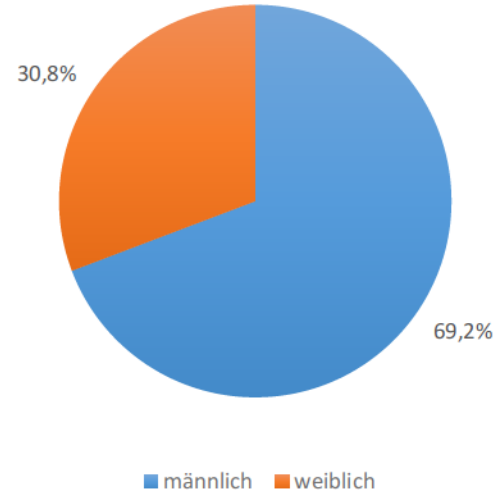


Abb. A4.13-1

Verteilung des Alters

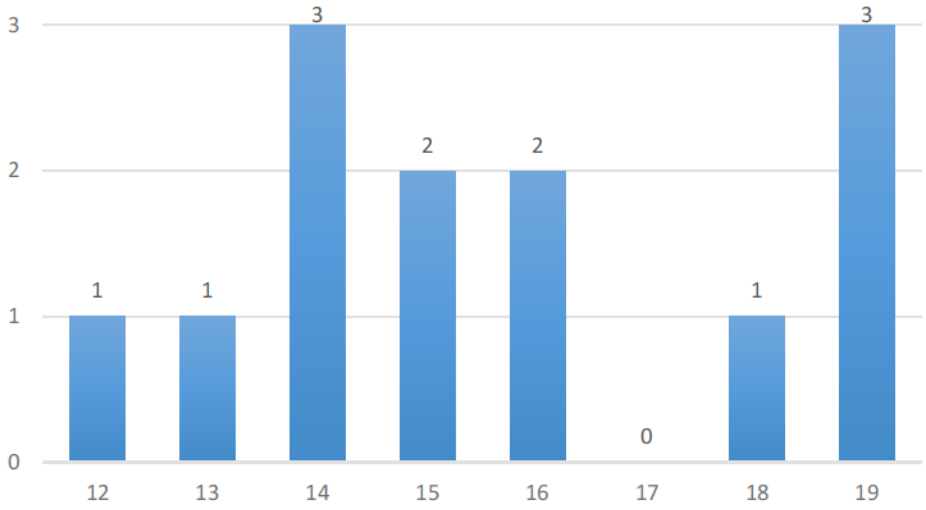


Abb. A4.13-2

Welchen Gerätetyp nutzt Du für den Internetzugang?

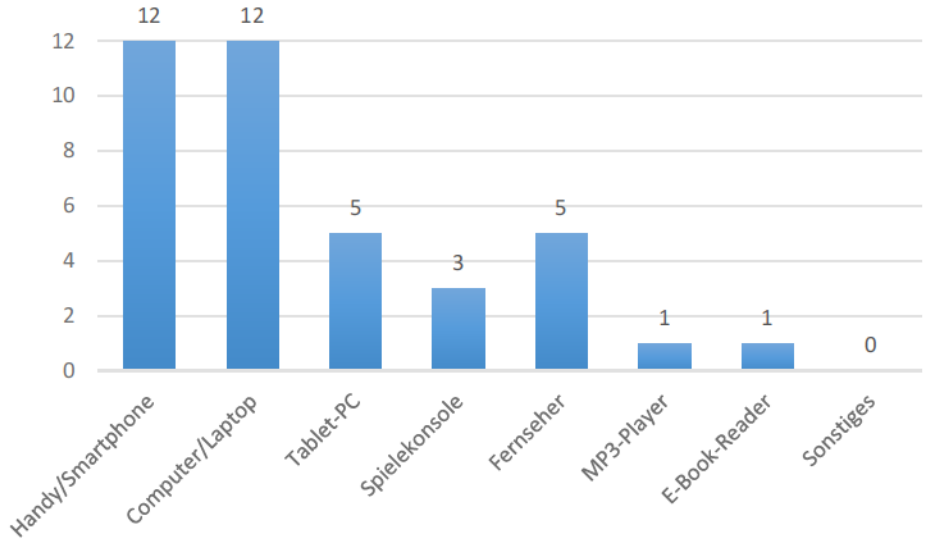


Abb. A4.13-3

Wozu nutzt Du das Internet?

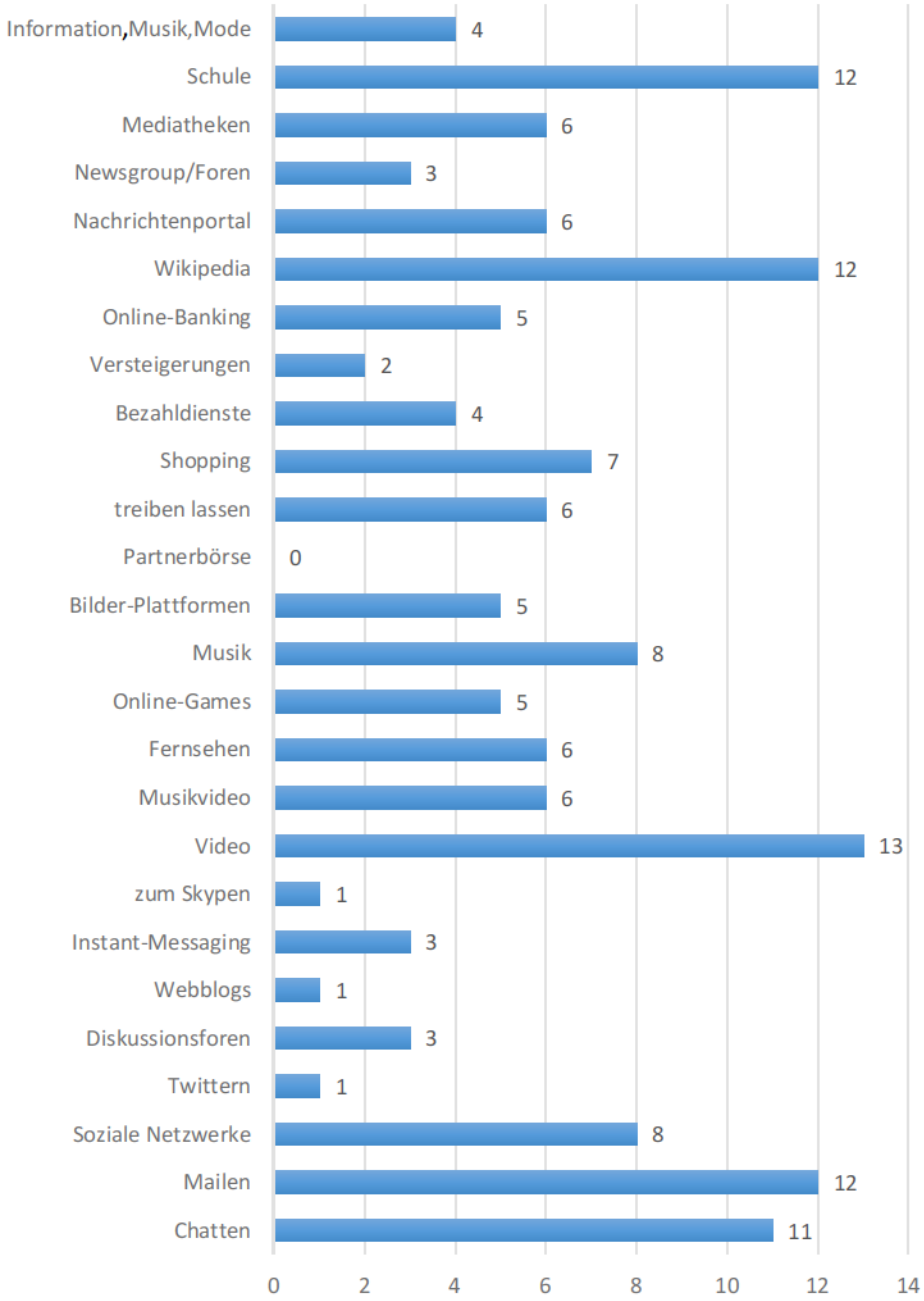


Abb. A4.13-4

Auf welcher Weise bist Du im Netz?

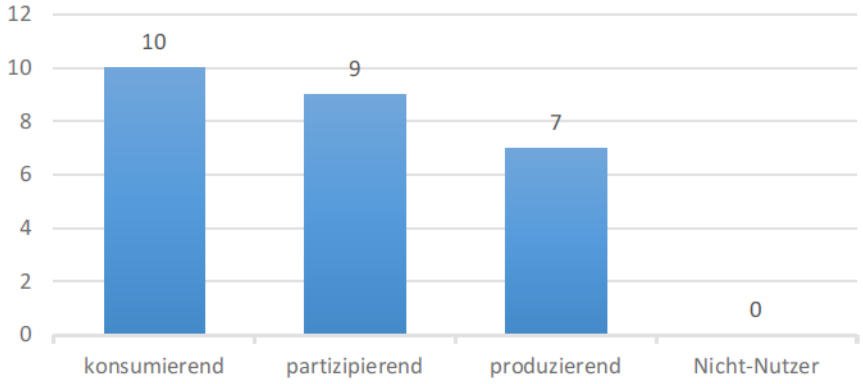


Abb. A4.13-5

Wie häufig bist Du im Internet?

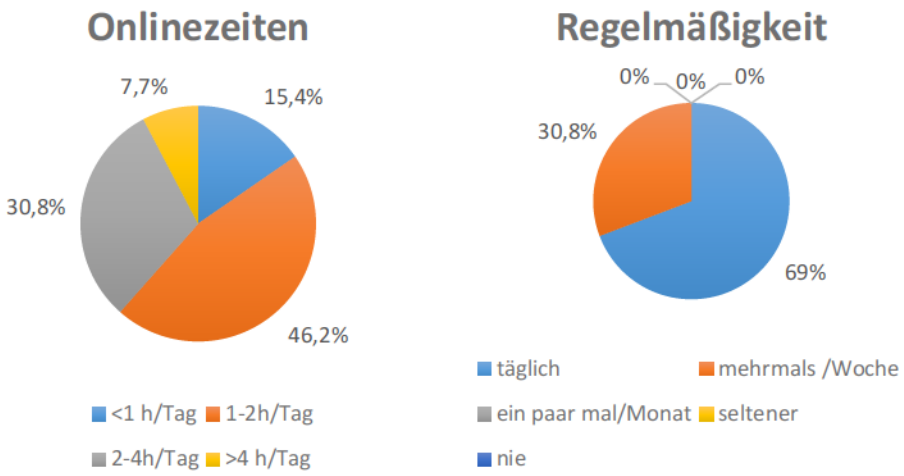


Abb. A4.13-6

Was sind Deine Motive für die Internetnutzung?

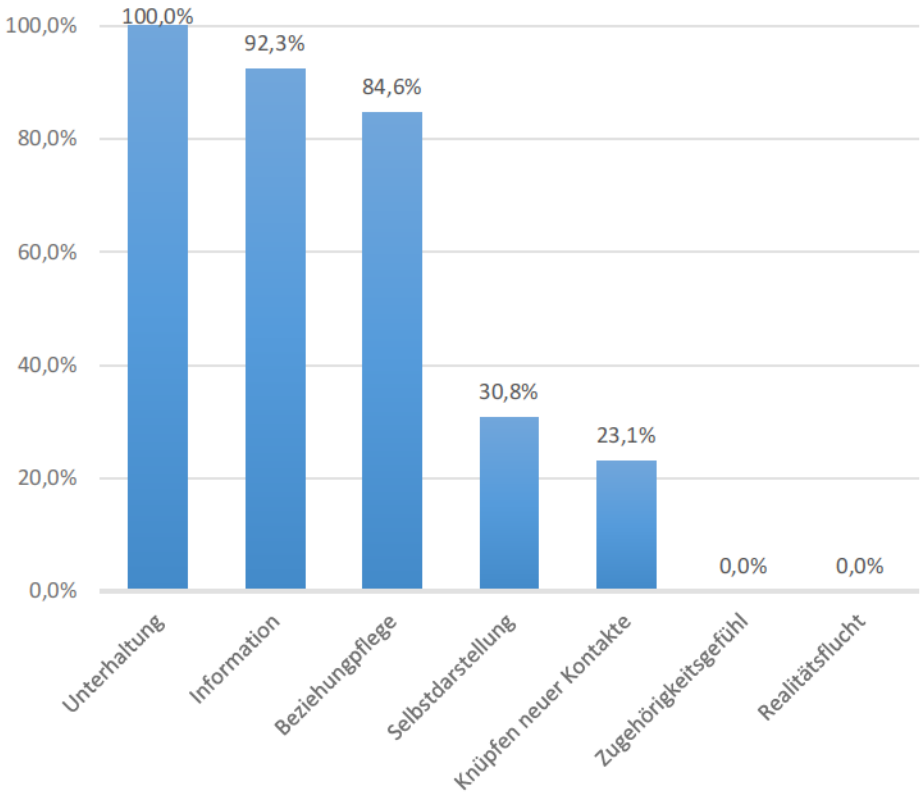


Abb. A4.13-7

Was benutzt Du?

Messenger

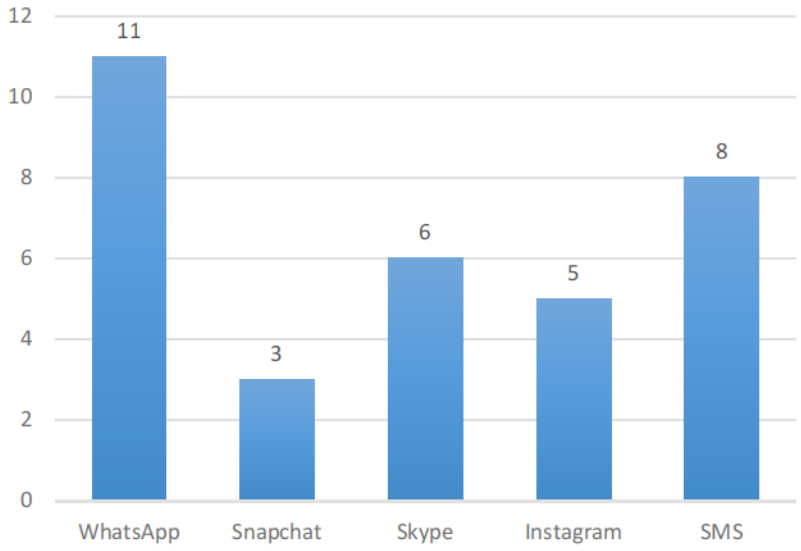


Abb. A4.13-8

Was benutzt Du?

Soziale Netzwerke

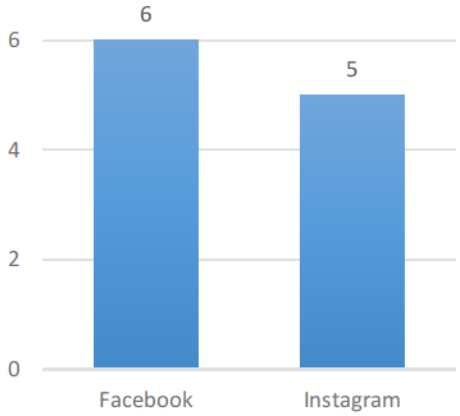


Abb. A4.13-9

Was benutzt Du?

Browser

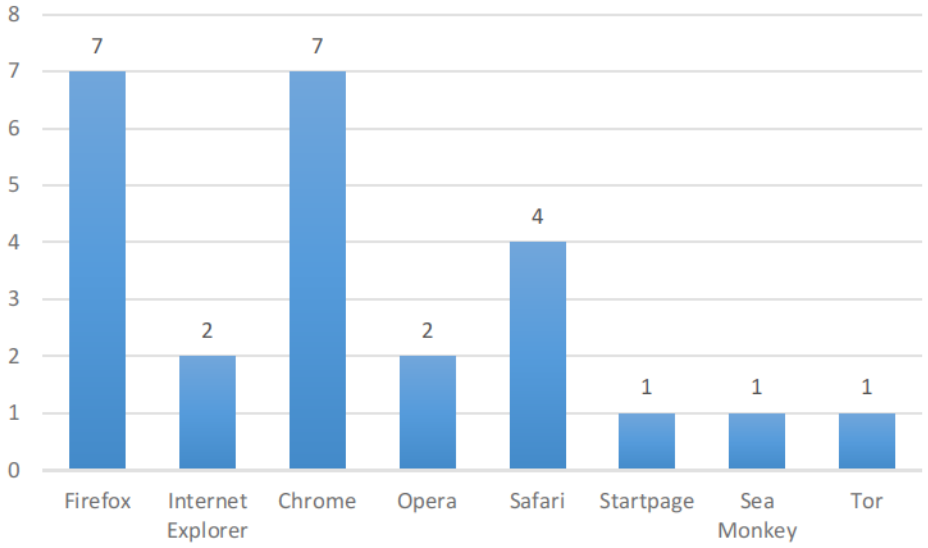


Abb. A4.13-10

Was benutzt Du?

Browser-Tools

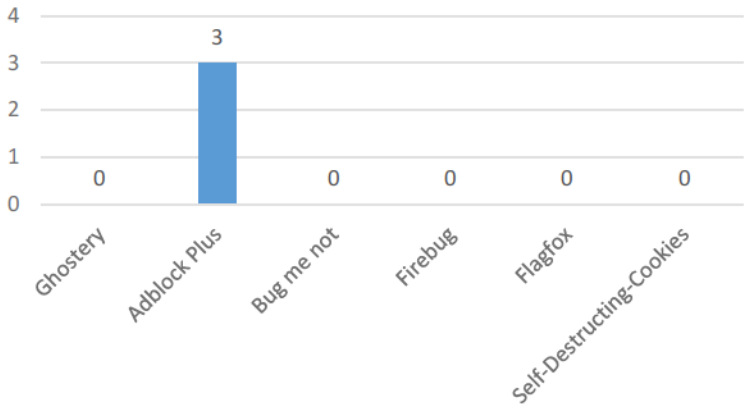


Abb. A4.13-11

Was benutzt Du?

Apps

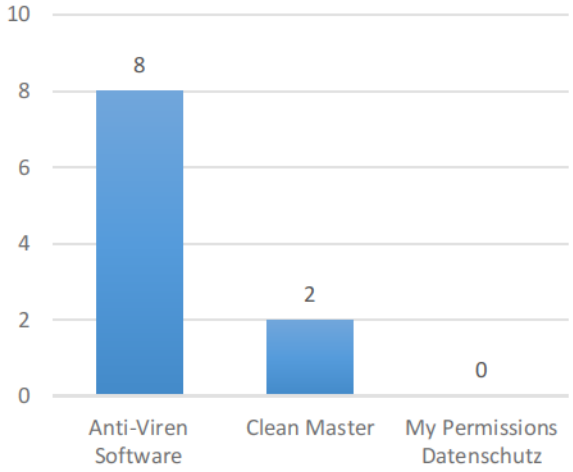


Abb. A4.13-12

Wenn Du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich persönlich bei den folgenden Punkten?

Durchschnitt -
Punkte von 1 *sehr kompetent* bis 5 *sehr unkompetent* und 6 *weiß nicht*

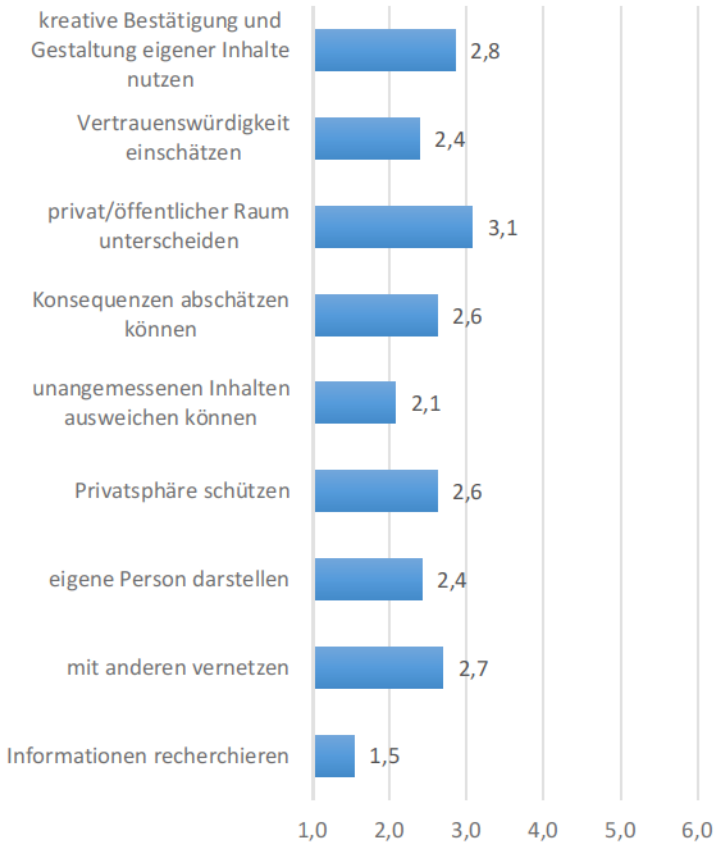


Abb. A4.13-13

Welche Internetseiten nutzt Du am liebsten bzw. auf welchen Seiten gehst Du am häufigstem?

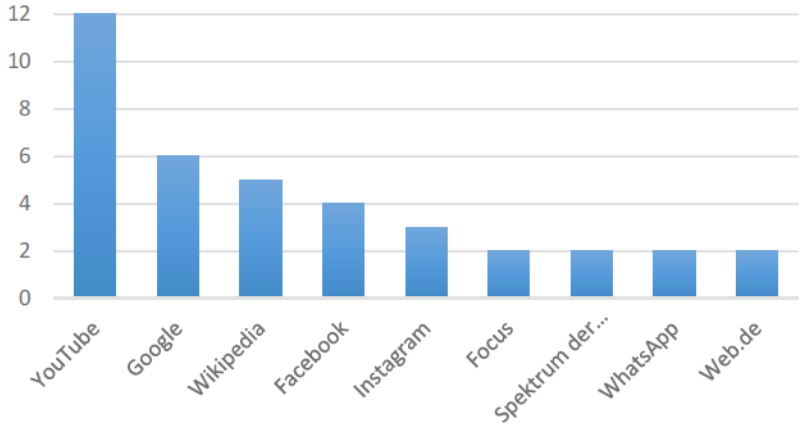


Abb. A4.13-14

Wie wichtig ist dir jeweils einer der u. s. Aspekte bei der Nutzung eines Messengers?

Durchschnitt - Punkte von 1 *sehr wichtig* bis 5 *sehr unwichtig* und 6 *weiß nicht*

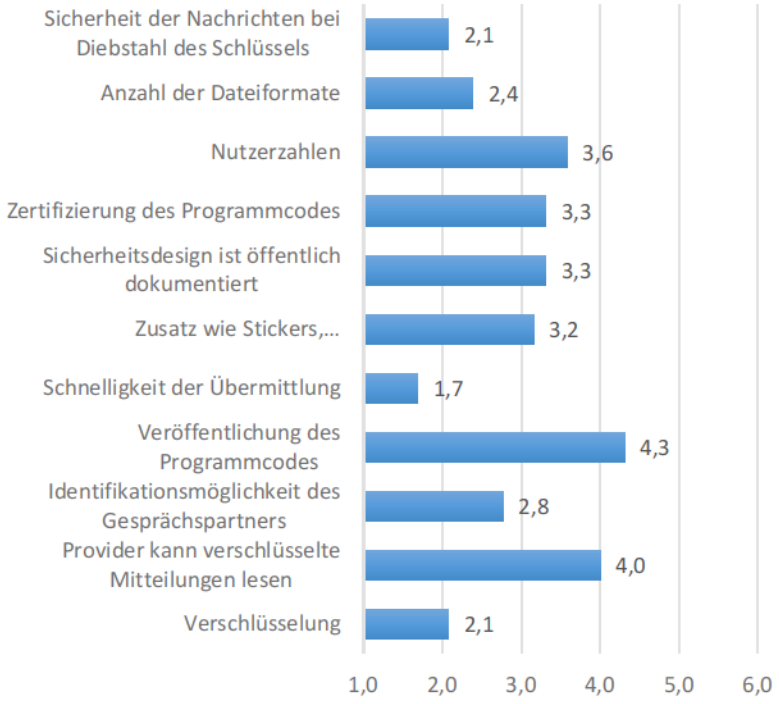


Abb. A4.13-15

Welche Informationen würdest Du über Dich im Internet veröffentlichen?

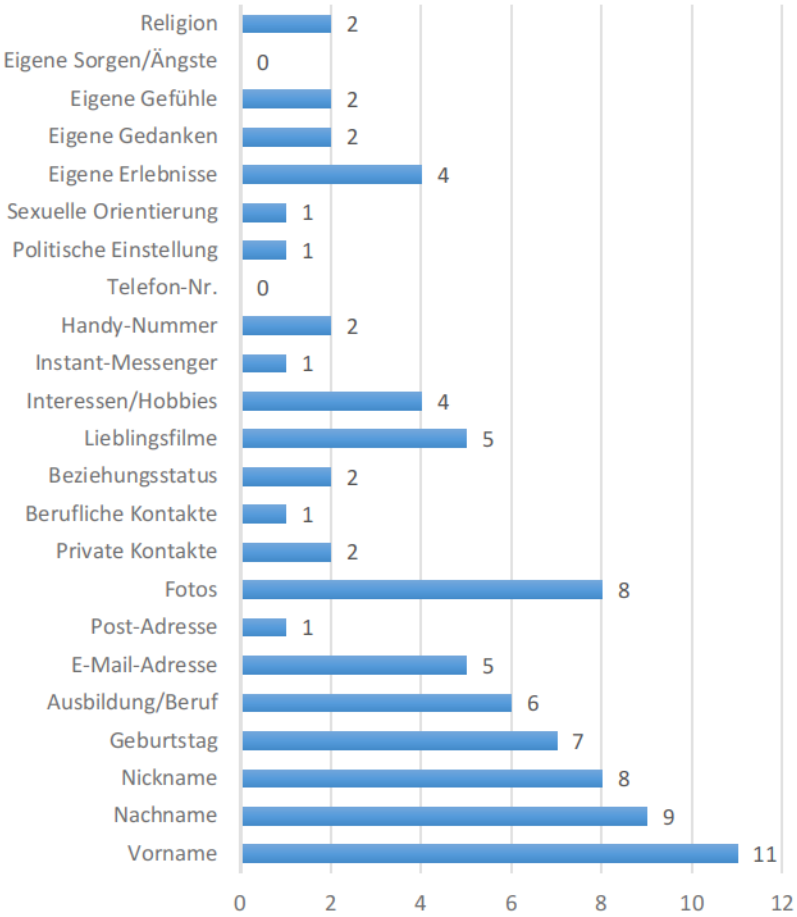


Abb. A4.13-16

Mit wem teilst Du die Informationen auf Sozialen Netzwerken?

Mehrfachantworten möglich.

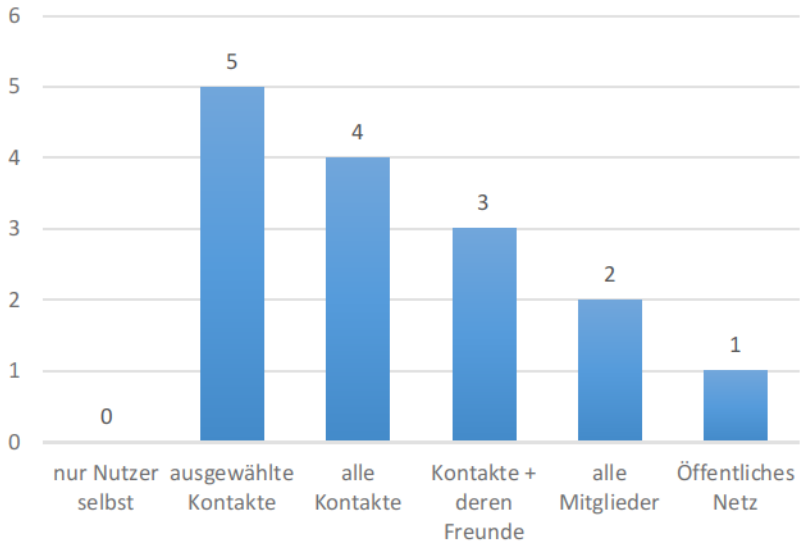


Abb. A4.13-17

Mit wem teilst Du die Informationen auf anderen Plattformen?

Mehrfachantworten möglich.

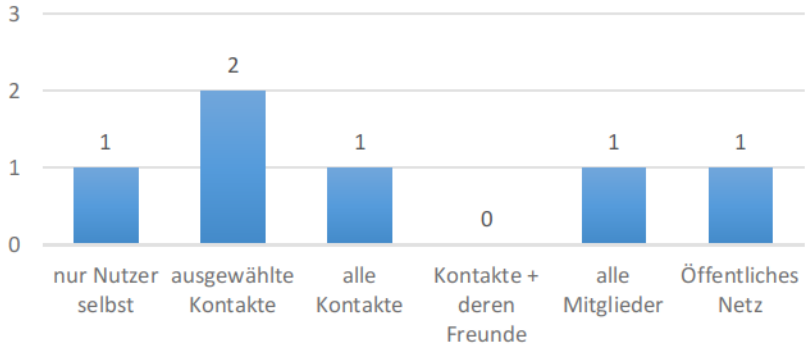


Abb. A4.13-18

Was hast Du in den Privatsphäreeinstellungen in Sozialen Netzwerken geändert?

Mehrfachantworten möglich.

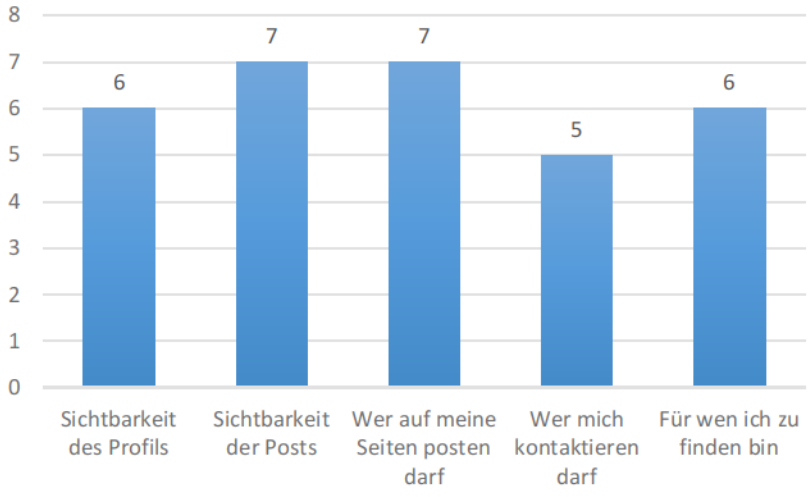


Abb. A4.13-19

Datensicherheit in Communities/Messenger: ich fühle mich bei …

Durchschnitt aller Rückmeldungen
Punkte von 1 *sehr sicher*
bis 5 *gar nicht sicher* und 6 *weiß nicht*

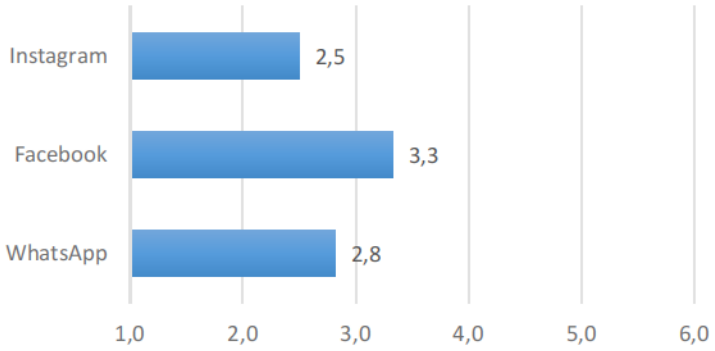


Abb. A4.13-20

Wie sehr vertraust Du …

Durchschnitt aller Rückmeldungen
Punkte von 1 *vertraue ich blind*
bis 5 *vertraue ich überhaupt nicht*
und 6 *weiß nicht*

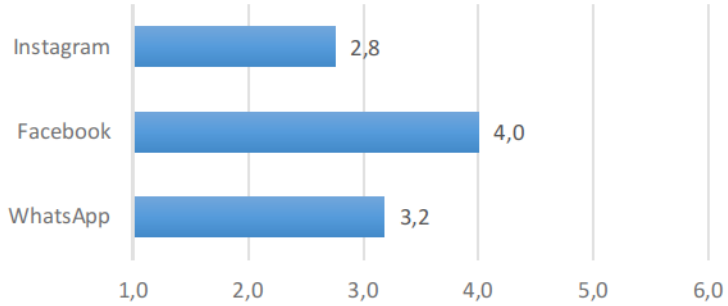


Abb. A4.13-21

Was glaubst Du, wie sicher persönliche Daten im Internet sind?

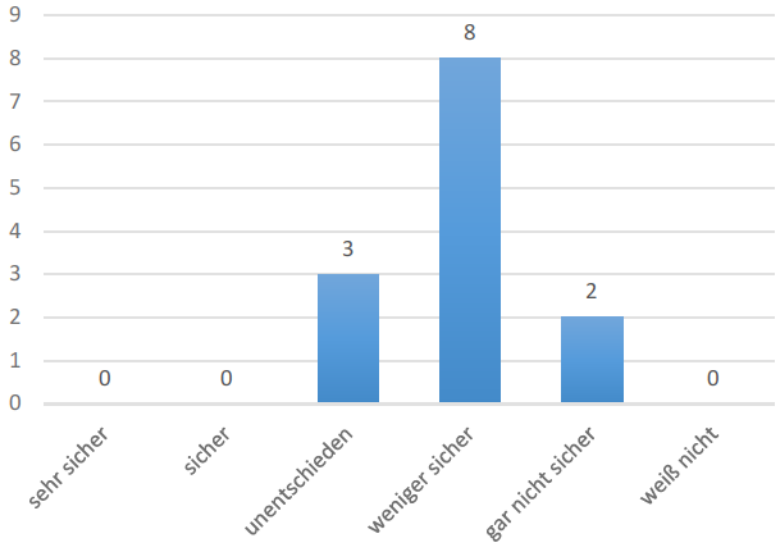


Abb. A4.13-22

Welche Aussagen treffen für Dich zu?

Durchschnitt aller Rückmeldungen
Punkte von 1 *volle Zustimmung* bis 5 *keine Zustimmung* und 6 *weiß nicht*

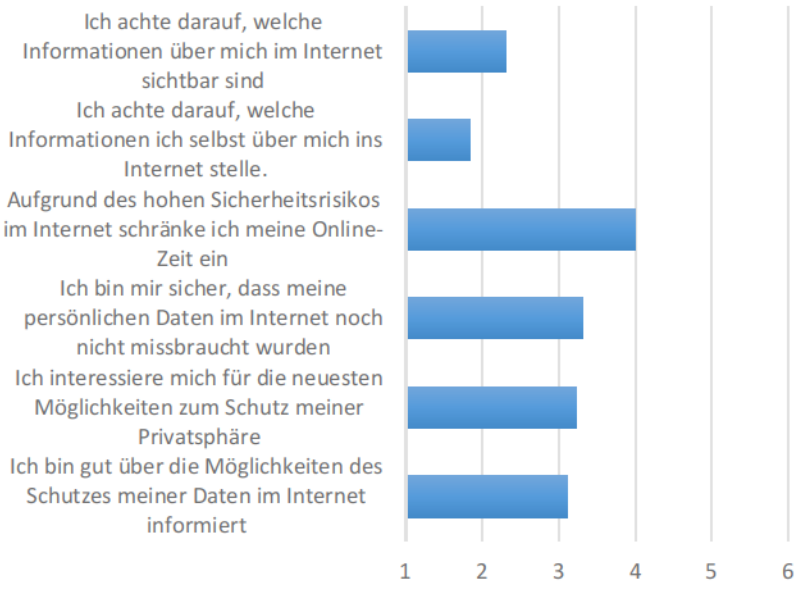


Abb. A4.13-23

Was sind für Dich Risiken im Internet?

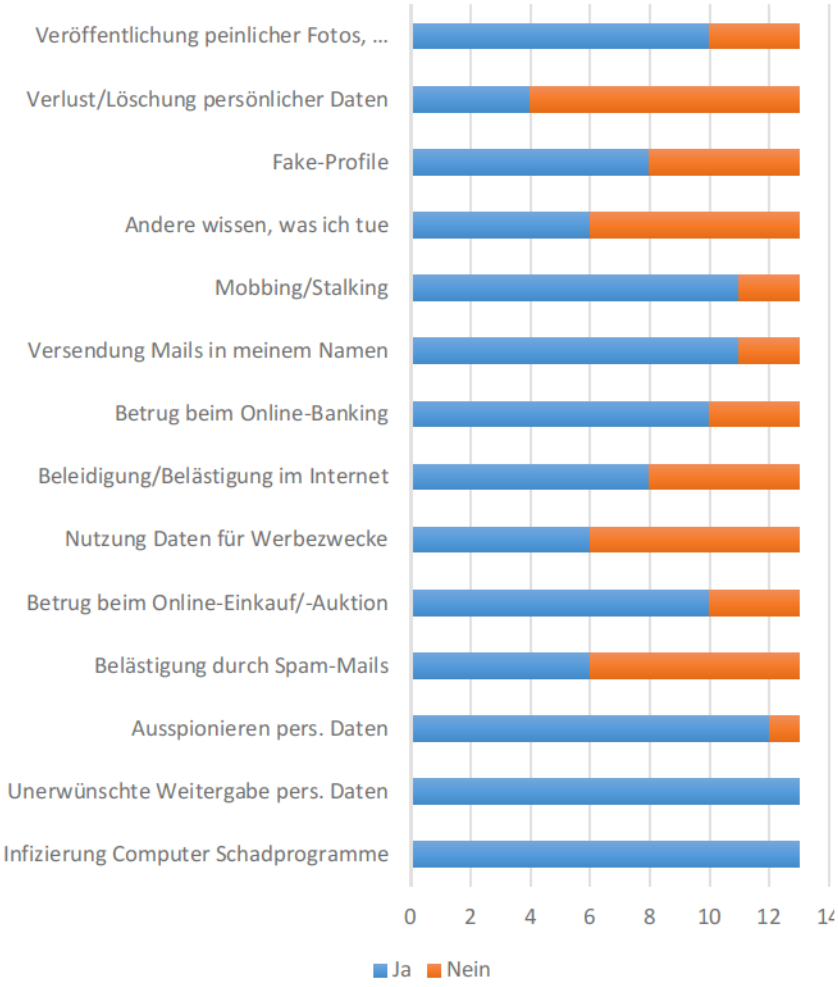


Abb. A4.13-24

Zähle Maleware auf!

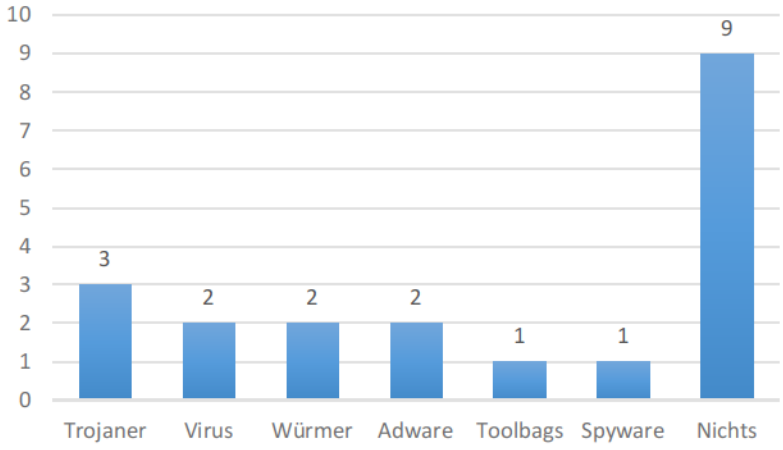


Abb. A4.13-25

Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten?

Ich …

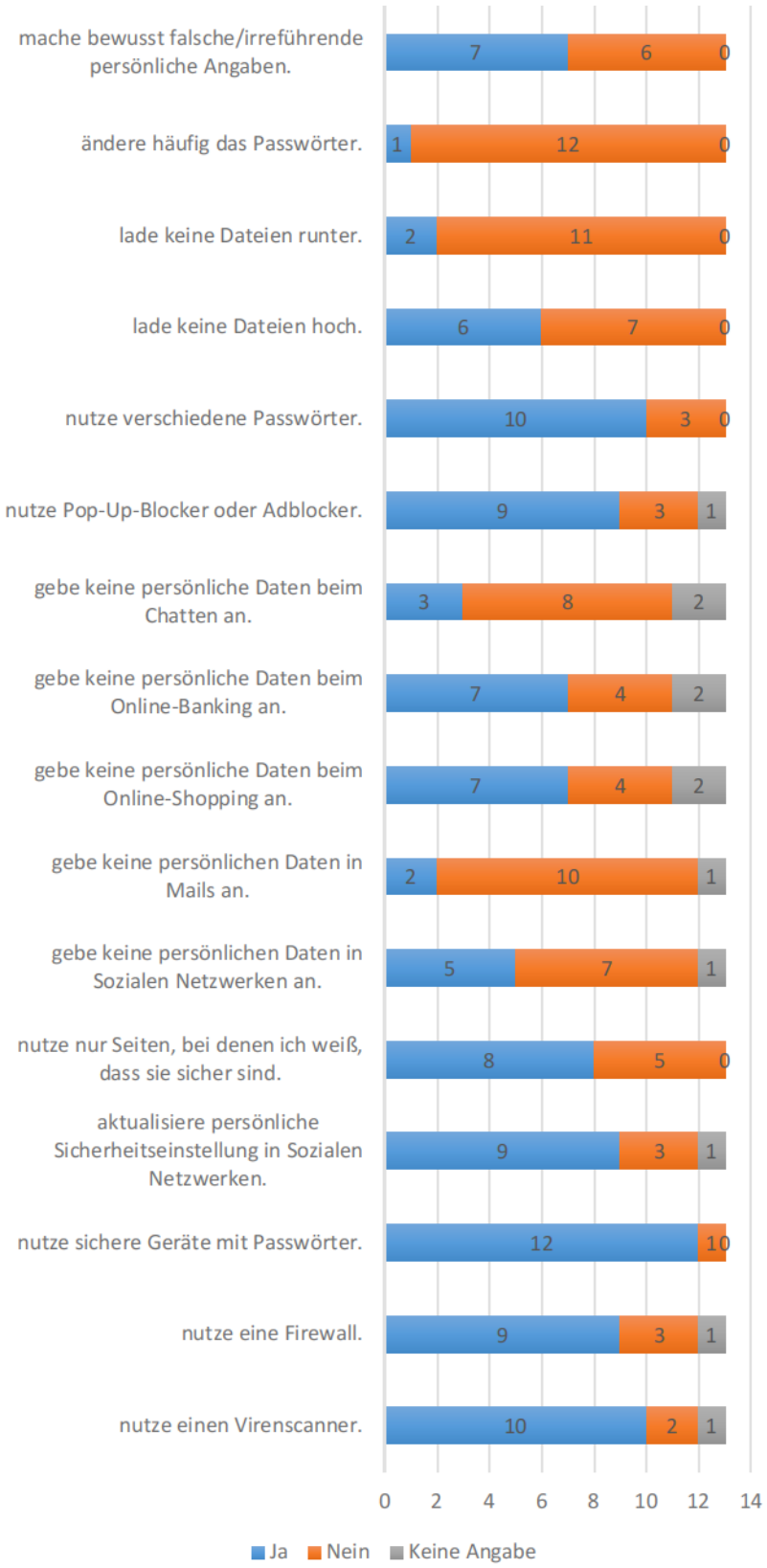


Abb. A4.13-26

Hast Du schon einmal folgende Strategie genutzt?

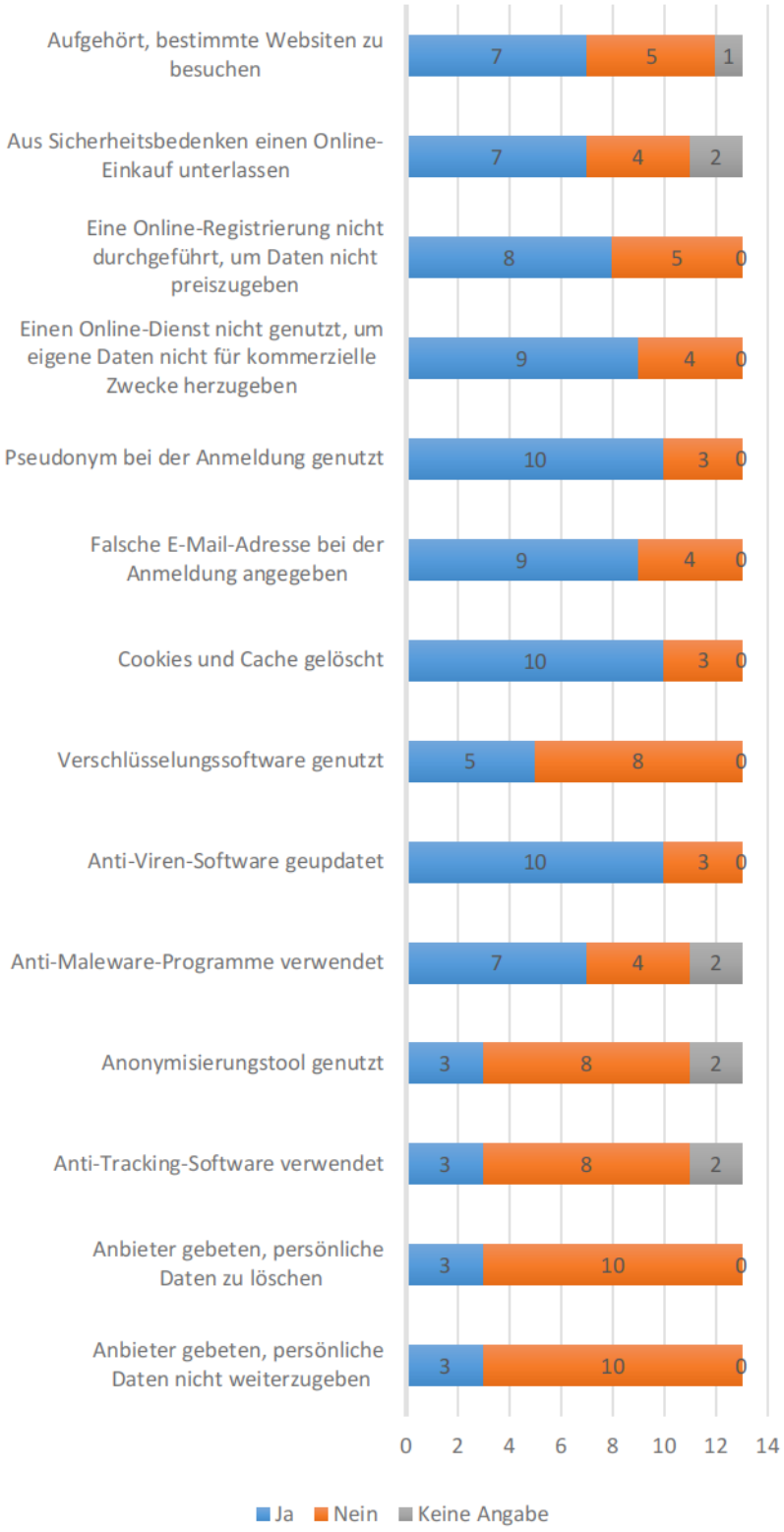


Abb. A4.13-27

Stimmen die folgenden Aussagen?

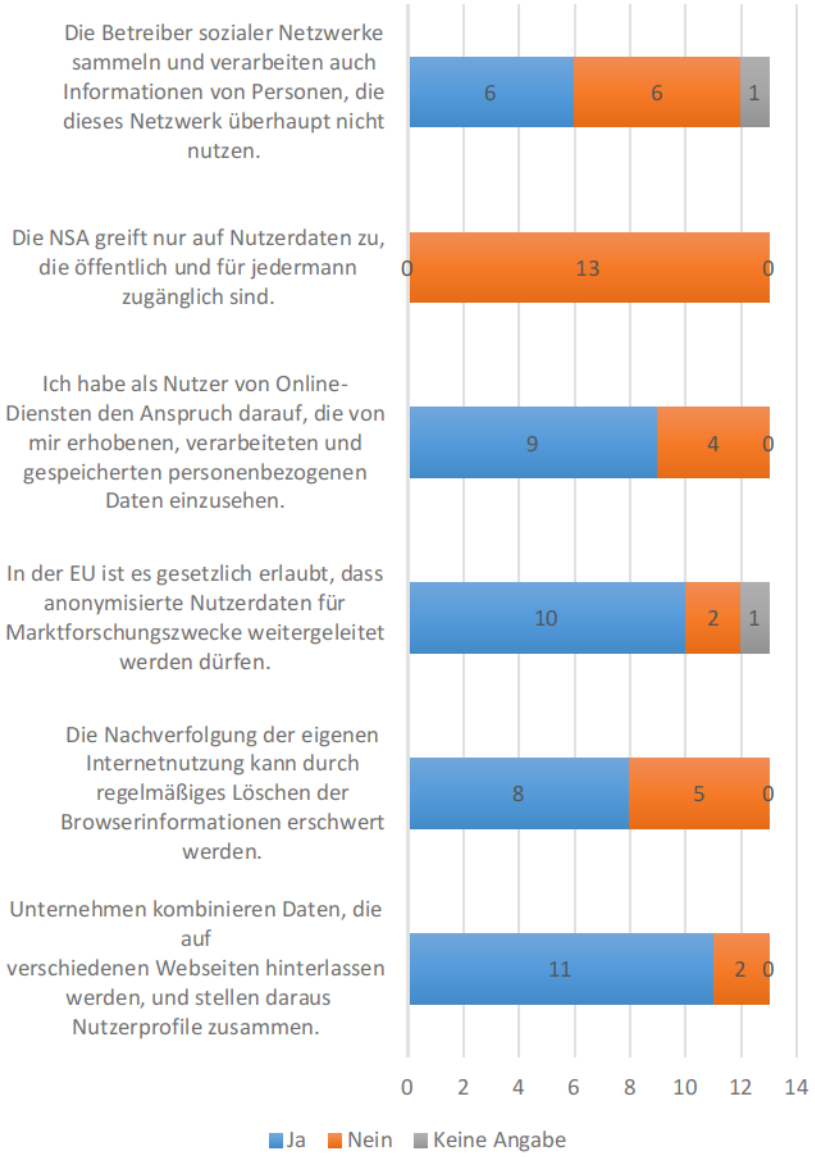


Abb. A4.13-28

Welche Deiner Rechte und Deiner Pflichten in Bezug auf Datenschutz sind Dir (bereits) bekannt?

- Rechte am eigenen Bild
- Viele aber fallen zurzeit nicht ein
- Ich sollte nur notwendige Daten angeben / Ich habe Rechte an meinem Bild, gebe sie manchmal unbewusst ab
- Urheberrechte bei Bildern
- Urheberrecht, Datenschutzbedingungen müssen gezeigt werden, Daten löschen können

Worüber hättest du gerne mehr Informationen?

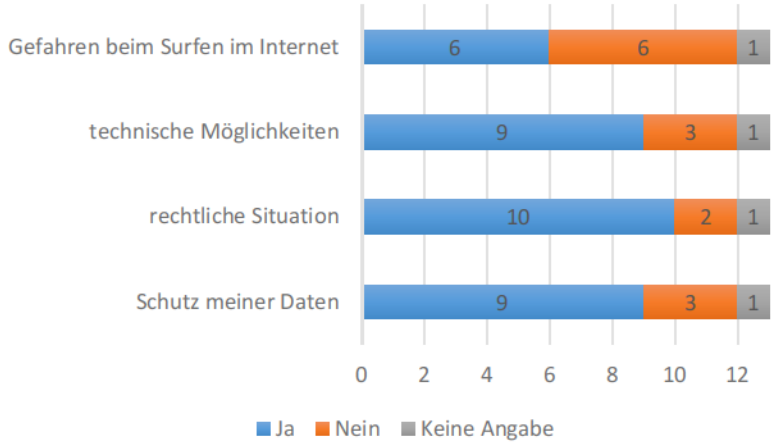
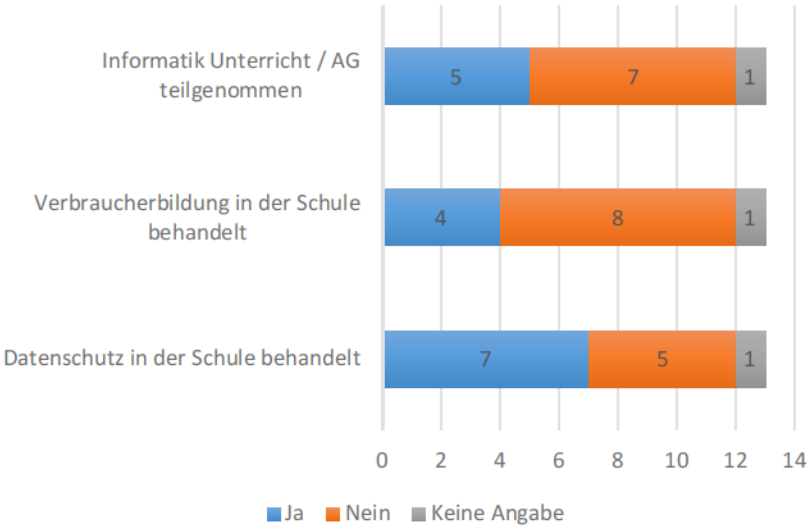


Abb. A4.13-29

Allgemeine Abfrage:



Wenn Datenschutz in der Schule behandelt worden ist, dann in den Fächern/Projekten:

- Informatik
- ITG
- Deutsch
- Kompetenztraining
- EDV
- Medienpädagogik

Abb. A4.13-30

ANHANG 4.14

Interviewfragebogen der Vorbefragung

Die folgenden Seiten umfassen den Interviewfragebogen aus der Erstbefragung im Sommer 2016; aus diesem Katalog an Fragen sind den einzelnen Gruppen nur ausgewählte Fragen gestellt worden.

Nr.	Frage	Bemerkungen
D1	Welche Nachteile können erwachsen, wenn du deine Kontodaten per WhatsApp weiterleitest?	
D2	Was leistet die Privatsphäreneinstellung bei WhatsApp?	
N4	Welche Rechte trittst du an Facebook ab, wenn du Fotos hochlädst?	
N5	Was musst du beachten, wenn du bei Facebook ein Party-Foto hochlädst, bei dem neben dir noch weitere Freunde abgebildet sind?	
N6	Auf Facebook lädst du ein Foto von einem Konzert in dein Profil hoch, auf dem geschätzt 30 Personen aus dem Publikum erkennbar sind. Was musst du beachten?	
N7	In Berlin verfolgst du eine Kundgebung mit A. Merkel, bei der du ein Foto von ihr gemacht hast. Darfst du das Foto in Facebook hochladen? Begründung!	
N10	Wie lange werden deine Facebook-Daten gespeichert?	Sollten sie sagen, dass FB-Daten gelöscht werden können, kann man daraus fehlendes Hintergrundwissen und nicht ausreichende Datenschutzkompetenz schließen
N12	Warum ist es sinnvoll, seinen Facebook-Account so gründlich wie möglich mit den erbetenen Angaben zu füllen?	(a) Damit Freunde und Bekannte mich finden; (b) Damit es nicht zu Verwechslungen kommt; (c) Es ist sinnvoll, weil … [Begründung von Schülern]
N14	Wer kann deine Facebook-Likes sehen?	Freunde, FB-Nutzer, das ganze Internet, …
N17	Welche Funktion hat der Graph-API-Explorer von Facebook? Welche Informationen kannst du durch diese abrufen?	
N24	Würdest du zur Verbesserung deiner Account-Sicherheit deine Telefonnummer angeben?	
N25	Wo werden deine Facebook-Daten gespeichert? Wie kritisch siehst du das?	
A2	Wie angemessen findest du es, dass ein QR-Code-Reader deinen Standort mittels GPS abruft?	
M3	Du erhältst eine E-Mail von einem dir unbekannten Absender. Was ist beim Öffnen der Anhängen zu beachten?	Ggf. Änderung in Absender als bekannten Freund und bei Dateitypen differenzieren

Nr.	Frage	Bemerkungen
M6	Welche Möglichkeiten hast du, damit dein E-Mail-Anbieter so wenig Informationen wie möglich aus deinem E-Mail-Verkehr erhält? Welche wendest du davon an?	
E4	Du hast nach Turnschuhen gegoogelt und im Anschluss wird dir bei der Recherche zu deinem Referat Werbung für Turnschuhe eingeblendet. Ist das Zufall? Wie stehst du zu personalisierter Werbung? Was ist deine Meinung dazu?	
B2	Was musst du bei der Nutzung eines Browsers auf deinem Gerät bei einem öffentlichem Internetzugang beachten?	
B4	Nach dem Aufruf einer URL erscheint die Meldung, dass „das Zertifikat ungültig“ ist. Was heißt das? Wie verhältst du dich?	
B6	Welche Alternativen zu Google kennst du? Welche Vorteile hat Startpage? Wie funktioniert Startpage?	
B10	Was sind sogenannte *Third-Party-Cookies*? Wozu werden sie benötigt?	
B11	Wie kannst du Chroniken löschen? Welche Vorteile haben Chroniken?	
B12	Was machst du, wenn du auf einem fremden Computer gesurft hast und den Browser schließt?	
B14	Würdest du einen Passwort-Manager in deinem Browser nutzen? Begründung!	
W4	Welche Möglichkeiten hast du, das Tracking beim Surfen zu verhindern?	
T1	Was ist VPN und was leistet VPN? Wie funktioniert VPN, welche Bedeutung hat VPN? In welchen Fällen nutzt du ein VPN?	
T4	Warum sollte ein W-LAN durch ein Passwort geschützt sein?	
T5	Was meint WPA2-PSK?	
T6	Was ist ein MAC-Filter?	
T10	Was ist ein Router, was ist ein Gateway?	
V1	Welche Bedeutung hat der private/öffentliche Schlüssel bei der Verschlüsselung?	
V5	Bei welchen Internethandlungen solltest du auf eine verschlüsselte Verbindung achten? Woran erkennst du eine verschlüsselte Verbindung?	

Nr.	Frage	Bemerkungen
V6	Was sagt das Schlosssymbol neben der URL im Browser aus? (Ggf. Screenshot)	
J1	Wie gehst du vor, wenn ein Anbieter falsche Daten über dich gespeichert hat?	
J 7	Welche Daten über dich und dein Surfverhalten dürfen ohne deine Einwilligung gespeichert werden?	
J 8	Was bedeutet informationelle Selbstbestimmung?	
J12	Wer oder was sind sog. *Whistle Blower*? Welche Bedeutung haben sie? Welchen Gefahren setzen sie sich aus?	
J 13	Eine Firma, die personenbezogene Daten von dir gespeichert hat, ist ein Tochterunternehmen eines Großkonzerns, der wiederum viele weitere Tochterunternehmen unterhält und mit externen Dienstleistern zusammenarbeitet. Ist es legal, dass die Daten über dich untereinander ausgetauscht werden? Begründung!	
J 15	Der Staat bzw. die Politiker behaupten, dass sie möglichst viel von den Bürgern über ihre Netzaktivitäten und deren Inhalte wissen müssen (und damit in deren digitale Privatsphäre eindringen), um Gefahren von Terror u. ä. rechtzeitig abwehren zu können. Wie beurteilst du das? Wie weit darf der Staat gehen?	
S4	Was ist im Fall von Cybermobbing zu tun?	
S6	Was steckt hinter dem Begriff *Datenschutz*?	
S8	Wobei gibst du bewusst oder unbewusst Daten von dir preis?	
S11	Welche Gedanken machst du dir, bevor du dich bei einem Dienst anmeldest? Begründung!	
O2	Welches Verfahren ist das sicherste bei Online-Überweisungen?	
O1	Wie verhältst du dich bei einer Aufforderung (per E-Mail) einem Link zur Bankseite zu folgen und dort sich mit Kontonummer und PIN zu legitimieren?	

ANHANG 4.15

Fragebogen der Prä-Pilotierung

Die folgenden Seiten umfassen den aus Lime Survey exportierten Fragebogen der Prä-Pilotierung vom Sommer 2017.

Herzlich Willkommen zur Umfrage zum Thema Datenschutzkompetenz von Schülerinnen und Schülern.

In dieser Umfrage soll überprüft werden, wie gut und verständlich die Software ist, daher sind die Daten erstmal irrelevant. Ich bitte trotzdem um gewissenhaftes ausfüllen, da diese Prä-Pilotierung die Umfrage verbessern soll.

Generell solltest du die Aufgaben aufmerksam, genau und komplett lesen und deine Antworten frei und ehrlich geben. Da die Umfrage anonym ist, können deinen Antworten auch nicht auf deine Person zurückverfolgt werden.

Teil A: Gruppe Persönlicher Fragen

A1.

Hier muss ein Code eingetragen werden, anhand dessen wir den Rückmeldebogen / deine Rückmeldung nachvollziehen können. Bist du ein Schüler / eine Schülerin aus dem MNU-Kurs in München, so erhälst du diesen mit dem Rückmeldebogen.

P00 (Dies stellt ein internes Kürzel dar)

A2. Wie alt bist du?

P002

A3. Angabe zum Geschlecht:

P001

- ☐ weiblich
- ☐ männlich

A4. Ich habe Zugang zu:

P004

- ☐ Laptop
- ☐ Desktop-Computer (PC)
- ☐ Smartphone
- ☐ Spielekonsole
- ☐ Tablet

Sonstiges ☐

Sonstiges _____

A5. Wie viele Stunden verbringst du pro Woche am Laptop?

P006a

0-5 ☐
6-10 ☐
11-15 ☐
16-20 ☐
21-25 ☐
26-30 ☐
>30 ☐

A6. Wie viele Stunden verbringst du pro Woche am Desktop-Computer (PC)?

P006c

1-5 ☐
6-10 ☐
11-15 ☐
16-20 ☐
21-25 ☐
26-30 ☐
>30 ☐

A7. Wie viele Stunden verbringst du pro Woche am Smartphone?

P006b

1-5 ☐
6-10 ☐
11-15 ☐
16-20 ☐
21-25 ☐
26-30 ☐
>30 ☐

A8. **Wie viele Stunden verbringst du pro Woche an der Spielekonsole?**

P006d

- 1-5 ☐
- 6-10 ☐
- 11-15 ☐
- 16-20 ☐
- 21-25 ☐
- 26-30 ☐
- >30 ☐

A9. **Wie viele Stunden verbringst du pro Woche am Tablet?**

P006e

- 1-5 ☐
- 6-10 ☐
- 11-15 ☐
- 16-20 ☐
- 21-25 ☐
- 26-30 ☐
- >30 ☐

A10. **Wie viele Stunden verbringst du pro Woche an dem Gerät, welches du in obiger Liste bei Sonstiges eingetraten hast?**

P006

- 1-5 ☐
- 6-10 ☐
- 11-15 ☐
- 16-20 ☐
- 21-25 ☐
- 26-30 ☐
- >30 ☐

A11. **Folgende Geräte nutze ich alleine / gehören mir:**

P005

- Laptop ☐
- Desktop-Computer (PC) ☐
- Smartphone ☐

Spielekonsole ☐

Tablet ☐

Sonstiges ☐

Sonstiges

A12.

Nimmst du das Smartphone immer und überall mit oder gibt es Phasen, in denen du es bewusst weglegst / abgenommen bekommst?

P007

Ich habe mein Smartphone immer zur Hand. ☐

Ich lege das Smartphone freiwillig weg. ☐

Ich muss das Smartphone weglegen, bzw. bekomme es abgenommen. ☐

A13. Wie lange sind die Smartphone-Pausen im Schnitt im Laufe eines Tages?

P007Z

kürzer als eine Stunde ☐

1 Std. ☐

2 Std. ☐

3 Std ☐

4-5 Std. ☐

6-7 Std. ☐

8-10 Std. ☐

länger als zehn Stunden. ☐

A14. Wurden Themen der Verbraucherbildung im Unterricht behandelt?

P10

Finanzen und Konsum ☐

Gesundheit und Ernährung ☐

Datenschutz ☐

Keines der Themen wurde im Unterricht behandelt ☐

A15. In welchen Fächern wurden das Thema "Finanzen und Konsum" des Verbraucherschutzes behandelt?

P10b

Deutsch ☐

- Englisch ☐
- Französich ☐
- Latein ☐
- andere Fremdsprache ☐
- Geschichte ☐
- Sozialkunde ☐
- Erdkunde ☐
- Mathematik ☐
- Chemie ☐
- Physik ☐
- Biologie ☐
- Bildende Kunst ☐
- Musik ☐
- Darstellendes Spiel ☐
- Katholische Religion ☐
- Evangelische Religion ☐
- Ethik ☐
- sonstige Religion ☐
- Sport ☐
- Informatik ☐
- ITG ☐
- Philosophie ☐
- Sonstiges ☐

Sonstiges

A16. In welchn Fächern wurden das Thema "Gesundheit und Ernährung" des Verbraucherschutzes behandelt?

P10d

- Deutsch ☐
- Englisch ☐

Französich ☐
Latein ☐
andere Fremdsprache ☐
Geschichte ☐
Sozialkunde ☐
Erdkunde ☐
Mathematik ☐
Chemie ☐
Physik ☐
Biologie ☐
Bildende Kunst ☐
Musik ☐
Darstellendes Spiel ☐
Katholische Religion ☐
Evangelische Religion ☐
Ethik ☐
sonstige Religion ☐
Sport ☐
Informatik ☐
ITG ☐
Philosophie ☐
Sonstiges ☐

Sonstiges

A17. In welchen Fächern wurden das Thema "Datenschutz" des Verbraucherschutzes behandelt?

P10c

Deutsch ☐
Englisch ☐
Französich ☐

Latein ☐
andere Fremdsprache ☐
Geschichte ☐
Sozialkunde ☐
Erdkunde ☐
Mathematik ☐
Chemie ☐
Physik ☐
Biologie ☐
Bildende Kunst ☐
Musik ☐
Darstellendes Spiel ☐
Katholische Religion ☐
Evangelische Religion ☐
Ethik ☐
sonstige Religion ☐
Sport ☐
Informatik ☐
ITG ☐
Philosophie ☐
Sonstiges ☐

Sonstiges

A18. Hast Du bisher (seit Klassenstufe 5) an einem Informatikunterricht oder einer AG Informatik regelmäßig teilgenommen?

P11

Ja ☐
Nein ☐

A19. **In welcher/n Klassenstufe/n hast du daran teilgenommen und mit wie vielen Stunden?**

P11b

5	
6	
7	
8	
9	
10	
11	
12	
13	

Teil B: Internet

B1. **Wozu nutzt Du das Internet?**

I01

- ☐ zum Chatten
- ☐ zum Mailen
- ☐ um in Soziale Netzwerken aktiv zu sein
- ☐ zum Twittern
- ☐ um in Diskussionsforen aktiv zu sein
- ☐ um Webblogs zu lesen
- ☐ zum Instant-Messaging
- ☐ zum Skypen
- ☐ zum Filme schauen
- ☐ zum Musikvideo schauen
- ☐ zum Fernsehen
- ☐ um Online-Games zu spielen
- ☐ zum Musik hören
- ☐ um Bilder-Plattformen zu durchsuchen

um mich treiben zu lassen ☐
zum Online-Shoppen ☐
um Bezahldienste zu nutzen ☐
um an Versteigerungen teilzunehmen ☐
zum Online-Banking ☐
um mich zu informieren (z.B. auf Wikipedia) ☐
um Nachrichtenportale zu lesen ☐
um Newsgroup/Foren zu lesen ☐
um Mediatheken zu nutzen ☐
um mich speziell für die Schule zu informieren ☐
Sonstiges ☐

Sonstiges

B2. Welchen Gerätetyp nutzt Du für den Internetzugang?

I02

Handy / Smartphone ☐
Computer / Laptop ☐
Tablet-PC ☐
Spielekonsole ☐
Fernseher ☐
MP3-Player ☐
E-Book-Reader ☐
Sonstiges ☐

Sonstiges

B3. Auf welche Weise bist du im Netz?

I03

konsumierend (z.B. Youtube-Videos anschauen, Texte lesen) ☐
partizipierend (z.B. Youtube-Videos bewerten, Kommentare schreiben) ☐
produzierend (z.B. Youtube-Videos hochladen, Texte selber schreiben) ☐
Nicht-Nutzer ☐

B4. Wie häufig bist du im Internet?

I04a:

- ☐ täglich (6-7 Tage pro Woche)
- ☐ mehrmals pro Woche (3-5 Tage pro Woche)
- ☐ ein paar mal im Monat (ca. 8 Tage im Monat)
- ☐ selten (1-5 Tage im Monat)
- ☐ nie

B5. Wie groß ist dann der Zeitumfang im Schnitt, in dem du das Internet nutzt?

I04 b

- ☐ weniger als eine Stunde
- ☐ ein bis zwei Stunden
- ☐ zwei bis vier Stunden
- ☐ mehr als vier Stunden

B6. Was sind deine Motive für die Internetnutzung?

I05

- ☐ Unterhaltung
- ☐ Beziehungspflege
- ☐ Informationsbeschaffung
- ☐ Zugehörigkeitsgefühl
- ☐ Knüpfen neuer Kontakte
- ☐ Selbstdarstellung
- ☐ Realitätsflucht
- ☐ Sonstiges

Sonstiges

B7. Welchen / Welche Messenger nutzt du?

I06

- ☐ WhatsApp
- ☐ Snapchat
- ☐ Telegram
- ☐ Threema
- ☐ BlackBerry Messenger

Hangout ☐
Xabber ☐
ChatOn ☐
Skype ☐
Instagram ☐
SMS ☐
Facebook Messenger ☐
TextSecure ☐
Kik ☐
Sonstiges ☐

Sonstiges

B8. Welche Sozialen Netzwerke nutzt du?

I07

Facebook ☐
Google+ ☐
Twitter ☐
Youtube ☐
Tumblr ☐
Instagram ☐
MySpace ☐
LinkedIn ☐
Pinterest ☐
Sonstiges ☐

Sonstiges

B9. Welche/n Browser nutzt du?

I08

Firefox ☐
Internet Explorer ☐
Chrome ☐

Safari ☐
Opera ☐
Sea Monkey ☐
Tor ☐
Sonstiges ☐

Sonstiges

B10. Welche Browsertools nutzt du?

I09

Ghostery ☐
Adblock Plus ☐
Bug me not ☐
Firebug ☐
Flagfox ☐
Self-Destructing-Cookies ☐
Keine ☐
Sonstiges ☐

Sonstiges

B11. Welche der folgenden Apps verwendest du?

I10

Antiviren Software ☐
Clean Master ☐
My Permissions Datenschutz ☐
Keine ☐
Sonstiges ☐

Sonstiges

B12. Wenn du an die eigenen Fähigkeiten/Internetkompetenzen denkst, für wie kompetent hältst Du Dich persönlich bei den folgenden Punkten?

I11b

	nicht kompetent				sehr kompetent
Informationen im Internet recherchieren können	☐	☐	☐	☐	☐
Sich mit anderen im Internet vernetzen können	☐	☐	☐	☐	☐
Die eigene Person im Internet angemessen darstellen können	☐	☐	☐	☐	☐
Die eigene Privatsphäre im Internet gut schützen können	☐	☐	☐	☐	☐
Gewalttätige, rassistische und pornografische Inhalten ausweichen können	☐	☐	☐	☐	☐
Konsequenzen des eigenen Hochladens im digitalen Raum abschätzen können	☐	☐	☐	☐	☐
Zwischen privaten und öffentlichen Räumen im Internet unterscheiden können	☐	☐	☐	☐	☐
Vertrauenswürdigkeit von Informationsquellen im Internet einschätzen können	☐	☐	☐	☐	☐
Das Internet und digitale Medien zu kreativen Betätigungen und der Gestaltung eigener Inhalte nutzen können	☐	☐	☐	☐	☐

B13. Welche Internetseiten nutzt Du am liebsten bzw. auf welchen Seiten gehst du am häufigstem?

I12 - Bei mehreren Angaben in Sonstigem, bitte durch Komata trennen.

- ☐ Focus
- ☐ Youtube
- ☐ Spektrum der Wissenschaft
- ☐ Wikipedia
- ☐ Google+
- ☐ Gmail
- ☐ Amazon
- ☐ Wetter.com
- ☐ Google
- ☐ GMX.de
- ☐ WhatsApp
- ☐ Pinterest
- ☐ Web.de
- ☐ Facebook

Instagram ☐
9gag ☐
Sonstiges ☐

Sonstiges

B14. Wie wichtig ist dir jeweils einer der u.s. Aspekte bei der Nutzung eines Messengers?

I13

	sehr wichtig				unwichtig
Verschlüsselung bei der Übermittlung	☐	☐	☐	☐	☐
Provider kann verschlüsselte Mitteilungen lesen	☐	☐	☐	☐	☐
Identifikationsmöglichkeit des Gesprächspartners	☐	☐	☐	☐	☐
Veröffentlichung des Programmcodes zwecks Verifikation	☐	☐	☐	☐	☐
Schnelligkeit der Übermittlung	☐	☐	☐	☐	☐
Zusatz wie Stickers, Sprachnachrichten, Telefonieren, Videoanrufe, ...	☐	☐	☐	☐	☐
Dass das Sicherheitsdesign öffentlich dokumentiert ist	☐	☐	☐	☐	☐
Zertifizierung des Programmcodes	☐	☐	☐	☐	☐
Nutzerzahlen	☐	☐	☐	☐	☐
Anzahl der Dateiformate, die weitergeleitet werden können	☐	☐	☐	☐	☐
Sicherheit der Nachrichten bei Diebstahl des Schlüssels	☐	☐	☐	☐	☐

B15. Welche Informationen würdes Du über Dich im Internet veröffentlichen?

I14

Vorname ☐
Nachname ☐
Nickname ☐
Geburtstag ☐
Ausbildung/Beruf ☐
E-Mail-Adresse ☐
Post-Adresse ☐

- [ ] Fotos
- [ ] Private Kontakte
- [ ] Berufl. Kontakte
- [ ] Beziehungsstatus
- [ ] Lieblingsfilme / -serien / -bücher / -musik
- [ ] Interessen/Hobbies
- [ ] Instant-Messenger Kontakt
- [ ] Handy-Nummer
- [ ] Telefon-Nr.
- [ ] Politische Einstellung
- [ ] Sexuelle Orientierung
- [ ] Eigene Erlebnisse
- [ ] Eigene Gedanken
- [ ] Eigene Gefühle
- [ ] Eigene Sorgen/Ängste
- [ ] Religion
- [ ] überhaupt keine
- [ ] Sonstiges

Sonstiges

B16. Mit wem teilst Du die Informationen in sozialen Netzwerken?

I15

- [ ] nur Nutzer selbst
- [ ] ausgewählte Kontakte
- [ ] alle Kontakte
- [ ] Kontakte + deren Freunde
- [ ] alle Mitglieder
- [ ] Öffentliches Netz

B17. Mit wem teilst Du die Informationen auf sonstigen Plattformen (Youtube, Instagram, Snapchat...)?

I16

- ☐ nur Nutzer selbst
- ☐ ausgewählte Kontakte
- ☐ alle Kontakte
- ☐ Kontakte + deren Freunde
- ☐ alle Mitglieder
- ☐ Öffentliches Netz

B18. Zu deinen Einstellungen zur Privatsphäre in sozialen Netzwerken:

Hast du Einstellungen zur Privatsphäre geändert?

I17

- ☐ Ja
- ☐ Nein

B19. Was hast du geändert?

I17b

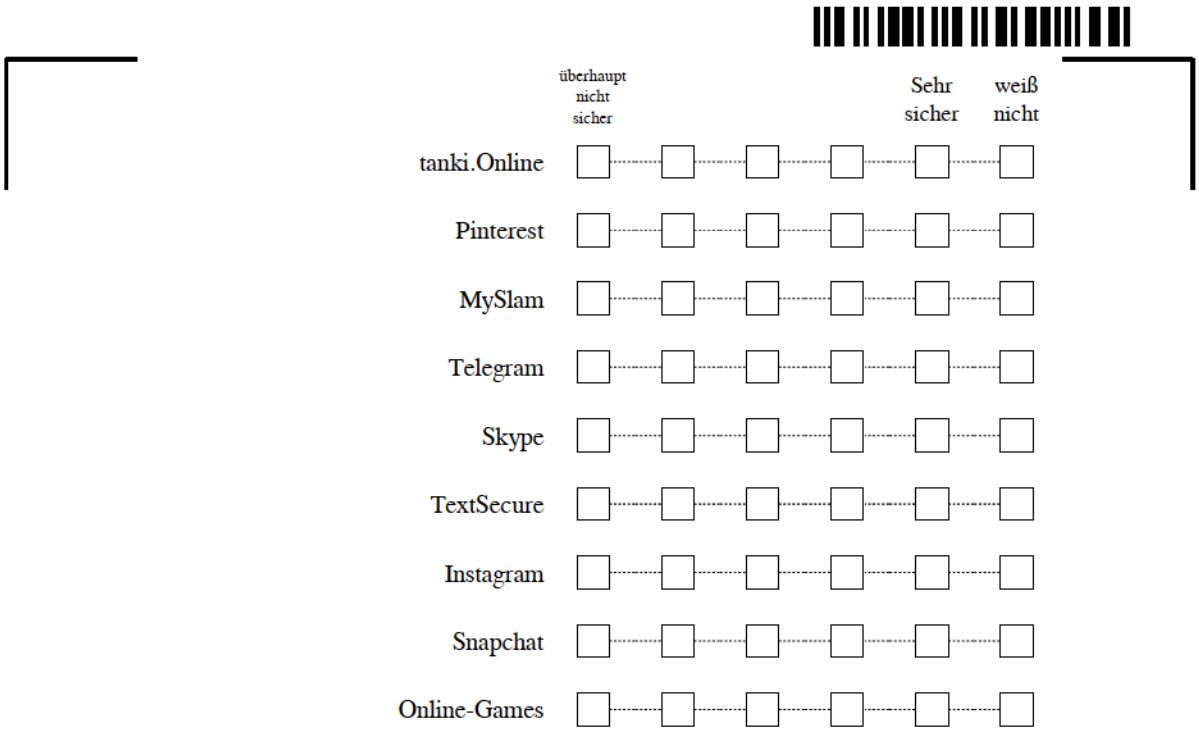
- ☐ Sichtbarkeit des Profils
- ☐ Sichtbarkeit der Posts
- ☐ Wer auf meine Seiten posten darf
- ☐ Wer mich kontaktieren darf
- ☐ Für wen ich zu finden bin
- ☐ Sonstiges

Sonstiges

B20. In Bezug auf Datensicherheit fühle ich mich in folgenden Communities ...

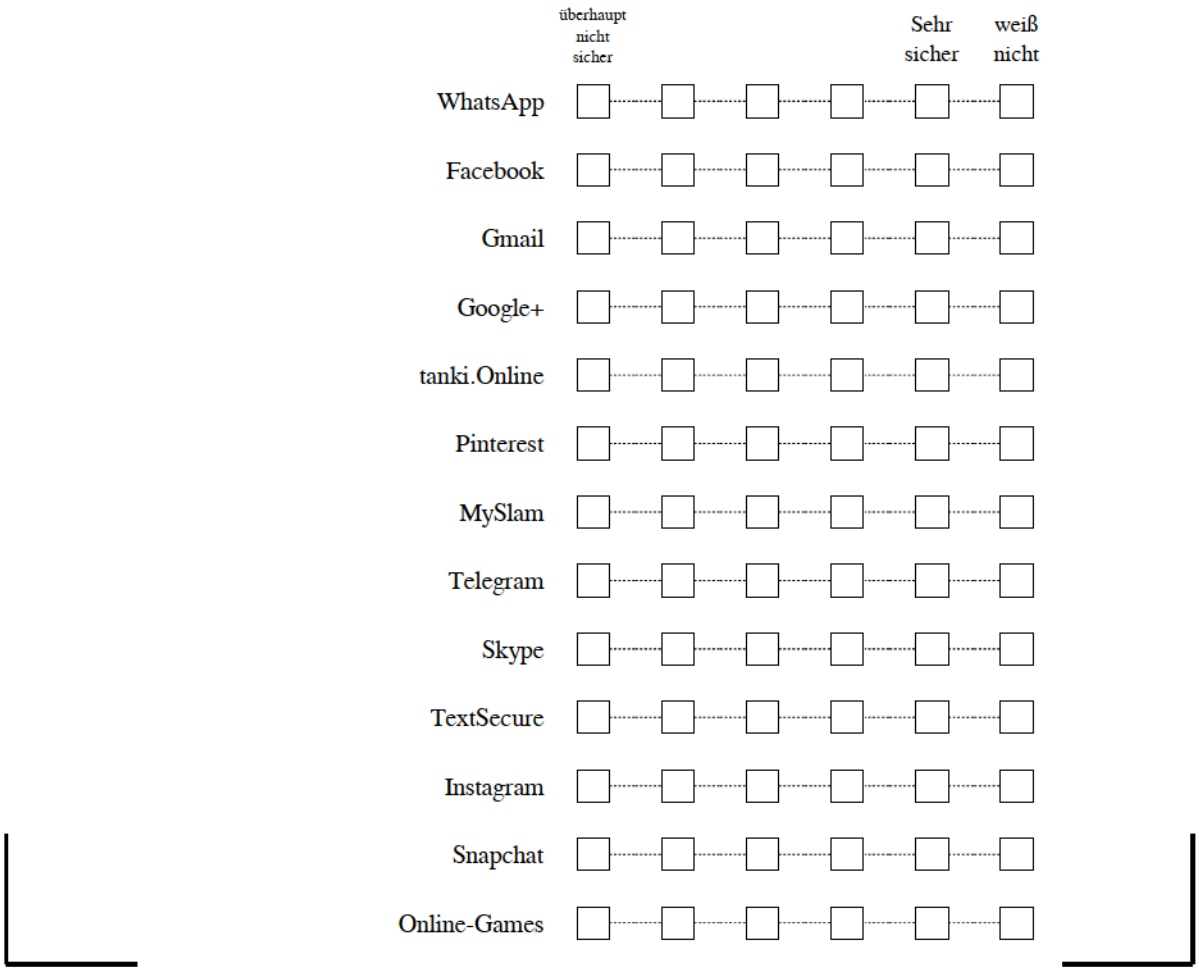
I18

	überhaupt nicht sicher				Sehr sicher	weiß nicht
WhatsApp	☐	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐	☐
Gmail	☐	☐	☐	☐	☐	☐
Google+	☐	☐	☐	☐	☐	☐



B21. In Bezug auf Datensicherheit fühle ich mich bei folgenden Messengern …

I18b



B22. Wie sehr vertraust du ...

I19

	sehr					gar nicht	weiß nicht
WhatsApp	☐	☐	☐	☐	☐	☐	☐
Facebook	☐	☐	☐	☐	☐	☐	☐
Gmail	☐	☐	☐	☐	☐	☐	☐
Google+	☐	☐	☐	☐	☐	☐	☐
tanki.Online	☐	☐	☐	☐	☐	☐	☐
Amazon	☐	☐	☐	☐	☐	☐	☐
Pinterest	☐	☐	☐	☐	☐	☐	☐
MySlam	☐	☐	☐	☐	☐	☐	☐
Telegram	☐	☐	☐	☐	☐	☐	☐
Skype	☐	☐	☐	☐	☐	☐	☐
Textsecure	☐	☐	☐	☐	☐	☐	☐
Instagram	☐	☐	☐	☐	☐	☐	☐
Snapchat	☐	☐	☐	☐	☐	☐	☐
Online-Games	☐	☐	☐	☐	☐	☐	☐

B23. Was glaubst du, wie sicher sind persönliche Daten im Internet?

I20

sehr sicher				gar nicht sicher	weiß nicht
☐	☐	☐	☐	☐	☐

B24. Welche Aussagen treffen für Dich zu?

I21

	sehr					gar nicht	weiß nicht
Ich bin gut über die Möglichkeiten des Schutzes meiner Daten im Internet informiert.	☐	☐	☐	☐	☐	☐	☐
Ich interessiere mich für die neuesten Möglichkeiten zum Schutz meiner Privatsphäre im Internet.	☐	☐	☐	☐	☐	☐	☐
Ich bin mir sicher, dass meine persönlichen Daten im Internet noch nicht missbraucht wurden.	☐	☐	☐	☐	☐	☐	☐
Aufgrund des hohen Sicherheitsrisikos im Internet schränke ich meine Online-Zeit ein.	☐	☐	☐	☐	☐	☐	☐

	sehr				gar nicht	weiß nicht
Ich achte darauf, welche Informationen ich selbst über mich ins Internet stelle.	☐	☐	☐	☐	☐	☐
Ich achte darauf, welche Informationen über mich im Internet sichtbar sind.	☐	☐	☐	☐	☐	☐
Meine persönlichen Daten im Internet sind sicher.	☐	☐	☐	☐	☐	☐

B25. Was sind für dich Risken im Internet?

I22

	Ja	Unsicher	Nein
Infizierung des Computers mit Schadprogrammen	☐	☐	☐
Unerwünschte Weitergabe von persönlichen Daten an Dritte	☐	☐	☐
Ausspionieren meiner persönlichen Daten	☐	☐	☐
Belästigung durch Spam-Mails	☐	☐	☐
Betrug beim Online-Einkauf/Online-Auktion	☐	☐	☐
Nutzung meiner Daten für Werbezwecke	☐	☐	☐
Beleidigung oder Belästigung im Internet	☐	☐	☐
Betrug beim Online-Banking	☐	☐	☐
Versendung unerwünschter E-Mails in meinem Namen	☐	☐	☐
Mobbing/Stalking/Beleidigungen	☐	☐	☐
Andere wissen, was ich tue, oder kennen meinen Aufenthaltsort	☐	☐	☐
Fake-Profile	☐	☐	☐
Verlust oder Löschung persönlicher Daten	☐	☐	☐
Veröffentlichung peinlicher/intimer Chats/Fotos/…	☐	☐	☐

B26. Welche Maßnahmen ergreifst Du, um die Internetnutzung sicher zu gestalten?

Ich...

I24

	Ja	Unsicher	Nein
... nutze einen Virenscanner.	☐	☐	☐
... nutze eine Firewall.	☐	☐	☐

	Ja	Unsicher	Nein
... nutze sichere Geräte mit persönlichem Passwort.	☐	☐	☐
... aktualisiere persönliche Sicherheitseinstellungen in sozialen Netzwerken gegenüber Grundeinstellungen.	☐	☐	☐
... nutze nur Seiten, bei denen ich weiß, dass sie sicher sind.	☐	☐	☐
... gebe keine persönlichen Daten in sozialen Netzwerken preis.	☐	☐	☐
... gebe keine persönlichen Daten beim Mailen preis.	☐	☐	☐
... gebe keine persönlichen Daten beim Online-Shopping preis.	☐	☐	☐
... gebe keine persönlichen Daten beim Online-Banking preis.	☐	☐	☐
... gebe keine persönlichen Daten beim Chatten preis.	☐	☐	☐
... nutze Pop-Up- Blocker oder Adblocker.	☐	☐	☐
... nutze verschiedene Passwörter.	☐	☐	☐
... lade keine Dateien hoch.	☐	☐	☐
... lade keine Dateien herunter.	☐	☐	☐
... ändere häufig das Passwort.	☐	☐	☐
... mache bewusst falsche/irreführende persönliche Angaben.	☐	☐	☐

B27. Hast Du schon einmal folgende Strategie genutzt?

I25

	Ja	Unsicher	Nein
Aufgehört bestimmte Webseiten zu besuchen	☐	☐	☐
Aus Sicherheitsbedenken einen Online-Einkauf unterlassen	☐	☐	☐
Eine Online-Registrierung nicht durchgeführt, um Daten nicht angeben zu müssen	☐	☐	☐
Einen Online-Dienst nicht genutzt, um eigene Daten nicht für kommerzielle Zwecke herzugeben	☐	☐	☐
Ein Pseudonym bei der Anmeldung benutzt	☐	☐	☐
Eine falsche E-Mail-Adresse bei der Anmeldung angeben	☐	☐	☐
Im Internetbrowser die Cookies und den Cache gelöscht	☐	☐	☐
Eine Verschlüsselungssoftware benutzt	☐	☐	☐

	Ja	Unsicher	Nein
Anti-Viren-Software regelmäßig geupdatet	☐	☐	☐
Nutzung von Anti-Malware-Programmen	☐	☐	☐
Nutzung von Anonymisierungstools	☐	☐	☐
Nutzung von Anti-Tracking-Software	☐	☐	☐
Anbieter gebeten, persönliche Daten zu löschen	☐	☐	☐
Anbieter gebeten, persönliche Daten nicht weiterzugeben	☐	☐	☐

B28. Stimmen die folgenden Aussagen:

I26

	Ja	Nein	Weiß ich nicht
Die Betreiber sozialer Netzwerke sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk überhaupt nicht nutzen.	☐	☐	☐
Die NSA greift nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.	☐	☐	☐
Ich habe als Nutzer von Online-Diensten den Anspruch darauf, die von mir erhobenen, verarbeiteten und gespeicherten personenbezogenen Daten einzusehen.	☐	☐	☐
In der EU ist es gesetzlich erlaubt, dass anonymisierte Nutzerdaten für Marktforschungszwecke weitergeleitet werden dürfen.	☐	☐	☐
Die Nachverfolgung der eigenen Internetnutzung kann durch regelmäßiges Löschen der Browserinformationen erschwert werden.	☐	☐	☐
Unternehmen kombinieren Daten, die auf verschiedenen Webseiten hinterlassen werden, und stellen daraus Nutzerprofile zusammen.	☐	☐	☐

B29. Welche deiner Rechte und Deiner Pflichten in Bezug auf Datenschutz sind Dir (bereits) bekannt?

B30. Worüber hättest Du gerne mehr Informationen?

I28

	Ja	Unsicher	Nein
… zum Schutz meiner Daten im Internet	☐	☐	☐
… zur rechtlichen Situation in Bezug auf Datenschutz	☐	☐	☐
… zu technischen Möglichkeiten	☐	☐	☐

	Ja	Unsicher	Nein
… zu den Gefahren beim Surfen im Internet	☐	☐	☐

Teil C: OPLIS

In folgender Gruppe werden Fragen zur Online-Privatheitskompetenz (vlg. Masur, Teutsch & Trepte) gestellt.

C1. Was verbirgt sicht hinter dem Begriff "Browserverlauf"?

Im Browserverlauf werden ...

TEC01

- ... die Adressen der besuchten Websites gespeichert. ☐
- ... Cookies von besuchten Websites abgelegt. ☐
- ... potenziell infizierte Websites separat abgelegt. ☐
- ... je nach Browsertyp unterschiedliche Informationen über den Nutzer gespeichert. ☐
- Weiß nicht ☐

C2. Was ist ein "Cookie"?

TEC02

- Ein Computer-Virus, das man sich beim Besuch einer Website einfangen kann. ☐
- Ein Browser-Plugin, das sicheres Surfen gewährleistet. ☐
- Ein Programm, mit dem man die Datenspeicherung von Web-Anbietern unterbinden kann. ☐
- Eine Text-Datei, die es Websites ermöglicht, den Nutzer beim erneuten Besuch wiederzuerkennen. ☐
- Weiß nicht ☐

C3. Was versteht man unter dem Begriff "Cache"?

TEC03

- Einen Puffer-Speicher, der das Surfen im Internet beschleunigt. ☐
- Ein Browser-Plug-In, welches den Datentransfer beim Surfen verschlüsselt. ☐
- Ein Programm, welches Daten über den Internetnutzer gezielt ausspioniert und an Dritte weiterleitet. ☐
- Ein Programm, welches Daten auf eine externe Festplatte kopiert, um diese vor Datenklau zu schützen. ☐
- Weiß nicht ☐

C4. Was versteht man unter einem "Trojaner"?

Ein Trojaner ist ein Computerprogramm, dass ...

TEC04

- ... als nützliche Anwendung getarnt ist, im Hintergrund aber eine andere Funktion erfüllt. ☐
- ... den Rechner vor Viren und anderen Schadprogrammen schützt. ☐
- ... nur zum Spaß entwickelt wurde und keine spezifische Funktion hat. ☐

... als Computervirus in den 90ern Schaden anrichtete, heute aber nicht mehr existiert. ☐

Weiß nicht ☐

C5. Was ist eine "Firewall"?

TEC05

Ein Sicherungssystem, das den Computer vor unerwünschten Netzangriffen schützen soll. ☐

Ein veraltetes Schutzprogramm gegen Computer-Viren. ☐

Ein Browser-Plugin, das sicheres Surfen ermöglicht. ☐

Eine neue technische Entwicklung, die verhindert, dass Daten bei einem Kurzschluss verloren gehen. ☐

Sie schützt den Rechner vor Überhitzung und den daraus entstehenden Schwelbränden, die ohne Firewall auf der Hauptplatine auftreten können. ☐

Sie überwacht den eingehenden und ausgehenden Datenverkehr im Internet und kann so die Verbreitung von Phishing-Mails eindämmen. ☐

Sie überwacht den eingehenden und ausgehenden Datenverkehr im Internet und kann so die Verbreitung von Viren und anderen Schadprogrammen eindämmen. ☐

Sie überwacht den eingehenden Datenverkehr und kann so bei Ermittlungen gegen Benutzer illegaler Download-Börsen helfen. ☐

Weiß nicht ☐

C6. Sind folgende Aussagen wahr oder falsch?

PRA01-05

	wahr	falsch	weiß nicht
Die National Security Agency (NSA) greift nur auf Nutzerdaten zu, die öffentlich und für jedermann zugänglich sind.	☐	☐	☐
Betreiber sozialer Netzwerke (z. B. Facebook) sammeln und verarbeiten auch Informationen von Personen, die dieses Netzwerk gar nicht nutzen.	☐	☐	☐
Daten, die Betreiber sozialer Netzwerke (z. B. Facebook) über die Nutzer sammeln, werden nach 5 Jahren gelöscht.	☐	☐	☐
Unternehmen kombinieren Daten, die auf verschiedenen Websites im Internet hinterlassen werden und stellen daraus Nutzerprofile zusammen.	☐	☐	☐
E-Mails werden häufig über mehrere Rechner weitergeleitet, bevor sie bei ihrem eigentlichen Empfänger ankommen.	☐	☐	☐

C7. Sind folgende Aussagen wahr oder falsch?

GES01,GES03,GES04

	wahr	falsch	weiß nicht
Die Weiterleitung anonymisierter Nutzerdaten zu Marktforschungszwecken ist in der EU gesetzlich erlaubt.	☐	☐	☐
Für alle sozialen Netzwerkseiten gelten in Deutschland die gleichen Standard-AGBs. Abweichungen müssen von den Betreibern kenntlich gemacht werden.	☐	☐	☐
Laut dem deutschen Gesetz haben Nutzer von Online-Anwendungen, die personenbezogene Daten erheben und verarbeiten, einen Anspruch darauf, die über sie gespeicherten Daten einzusehen.	☐	☐	☐

C8. Informationelle Selbstbestimmung ist...

GES05

... ein Grundrecht deutscher Bürger. ☐

... ein philosophischer Begriff. ☐

... die zentrale Forderung datenverarbeitender Stellen. ☐

... die zentrale Aufgabe des Bundesdatenschutzbeauftragten. ☐

C9. Sind die folgenden Aussagen wahr oder falsch?

STR

	wahr	falsch	weiß nicht
Das Nachverfolgen der eigenen Internetnutzung kann durch das regelmäßige Löschen von Browserinformationen (Cookies, Cache, Browserverlauf) erschwert werden.	☐	☐	☐
Durch das Surfen im „Private Browsing"-Modus kann die Rekonstruktion des eigenen Surfverhaltens erschwert werden, da keine Browserinformationen gespeichert werden.	☐	☐	☐
Durch die Nutzung von falschen Namen oder Pseudonymen kann die Identifikation der eigenen Person im Internet zumindest erschwert werden.	☐	☐	☐
Auch wenn selbst schwere Passwörter von IT-Profis geknackt werden können, ist es sinnvoll Passwörter zu verwenden, die aus einer Kombination aus Buchstaben, Zahlen und Sonderzeichen bestehen und keine Wörter, Namen oder einfache Zahlenkombinationen enthalten.	☐	☐	☐
Um den Zugang zu eigenen Daten zu erschweren, sollte man verschiedene Passwörter und Benutzernamen für unterschiedliche Anwendungen nutzen und diese häufig ändern.	☐	☐	☐

C10. Sind folgende Aussagen wahr oder falsch?

ZUS1

	wahr	falsch	weiß nicht
Unternehmen kombinieren Daten, die auf verschiedenen Websites im Internet hinterlassen werden, und stellen daraus Nutzerprofile zusammen.	☐	☐	☐
Um sich vor Hackerangriffen zu schützen, ist es sinnvoll, das eigene WLAN auszuschalten, wenn dieses nicht gebraucht wird.	☐	☐	☐
Die Nutzung von Anonymisierungsprogrammen (z.B. Tor) kann vor der Sammlung und Auswertung der eigenen Daten durch Geheimdienste und andere Institutionen schützen.	☐	☐	☐
Online-Shops (z.B. Amazon) werten das Nutzungsverhalten von Kunden aus und erstellen auf dieser Basis Kaufempfehlungen oder entsprechend zugeschnittene Werbung.	☐	☐	☐
Unternehmen sind in der Lage, Nutzern Online-Werbung anzuzeigen, die auf ihrem Surf-Verhalten basiert.	☐	☐	☐
Alle Browser bieten die Möglichkeit, das Speichern von Drittanbieter-Cookies zu unterbinden.	☐	☐	☐
Alle Browser unterstützen automatisch das aktuelle Transport Layer Security Verfahren (TLS 1.2.), welches vor allem mit HTTPS eingesetzt wird.	☐	☐	☐

C11. Schätze dich selbst bei folgenden Fragen ein:

ZUS2

	stimme gar nicht zu				stimme voll und ganz zu
Ich kann gut einschätzen, was Online-Unternehmen mit meinen Daten und Informationen machen.	☐	☐	☐	☐	☐
Ich kenne Hard- und Softwareanwendungen, mit deren Hilfe man die eigenen Daten schützen kann.	☐	☐	☐	☐	☐
Über meine Rechte als Nutzer von Online-Angeboten weiß ich gut Bescheid.	☐	☐	☐	☐	☐

C12. In letzter Zeit hast du wie häufig ...

	nie				sehr häufig
... dich auf einer Website oder bei einem Online-Dienst nicht angemeldet (registriert), weil man dort seine persönlichen Daten angeben musste?	☐	☐	☐	☐	☐
... bei der Anmeldung nicht Deine offizielle E-Mailadresse angegeben, um Deine Identität zu verschleiern?	☐	☐	☐	☐	☐
... in Deinem Internetbrowser die Cookies oder den Cache gelöscht?	☐	☐	☐	☐	☐
... Online-Dienstanbieter gebeten, Deine persönlichen Daten aus ihrer Datenbank zu löschen?	☐	☐	☐	☐	☐

Teil D: Computersicherheit und Medienkompetenz

In dieser Gruppe werden Fragen zur Studie Medienkompetenz gestellt

D1.

Im Folgenden wird nur noch zwischen Computer und Smartphone unterschieden.
Wenn dein Tablet als Betriebsystem Windows, Linux o. ä. hat, wird es als Computer eingestuft.Wenn dein Tablet als Betriebsystem Android, iOs o. ä. hat, wird es als Smartphone eingestuft.

Als was würdest du dein Tablet einstufen?

CM01

Computer ☐

Smartphone ☐

D2. Im Folgenden sind eine Reihe von Programmen genannt. Bitte gib für jedes Programm an, ob dieses auf dem Computer installiert ist oder nicht.

CM29

	Installiert	Nicht installiert	Weiß nicht
Textverarbeitungsprogramm (z.B. Word, Write)	☐	☐	☐
Anti-Viren-Programm (z.B. Norton, McAfee, AntiVir)	☐	☐	☐
Brennprogramm (z.B. Nero, WinOnCD)	☐	☐	☐

	Installiert	Nicht installiert	Weiß nicht
E-Mail-Programm (z.B. Outlook, Mozilla Thunderbird)	☐	☐	☐
Zusätzliche Firewall (z.B. ZoneAlarm, Sygate)	☐	☐	☐
Instant Messenger (z.B. ICQ, Skype, Yahoo, MSN)	☐	☐	☐
Internet-Tauschbörsen (z.B. eMule, Azureus, Gnutella, KaZaA)	☐	☐	☐
Spam-Filter (z.B. Spamihilator)	☐	☐	☐
Anti-Spyware-Programm (z.B. Ad-Aware, Spybot S&D)	☐	☐	☐
Bildbearbeitungsprogramm (z.B. Gimp, Photoshop)	☐	☐	☐
Cloudspeicher (z.B. Dropbox, OneDrive, Owncloud)	☐	☐	☐

D3. Im Folgenden sind eine Reihe von Programmen genannt. Bitte gibt für jedes Programm an, ob dieses auf dem Smartphone installiert ist oder nicht.

CM29b

	Installiert	Nicht installiert	Weiß nicht
Anti-Viren-Programm (z.B. Bitdefender Mobile Security, Avast, Sophos)	☐	☐	☐
E-Mail-Programm (z.B. TempMail, ProtonMail, Outlook)	☐	☐	☐
Messenger (z.B. WhatsApp, Telegram, Threema)	☐	☐	☐
Spam-Filter (z.B. SpamDrain)	☐	☐	☐
Anti-Spyware-Programm (z.B. Malwarebytes Anti-Malware, Anti Spy Mobile FREE)	☐	☐	☐
Bildbearbeitungsprogramm (z.B. Snapchat, Photodirector)	☐	☐	☐
Cloudspeicher (z.B. Dropbox, OneDrive, Owncloud)	☐	☐	☐

D4. Im Folgenden geht es um Einstellungen am Computer. Bitte gib für jede Einstellung an, ob diese auf deinem Computer aktiviert ist oder nicht.

CM210

	Aktiviert	Nicht aktiviert	Weiß nicht
Im Betriebssystem integrierte Firewall (z.B. Windows Firewall, Apple Firewall)	☐	☐	☐
Aktive Inhalte im Browser (z.B. Javascript, ActiveX)	☐	☐	☐
Add-Ons im Browser (z.B. Browser Helper Objects)	☐	☐	☐

	Aktiviert	Nicht aktiviert	Weiß nicht
automatische Update-Services (z.B. Windows Update, smart)	☐	☐	☐
Benutzerkontensteuerung, wie hier zu sehen: (Das Bild befindet sich am Ende dieses Fragebogens)	☐	☐	☐

D5.

Im Folgenden findest du eine Reihe von Aussagen, die sich auf Deine Person beziehen.
Antworte bitte möglichst spontan, d. h. ohne über Deine Antwort lange nachzudenken, und ehrlich. Zudem gibt es keine richtigen oder falschen Antworten – es zählt das, wovon du überzeugt bist!

Wie sehr treffen die folgenden Aussagen auf dich zu?

CM213

	trifft überhaupt nicht zu				trifft voll und ganz zu
Wenn es um die Benutzung des Computers geht, sind meine Eltern ziemlich streng.	☐	☐	☐	☐	☐
Ich muss meine Eltern um Erlaubnis fragen, wenn ich an den Computer möchte.	☐	☐	☐	☐	☐
Was ich am Computer mache, ist meinen Eltern egal.	☐	☐	☐	☐	☐
Meine Eltern wollen immer genau wissen, was ich am Computer mache.	☐	☐	☐	☐	☐

D6.

Du findest im Folgenden eine Reihe von Aussagen.
Antworte bitte möglichst spontan und ehrlich, d. h. ohne über die Antwort lange nachzudenken. Bei diesen Fragen gibt es keine richtigen oder falschen Antworten – es zählt alleine Deine Meinung und wie du empfindest!

Wie sehr treffen die folgenden Aussagen auf dich zu?

CM46

	trifft überhaupt nicht zu				trifft voll und ganz zu
Ich prüfe sehr genau, wem ich meine Bankverbindung beim Online-Shopping angebe.	☐	☐	☐	☐	☐
Ich suche immer erst nach Möglichkeiten, Musik im Internet kostenlos zu bekommen, bevor ich daran denke, sie zu kaufen.	☐	☐	☐	☐	☐
Ich weiß genau, was ich tun muss, um den Kopierschutz einer Software oder eines Spiels zu umgehen (sogenanntes „cracken“).	☐	☐	☐	☐	☐
Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.	☐	☐	☐	☐	☐
Meine Eltern interessieren sich sehr dafür, welche Seiten ich besuche, wenn ich im Internet surfe.	☐	☐	☐	☐	☐

	trifft überhaupt nicht zu				trifft voll und ganz zu
Ich verwende gerne Freeware- oder Open-Source-Alternativen zu kostspieligen Software-Programmen.	☐	☐	☐	☐	☐
Ich sichere in regelmäßigen Abständen die wichtigsten Daten auf einem CD/DVD-Rohling oder einer externen Festplatte.	☐	☐	☐	☐	☐
Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.	☐	☐	☐	☐	☐
Wenn ich mir die Originalversion einer Software nicht leisten kann, suche ich nach kostenlosen und legalen Freeware-Alternativen.	☐	☐	☐	☐	☐
Ich denke nicht lange darüber nach, einen E-Mail-Anhang zu öffnen – ich tue es einfach.	☐	☐	☐	☐	☐
Wenn ich per E-Mail oder im Chat einen Link zugesendet bekomme, klicke ich ihn meistens an, auch wenn ich mir nicht sicher bin, auf welcher Seite ich lande.	☐	☐	☐	☐	☐
Ich mache selten Updates für meine Software.	☐	☐	☐	☐	☐
Ich habe mich schon einmal dabei erwischt, wie ich im Internet gezielt nach Seiten mit illegalen Inhalten gesucht habe.	☐	☐	☐	☐	☐
Meine Eltern haben mich noch nie danach gefragt, was ich tue, wenn ich im Internet bin.	☐	☐	☐	☐	☐
Ich achte nicht darauf, von welchen Seiten die Dateien stammen, die ich herunterlade.	☐	☐	☐	☐	☐
Ich freue mich, wenn mich fremde Leute im Chat ansprechen und antworte ihnen gerne.	☐	☐	☐	☐	☐
Meine Eltern achten darauf, dass das Computerspielen nicht Überhand nimmt.	☐	☐	☐	☐	☐
Auch wenn ich stundenlang zocke, haben meine Eltern nichts dagegen.	☐	☐	☐	☐	☐
Filme, Musik, Spiele oder andere Software lade ich manchmal auch von etwas zwielichtigen Seiten.	☐	☐	☐	☐	☐
Wenn ich von Fremden E-Mails erhalte, bin ich oft neugierig und öffne sie.	☐	☐	☐	☐	☐
Ich lege Wert darauf, Originalversionen meiner Software zu besitzen.	☐	☐	☐	☐	☐
Was ich wann und wie lange am Computer tue, ist meinen Eltern egal.	☐	☐	☐	☐	☐
E-Mails, bei denen ich die Vermutung habe, dass es sich um unerwünschte Nachrichten (Spam) handelt, lösche ich sofort.	☐	☐	☐	☐	☐
Ich vermeide es, auf Internetseiten zu surfen, die mir verdächtig oder zwielichtig erscheinen.	☐	☐	☐	☐	☐
Dateianhänge bei E-Mails lasse ich immer erst von meinem Virenprogramm prüfen, bevor ich sie öffne.	☐	☐	☐	☐	☐
Ich ändere in regelmäßigen Abständen alle meine Passwörter.	☐	☐	☐	☐	☐
Ich benutze Passwörter, die ich mir möglichst leicht merken kann.	☐	☐	☐	☐	☐

	trifft überhaupt nicht zu				trifft voll und ganz zu
Bestellungen im Internet bezahle ich am liebsten per Bankeinzug.	☐	☐	☐	☐	☐
Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.	☐	☐	☐	☐	☐
Ich weiß genau, wie ich an gefälschte Seriennummern für meine Software gelange.	☐	☐	☐	☐	☐
Für meine Lieblingsmusik bezahle ich gerne – auch im Internet.	☐	☐	☐	☐	☐

D7. Jetzt geht es um deine Einschätzungen zu Risiken im Umgang mit Computern und Internet!

Wie hoch ist deiner Ansicht nach das Risiko, …

CM47

	sehr geringes Risiko				sehr hohes Risiko
… dass beim Onlineshopping (Einkaufen im Internet) die Kontodaten ausgespäht werden?	☐	☐	☐	☐	☐
… dass ausgespähte Kontodaten dazu genutzt werden können, Geld von Deinem Konto abzuheben?	☐	☐	☐	☐	☐
… dass der Computer durch das Öffnen von Mailanhängen mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐	☐
… dass beim Onlinebanking (Bankgeschäften im Internet) die Kontodaten ausgespäht werden?	☐	☐	☐	☐	☐
… dass man es nicht merkt, wenn der Rechner mit einem Computervirus infiziert ist?	☐	☐	☐	☐	☐
… dass ein Computervirus von der Antivirensoftware nicht erkannt wird?	☐	☐	☐	☐	☐
… dass der Computer durch den Download von Dateien über Tauschbörsen (z.B. eMule, BitTorrent) mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐	☐
… dass der Computer beim Surfen im Internet (ohnen Dateien herunterzuladen) mit einem Computervirus infiziert werden kann?	☐	☐	☐	☐	☐

D8. Welche Aufgabe hat eine Firewall?

CM51

Sie schützt den Rechner vor Überhitzung und den daraus entstehenden Schwelbränden, die ohne Firewall auf der Hauptplatine auftreten können.	☐
Sie überwacht den eingehenden und ausgehenden Datenverkehr im Internet und kann so die Verbreitung von Phishing-Mails eindämmen.	☐
Sie überwacht den eingehenden und ausgehenden Datenverkehr im Internet und kann so die Verbreitung von Viren und anderen Schadprogrammen eindämmen.	☐
Sie überwacht den eingehenden Datenverkehr und kann so bei Ermittlungen gegen Benutzer illegaler Download-Börsen helfen.	☐
Weiß nicht	☐

D9. Welche der folgenden Abkürzungen steht für eine Art der Verschlüsselung in drahtlosen Netzwerken (WLANs)?

CM52

- ☐ EWP
- ☐ WEP
- ☐ PWE
- ☐ Weiß nicht

D10. Was ist ein Bot-Netz?

CM53

- ☐ Ein Netzwerk von Computern, die über eine Schadsoftware miteinander verbunden sind und von einem zentralen Computer im Internet (Server) aus ferngesteuert werden können.
- ☐ Ein Netzwerk von Hilfsprogrammen, die standardmäßig in jede Anti-Viren-Software eingebaut sind und sich gegenseitig über Virenfunde benachrichtigen.
- ☐ Ein Bereich im Internet, in dem sich besonders viele Hacker und Kriminelle treffen.
- ☐ Weiß nicht

D11. Ein sicheres Passwort…

CM54

- ☐ Sollte nur aus Zahlen bestehen, wie die Geheimzahl bei der Bank.
- ☐ Besteht aus einer gut durchmischten Kombination aus Buchstaben, Zahlen und Sonderzeichen.
- ☐ Sollte keine Sonderzeichen enthalten, da dies auf einigen Computern zu Problemen führen kann.
- ☐ Weiß nicht

D12. Sortiere die folgenden Dateianhänge je nach der Gefahr, einen Virus damit zu bekommen.Beim ersten Element ist die Gefahr am größten:

Diese Frage erfolgte online durch Drag-and-Drop: CM55

- ☐ .exe / .ini
- ☐ .pdf
- ☐ .docx / .xlsx / .pptx
- ☐ .odt / .ods / .odp
- ☐ .java / .class
- ☐ .vbs

D13. Bei welcher der folgenden E-Mails könnte es sich um einen typischen Betrugsversuch (Phishing) handeln?

(Die beiden Bilder der Sparkassen-E-Mails befinden sich am Ende dieses Fragebogens.)

CM56

Phishing-Versuch	kein Phishing-Versuch
☐	☐

Phishing-Versuch	kein Phishing-Versuch
☐	☐

D14. Welches der folgenden Dinge kann nicht passieren, wenn man einen Virus auf dem Computer hat?

CM57

- ☐ Vom eigenen Computer aus werden unerwünschte E-Mail-Nachrichten (Spam) versandt.
- ☐ Über das Stromnetz können auch andere Haushaltsgeräte angegriffen und mit dem Virus infiziert werden.
- ☐ Die Festplatte kann gelöscht oder gar zerstört werden.
- ☐ Andere Computer im Internet können angegriffen und mit dem Virus infiziert werden.
- ☐ Weiß nicht

D15. Welche der folgenden URLs garantiert einen mit hoher Wahrscheinlichkeit datenabhörsicheren Zugriff?

CM58

- ☐ http://www.postbank.de
- ☐ http://sicher-im-netz.de
- ☐ https://www.gmx.net/
- ☐ Weiß nicht

D16. Welche Arten von Daten können von einem Virus abgegriffen und an Fremde verschickt werden?

CM59

- ☐ Prinzipiell alle Daten, die auf dem Computer gespeichert sind oder eingegeben werden, inklusive Passwörtern und Zugangsdaten (z.B. zum Online-Banking, Kreditkartennummern etc.).
- ☐ Prinzipiell alle Daten, die auf dem Computer gespeichert sind oder eingegeben werden. Passwörter und Zugangsdaten können allerdings nicht gespeichert werden, da diese in Windows besonders gut gesichert sind.
- ☐ Vor allem illegal heruntergeladene MP3- und Videodateien, da bekanntermaßen Viren dafür spezialisiert sind.
- ☐ Weiß nicht

D17. Ist Dir oder jemandem aus Deinem Umfeld schon einmal einer der folgenden Vorfälle passiert?

CM61

	Selber schon passiert	Anderen aus meiner Familie passiert	Freunden oder Bekannten schon passiert	Noch nie bei jemanden aus meinem Umfeld gehört
Der Virenscanner hat einen Virus gemeldet.	☐	☐	☐	☐
Es sind Rechnungen über nicht bestellte Waren oder Dienstleistungen eingegangen.	☐	☐	☐	☐
Auf der Telefonrechnung waren Gebühren für den Anruf einer Telefonnummer verzeichnet, die niemand bewusst angerufen hat.	☐	☐	☐	☐
Von einem Online-Banking verwalteten Konto ist Geld abhanden gekommen.	☐	☐	☐	☐

	Selber schon passiert	Anderen aus meiner Familie passiert	Freunden oder Bekannten schon passiert	Noch nie bei jemanden aus meinem Umfeld gehört
Fremde haben die Zugangsdaten eines Benutzer-Kontos herausbekommen und genutzt, um Geschäfte zu ihrem Nutzen und auf Kosten des eigentlichen Besitzers zu machen.	☐	☐	☐	☐

D18. Jetzt geht es darum, wie Du und Deine Eltern gemeinsam mit Datenschutz umgehen:

*MP25**

	nie				immer
Wenn Du in einem Online-Shop einkaufst, wie häufig machst du dies mit deinem Vater oder deiner Mutter gemeinsam?	☐	☐	☐	☐	☐
Wie häufig reden dein Vater oder deine Mutter mit dir über deine Online-Einkäufe?	☐	☐	☐	☐	☐
Wenn Du in einem Sozialen Netzwerk (z.B. Facebook) unterwegs bist, wie häufig machst du dies mit deinem Vater oder deiner Mutter gemeinsam?	☐	☐	☐	☐	☐
Wie häufig reden dein Vater oder deine Mutter mit dir über dein Verhalten in Sozialen Netzwerken?	☐	☐	☐	☐	☐
Wenn Du Online-Game spielst, wie häufig machst du dies mit deinem Vater oder deiner Mutter gemeinsam?	☐	☐	☐	☐	☐
Wie häufig reden dein Vater oder deine Mutter mit dir über deine Spielerfahrungen?	☐	☐	☐	☐	☐
Wenn Du neue Apps/Software installierst, wie häufig machst du dies mit deinem Vater oder deiner Mutter gemeinsam?	☐	☐	☐	☐	☐
Wie häufig reden dein Vater oder deine Mutter mit dir über deine neuen Apps / neue Software?	☐	☐	☐	☐	☐
Wenn Du Musik oder Filme downloadest, wie häufig machst du dies mit deinem Vater oder deiner Mutter gemeinsam?	☐	☐	☐	☐	☐
Wie häufig reden dein Vater oder deine Mutter mit dir über das Downloaden von Dateien?	☐	☐	☐	☐	☐

D19. Nun geht es um das Thema Vertrauen. Wie sehr stimmst Du den folgenden Aussagen zu?

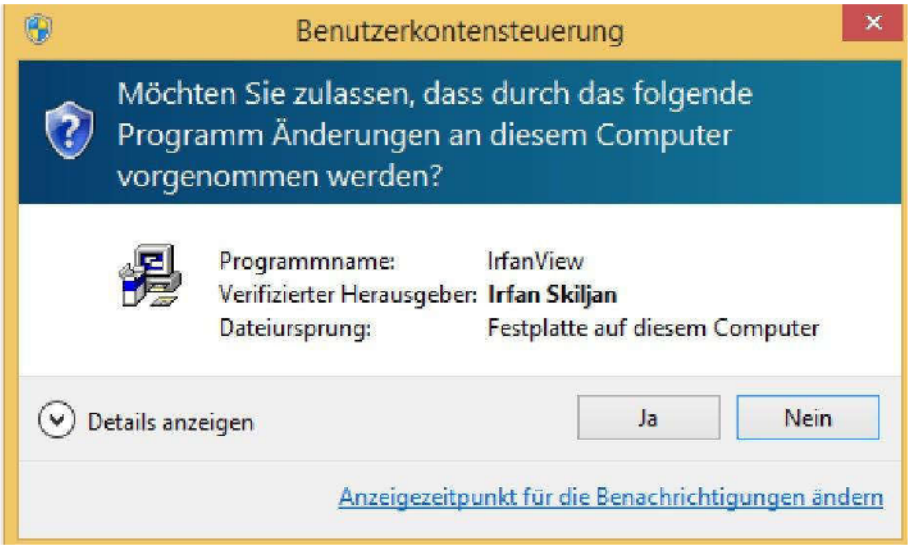
MP35

	stimme überhaupt nicht zu				stimme voll und ganz zu
Die meisten Menschen sind grundsätzlich ehrlich.	☐	☐	☐	☐	☐
Die meisten Menschen sind vertrauenswürdig.	☐	☐	☐	☐	☐
Die meisten Menschen sind grundsätzlich gut und freundlich.	☐	☐	☐	☐	☐
Die meisten Menschen vertrauen anderen.	☐	☐	☐	☐	☐
Ich habe Vertrauen in andere Menschen.	☐	☐	☐	☐	☐
Die meisten Menschen reagieren freundlich, wenn ihnen Vertrauen entgegen gebracht wird.	☐	☐	☐	☐	☐

	stimme überhaupt nicht zu				stimme voll und ganz zu
Ich habe Vertrauen in soziale Netzwerke.	☐	☐	☐	☐	☐
Ich habe Vertrauen in Betriebsysteme.	☐	☐	☐	☐	☐
Ich habe Vertrauen in Anti-Viren-Systeme.	☐	☐	☐	☐	☐
Ich habe Vertrauen in Online-Händler.	☐	☐	☐	☐	☐
Ich habe Vertrauen in Online-Spiele.	☐	☐	☐	☐	☐
Ich habe Vertrauen in App-Stores bzw. die Apps-/Softwareentwickler.	☐	☐	☐	☐	☐
Ich habe Vertrauen in Website-Anbieter, dass sie vertrauensvoll mit meinen persönlichen Daten umgehen.	☐	☐	☐	☐	☐

Vielen Dank für die Teilnahme an der Umfrage. Mit den Ergebnissen können wir ein erstes Bild einholen und mit deiner Rückmeldung den Test verbessern, vereinfachen, kürzen oder auch vertiefen.

Benutzerkontensteuerung:



Sparkasse 1:

Stadtsparkasse München

Sehr geehrter Kunde,

Da gegenwärtig die Betrügereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind wir genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der Stadtsparkasse München durchzuführen.

Der Sicherheitsdienst von der Stadtsparkasse München hat die Entscheidung getroffen, ein neues Datensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die Protokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu erstellt.

Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

FORM AUSFÜLLEN

Diese Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.

Danke für Ihre Zusammenarbeit,
Administration der Stadtsparkasse München

Sparkasse 2:

Stadtsparkasse München

Sehr geehrter Herr Müller,

ich wünsche Ihnen im Namen der Stadtsparkasse München alles Gute zum Geburtstag, Glück, Gesundheit und viel Erfolg im neuen Lebensjahr.

Gerne möchte ich Ihnen bei der Planung Ihres finanziellen Erfolgs hilfreich zur Seite stehen. Zu diesem Zweck habe ich Ihnen einen persönlichen Finanzplan zusammengestellt, mit dem ihre Anlagen ideal an die Herausforderungen des kommenden Jahres angepasst sind.

Sie finden den Finanzplan auf dieser **speziellen Internetseite:**

FINANZPLAN ABRUFEN

Bitte setzen Sie sich möglichst bald mit mir in Verbindung, falls Sie Interesse an einer Finanzberatung haben.

Mit freundlichen Grüßen,

Jürgen W. Hartmann
Ihr Finanzberater

ANHANG 4.16

Rückmeldebogen der Schüler zur Prä-Pilotierung

Die folgenden Seiten umfassen den Rückmeldebogen der Schüler zu dem Fragebogen der Prä-Pilotierung aus dem Sommer 2017.

Rückmeldebogen zur Befragung „Jugendliche und Datenschutz“

Du wirst gebeten, an einer Befragung zu dem o. g. Thema teilzunehmen. Diese erfolgt online über ein Software-Tool im Browser. Die URL bzw. den QR-Code erhältst Du von mir. Bitte achte darauf, die Fragen genau und konzentriert zu lesen. Auch wenn die Daten dieser Befragung nicht für die offizielle Studie, sondern nur zur Pilotierung genutzt werden, bitte ich Dich um wahrheitsgemäße Angaben. Vielen Dank!

Mit diesem Beiblatt bitte ich Dich um eine Rückmeldung zu dieser Befragung. Unter jeder Antwort einer Frage steht ein Code, der auf den einzelnen Seiten nicht einheitlich ist. Ich bitte Dich, diesen bei Bedarf in der ersten Spalte der u. s. Tabelle zu übernehmen, damit ich später eine korrekte Zuordnung zwischen der Frage und Deiner Bemerkung vornehmen kann.

Mit folgendem Gerät habe ich die Befragung durchgeführt am:

☐ PC/Laptop ☐ Smartphone ☐ Sonstiges: _____

Mein Teilnahme-Code lautet: _____

Code	Art des Problems und Verbesserungsmöglichkeit (unverständliche Frage, fehlende oder unzureichende Antwortmöglichkeit, …)

Was Du uns noch sagen möchtest? Welche Vorfälle Du im Zusammenhang mit Datenschutz kennst, die hier nicht behandelt worden sind? ….

ANHANG 4.17

Soziale Netzwerke aus Schülersicht

Die folgenden Seiten erläutern das Verständnis von dem Begriff *Soziales Netzwerk* für die einzelnen Befragungen.

Die Frage nach Sozialen Netzwerken wurde vom Autor erstmals im Rahmen der Schülerbefragung im Sommer 2016 gestellt (vgl. Anhang A4.12, Frage VII) und stammt in dieser Form aus keiner der genutzten Studien. In den fortlaufenden Befragungen wurde immer wieder auf die Frage der genutzten Sozialen Netzwerke zurückgegriffen.

Bei der Frage wurden folgende Internetplattformen[1] letztendlich gelistet:

Name	Definition/Charakterisierung
Facebook	Soziales Netzwerk
Google+[2]	Soziales Netzwerk
Twitter	„digitale Echtzeit-Anwendung zur Verbreitung von telegrammartigen Kurznachrichten; es wird zudem als Kommunikationsplattform, Soziales Netzwerk oder ein meist öffentlich einsehbares Online-Tagebuch beschrieben“ (DIVSI 25, S. 14)
YouTube	Videoportal
Tumblr	Blogging-Plattform
Instagram	Mikroblog und audiovisuelle Plattform
MySpace	Soziales Netzwerk
Snapchat	Instant-Messaging-System
Pinterest	Soziales Netzwerk
Steam	Internet-Vertriebsplattform für Spiele, Software, Filme, Computergeräte, usw.
Twitch	Live-Streaming-Videoportal (vorrangig zur Übertragung von Videospielen)

Tab. A4.17-1: Charakterisierung der in der Frage genutzten Sozialen Netzwerke

Diese Auflistung ist als eine Zusammenfassung folgender Überlegungen zu verstehen, von denen der Autor sich hat leiten lassen:

- Die Autoren der DIVSI-Studie U25 berichten, dass „gerade in den letzten Jahren … die Möglichkeiten der Verbreitung von Texten und Bildern noch einmal stark zugenommen [haben]. Waren die Kommunikationsmöglichkeiten im Internet früher auf das Versenden und Empfangen von E-Mails sowie auf die Teilnahme an Chat-Foren beschränkt, haben sich die Vernetzungsoptionen in den letzten Jahren vervielfältigt. Mit steigender Tendenz nehmen auch viele andere Online-Angebote neben den klassischen Online-Communitys wie z. B. Facebook einen Netzwerk-Charakter an (z. B. YouTube, Twitter)“ (DIVSI 25, S. 13f).
- Die BITKOM-Studie *jung und vernetzt* gibt als *genutzte Soziale Medien* an, dass *WhatsApp* (72 %), *Facebook* (56 %), *Skype* (46 %), *Google+* (19 %), *Instagram* (18 %),

[1] Die Beschreibungen sind, wenn nicht anders angegeben, aus *Wikipedia* entnommen.
[2] Es kann sein, dass die Schüler das „+“-Zeichen leicht übersehen haben und stattdessen die Suchmaschine *Google* meinten.

Twitter (8 %) zu den wichtigsten Medien gehören (BITKOM, S. 28). Ferner schreiben die Autoren: „In der Umfrage zeigte sich, dass auch Kurznachrichten- und Telefondienste wie *WhatsApp* und *Skype* als Soziale Netzwerke genannt werden. Die Frage ist, ob Messenger- oder Telefondienste wie *WhatsApp* oder *Skype* im engeren Sinne Soziale Netzwerke sind. Aus Sicht des BITKOM trifft das im Wesentlichen zu. Wichtigstes Merkmal eines Sozialen Netzwerks sind die persönlichen Profile, die von den Nutzern bei allen genannten Anwendungen angelegt werden können. Die Funktionen der Kurznachrichtendienste sind aber auf das Wesentliche reduziert – die Kommunikation per Text, Sprache oder Bild. Viele Jugendliche bevorzugen für den schnellen Austausch mit ihren Freunden offenbar schlanke Anwendungen gegenüber aufwändigen, multifunktionalen Netzwerken“ (BITKOM, S. 28).

- In der JIM-Studie 2017 wird nicht konkret nach Sozialen Netzwerken gefragt, jedoch nach den beliebtesten Internetangeboten (*YouTube* (62 %), *WhatsApp* (40 %), *Instagram* (27 %), *Snapchat* (16 %), *Facebook* (15,5 %), *Google* (10 %), *Netflix* (8 %), *Amazon* (4,5 %), *Twitter* (3,5 %), *Wikipedia* (2,5 %), *Spotify* (2,5 %), *Ebay* (1 %), *Tumblr* (1 %), *Minecraft* (0,5 %), *Skype* (0,5 %)) (JIM 2017, S. 33), nach den wichtigsten Apps (*WhatsApp* (87,8 %), *Instagram* (39 %), *Snapchat* (33 %), *YouTube* (32,8 %), *Facebook* (12 %)) (JIM 2017, S. 34) und den Aktivitäten im Internet mit Schwerpunkt Kommunikation (*WhatsApp* (93,5 %), *Instagram* (56,8 %), *Snapchat* (48,5 %), *Facebook* (23,3 %), *Twitter* (8,3 %), *Skype* (8,3 %), *Pinterest* (6,3 %), *Tumblr* (4 %), *Google+* (3,3 %)) (JIM 2017, S. 36).

Der Autor ist sich bewusst, dass in der tabellarischen Auflistung nur *Facebook*, *Google+*, *MySpace* und *Pinterest* streng genommen Soziale Netzwerke sind. Jedoch bestärkt durch die Aussagen der BITKOM-Studie und der DIVSI-Studie ist es legitim, die diversen Internetplattformen bei der Befragung unter Soziale Netzwerke zu subsummieren, denn eine ausgeprägte Profilgestaltung u. ä. Dinge, die ein Soziales Netzwerk charakterisieren, sind hierbei irrelevant.

Abschließend sei auch noch folgende Anmerkung aus der BITKOM-Studie *jung und vernetzt* gemacht. Als Kommunikationsformen nutzen die Befragten Kurznachrichten (70 %), persönliche Gespräche (66 %), Festnetztelefonate (36 %), Soziale Netzwerke wie *Facebook* oder *Twitter* (32%), Handytelefonate (28 %), Videotelefonate wie *Skype* (15 %), Internetchat wie Chatrooms und Messenger (13 %), E-Mail (7 %), Briefe schreiben (3 %) (BITKOM, S. 27). Auch hier wird *Twitter* zu den Sozialen Netzwerken gezählt.

Literaturverzeichnis

[BITKOM] BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Hg.) (2014): Jung und vernetzt. Kinder und Jugendliche in der digitalen Welt. Berlin. Online verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Jung-und-vernetzt-Kinder-und-Jugendliche-in-der-digitalen-Gesellschaft.html, zuletzt geprüft am 01.07.2018.

[DIVSI 25] Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (Hg.) (2014): DIVSI U25-Studie. Kinder, Jugendliche und junge Erwachsene in der digitalen Welt. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Hamburg. Online verfügbar unter www.divsi.de/wp-content/uploads/2014/02/DIVSI-U25-Studie.pdf, zuletzt geprüft am 01.07.2018.

[JIM 2017] Feierabend, Sabine; Plankenhorn, Theresa; Rathgeb, Thomas (2017): JIM-Studie 2017. Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Hg. v. Medienpädagogischer Forschungsverbund Südwest. Stuttgart, zuletzt geprüft am 05.01.2018.

Lebenslauf