Kommunikations- und Medienethik | 14

Stapf | Ammicht Quinn | Friedewald | Heesen | Krämer [Hrsg.]

Aufwachsen in überwachten Umgebungen

Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend

Nomos

Kommunikations- und Medienethik

herausgegeben von

Alexander Filipović
Christian Schicha
Ingrid Stapf

Band 14

Ingrid Stapf | Regina Ammicht Quinn
Michael Friedewald | Jessica Heesen
Nicole Krämer [Hrsg.]

Aufwachsen in überwachten Umgebungen

Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2021

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-8487-6916-2
ISBN (ePDF): 978-3-7489-2163-9

DOI: https://doi.org/10.5771/9783748921639

Onlineversion
Nomos eLibrary

Bis Band 4 erschienen bei Beltz Juventa, Weinheim.

Vorwort

Um im interdisziplinären Dialog die Auswirkungen der zunehmenden Digitalisierung, Datafizierung und Überwachung von Kindern und Jugendlichen in privaten wie institutionellen Kontexten auszuloten und zu diskutieren, veranstaltete das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte „Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt“ (http://www.forum-privatheit.de/) am 21. und 22. November 2019 in Berlin die Konferenz „Aufwachsen in überwachten Umgebungen – Wie lässt sich Datenschutz in Schule und Kinderzimmer umsetzen?“. Der vorliegende Band präsentiert die wichtigsten Vorträge und reflektiert die dort angestoßenen Diskussionen.

Das „Forum Privatheit“ arbeitet seit nunmehr sieben Jahren – ausgehend von technischen, juristischen, ökonomischen sowie geistes- und gesellschaftswissenschaftlichen Ansätzen – an einem interdisziplinär fundierten, zeitgemäßen Verständnis von Privatheit und Selbstbestimmung. Hieran anknüpfend werden Konzepte zur (Neu-)Bestimmung und Gewährleistung informationeller Selbstbestimmung und des Privaten in der digitalen Welt erstellt. Es versteht sich über seine Kerndisziplinen hinaus als eine Plattform für den fachlichen Austausch und erarbeitet Orientierungswissen für den öffentlichen Diskurs in Form wissenschaftlicher Publikationen, Tagungen, White-Papers und Policy-Papers. Mitglieder des „Forum Privatheit“ sind das Fraunhofer-Institut für System- und Innovationsforschung (ISI), Karlsruhe, das Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt, das Fachgebiet Soziologische Theorie und die Projektgruppe verfassungsverträgliche Technikgestaltung (provet), beide Universität Kassel, das Fachgebiet Sozialpsychologie der Universität Duisburg-Essen, das Internationale Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen, das Institut für Wirtschaftsinformatik und neue Medien der Ludwig-Maximilians-Universität München und das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein, Kiel.

Die inhaltliche Ausrichtung und Organisation der Konferenz stand in der Verantwortung des Internationalen Zentrums für Ethik in den Wissenschaften der Universität Tübingen und des Fachgebiets Sozialpsychologie der Universität Duisburg-Essen. Als Herausgeber*innen freuen wir uns, stellvertretend für das „Forum Privatheit“ insgesamt, nun diesen Konferenzband präsentieren zu können. Wir danken insbesondere den Autor*in-

nen für die Überarbeitung ihrer Vorträge und die Beisteuerung der jeweiligen Fachartikel. Ebenso zum Dank verpflichtet sind wir allen Beteiligten am „Forum Privatheit“. Die Konferenz „Aufwachsen in überwachten Umgebungen“ wäre ohne die vielfältige Unterstützung durch das interdisziplinäre Kollegium nicht möglich gewesen. Wir danken insbesondere all jenen, die organisatorisch oder inhaltlich an der Durchführung der Konferenz und ihrer verschiedenen Sektionen mitgewirkt haben, darunter vor allem Susanne Ruhm (Fraunhofer ISI). Bei Barbara Ferrarese bedanken wir uns für ihre hervorragende Öffentlichkeitsarbeit, bei Marit Hansen (ULD) für ihre Teilnahme an der Podiumsdiskussion. Dank für letztere schulden wir außerdem Emily Lardon und Mia Pagenkemper (Schülerinnen des Berliner Schiller-Gymnasiums) und Daniela Tews (Deutsches Kinderhilfswerk). Herrn Dr. Herbert Zeisel (BMBF) danken wir für die gelungene Eröffnung, dem Improvisationstheater Die Gorillas für ein sehr unterhaltsames Abendprogramm.

Dieser aus der Konferenz hervorgegangene Band wäre nicht ohne tatkräftige Unterstützung bei der Manuskriptbearbeitung und -korrektur zustande gekommen. Wir möchten uns sehr herzlich bedanken bei Dr. des. Yannic Meier von der Uni Duisburg-Essen für die Koordination und Unterstützung der Organisation des Bandes und der Manuskripterstellung sowie den wissenschaftlichen Hilfskräften Sandra Dürr, Teresa Maria Hummler, Alieren Renklıöz, Anna-Lisa Sander vom IZEW Tübingen und Catharina Velten von der Universität Duisburg-Essen. Für die angenehme und zielführende Zusammenarbeit mit dem Nomos-Verlag danken wir Frau Dr. Sandra Frey für die Koordination sowie Frau Eva Lang für die Druckerstellung.

Schließlich möchten wir uns auch bei Dr. Heike Prasse und Ingo Höllein vom Bundesministerium für Bildung und Forschung (BMBF) bedanken, das den Projektverbund unterstützt, sowie bei Dr. Jan-Ole Malchow, der für den Projektträger VDI-VDE die Forschungsarbeiten des „Forum Privatheit“, die Durchführung der Konferenz und das Erscheinen des Bandes begleitet hat. Wir möchten mit dem Band zu weiterführenden Diskussionen und Debatten um die immer wichtiger werdenden Fragen von Privatheit und Selbstbestimmung bei Kindern und Jugendlichen beitragen und zur weiteren Vertiefung des Themas in Theorie wie in Praxis anregen.

Tübingen, Duisburg und Karlsruhe, im Oktober 2020

Inhalt

Einleitung
Aufwachsen in überwachten Umgebungen: Privatheit von Heranwachsenden als ein neues interdisziplinäres Forschungsgebiet

Ingrid Stapf, Regina Ammicht Quinn, Michael Friedewald, Jessica Heesen und Nicole Krämer

Zwischen Überwachung und Fürsorge: Warum schon Kinder Privatheitskompetenz brauchen

Digitale Technologien prägen zunehmend Kindheit und Jugend: von der Videoüberwachung im Säuglingsalter über den Lernroboter im Kindergarten bis hin zu den durch Künstliche Intelligenz gesteuerten Lernassistenten für den individuellen Bildungserfolg. Digitale Medien werden für Lernprozesse, die Wissensvermittlung und die Informationsbeschaffung genutzt und unter dem Schlagwort der Computer Literacy diskutiert. Sie sind Teil des (Schul-)Alltags von Heranwachsenden und bieten einerseits neue Formen der Teilhabe, aber andererseits auch neue Formen der Überwachung von Schüler*innen durch kommerzielle Dienstleister sowie durch Lehrkräfte und Eltern. Die Anwendungen, die insbesondere von Kindern und Jugendlichen genutzt werden, beschränken sich nicht nur auf den formalen Bildungskontext, sondern halten – auch gerade im Zuge des Digitalisierungsschub durch die Corona-Pandemie – Einzug in die Kinderzimmer, einstmals als geschützt wahrgenommene Räume der Privat- und Intimsphäre.

„Ein Geheimnis würde ich eher meinen Eltern oder meinen Freunden anvertrauen als Siri. Auf die Freunde kann man sich verlassen, auf Siri nicht." Mit diesem Zitat eines Kindes begann die Jahreskonferenz des Forum Privatheit zum Thema „Aufwachsen in überwachten Umgebungen – Wie lässt sich Datenschutz in Schule und Kinderzimmer umsetzen?" Obwohl einzelne Kinder somit eine recht hohe Privatheitskompetenz im Umgang mit neuen Technologien aufweisen, kann keinesfalls davon ausgegangen werden, dass von neuen Technologien keine Risiken ausgehen. 30 Jahre nach Einführung der UN-Kinderrechtskonvention ist es wichtig, kritisch zu prüfen, in welchem Maße die Kinderrechte beim Umgang mit neuen Technologien gewährleistet werden. Dabei sind sowohl neue tech-

nologische Entwicklungen im formalen schulischen Kontext (im Sinne von Lernprogrammen und videobasiertem Unterricht) relevant, vermehrt aber auch die Tatsache, dass Technologien Einzug in die Kinderzimmer und Familien halten.

Dies zeigen Phänomene des Sharenting als „habitual use of social media to share news, images, etc. of one's children"[1] und *Oversharenting,* wenn dies exzessiv geschieht (vgl. Stapf 2019, Stapf in diesem Band). So wird die Social-Media-Nutzung von *WhatsApp* von Kindern durch Eltern begrenzt und ist mit der Datenschutz-Grundverordnung (DSGVO) zum Schutz der Kinder gar auf das Alter von 16 Jahren angehoben worden, während

> „parents share information about their children online, they do so without their children's consent. These parents act as both gatekeepers of their children's personal information and as narrators of their children's personal stories [...]. A conflict of interests exists as children might one day resent the disclosures made years earlier by their parents. (Steinberg 2017: 839)

Wenn Kinder ihre Eltern rückwirkend verklagen wegen intimer oder ihre Privatsphäre überschreitende Inhalte, die ohne ihre Einwilligung gepostet wurden[2] oder Fürsorgetragende ihre Kinder mit SpyApps überwachen oder die Social Media Nutzung heimlich über Software auswerten, dann zeigt sich ein Spannungsfeld. Es liegt zwischen den gesetzlich verbrieften Fürsorgeansprüchen von Heranwachsenden durch ihre Eltern (z.B. in Art. 6 GG oder Art. 5 UN-KRK) und der Sichtweise auf Kinder als eigenständige Rechtsträger*innen, die zwar noch in Entwicklungsprozessen stecken, dabei aber bezogen auf ihre sich entwickelnden Fähigkeiten verbriefte Rechte auf Mitbestimmung und Selbstbestimmung haben (u.a. Art. 12 UN-KRK). Beispiele des Sharenting deuten darauf hin, dass Kinder in der Praxis oft eher nicht als selbstständige Rechtssubjekte betrachtet werden, sondern vielmehr als Objekte elterlichen, kommerziellen oder schulischen Handelns allgemein und im Zusammenhang mit digitalen Medien. Dabei stellt sich die Frage, wieviel Überwachung oder auch Fürsorge langfristig dem Schutz des Kindes und seinen Fähigkeiten, selbstbestimmt über Pri-

1 vgl. Collins Dictionary „Sharenting"; online abrufbar unter: https://www.collinsdictionary.com/dictionary/english/sharenting [Abfrage am: 10.10.2020].

2 vgl. den Fall einer damals 18-jährigen österreichischen Schülerin, die ihre Eltern wegen Sharenting verklagte (online abrufbar unter: https://www.welt.de/vermischtes/article158099198/Sie-kannten-keine-Scham-und-keine- Grenze.html [Abfrage am: 10.10.2020]).

vatheit entscheiden zu können, dient (vgl. Stapf in diesem Band, Stapf 2020).

Mit Blick auf Bildungskontexte kann weiterhin die Analyse von Lernverhalten sehr persönliche Informationen über Fähigkeiten, Intelligenz oder gar inhaltliche Interessen offenlegen. Die technischen Schlüssel für diesen Zugang sind „Interaktivität" und „Personalisierung" von Lernen und Bildung, beispielsweise durch gamifizierte e-Learning Smartphone Apps. Der Vorteil von interaktiven und sich anpassenden Systemen liegt darin, dass sie sich sehr genau auf die lernende Person, d.h. das Kind, ausrichten und dabei individuelle Präferenzen und Kompetenzen berücksichtigen können. Besonders IT-basierte Systeme können zur Verfeinerung der Individualisierung beitragen, Lernprozesse dokumentieren und helfen, die lernende Person „optimal" zu fördern. Dabei bestehen Risiken, etwa wenn auf Grundlage von Profiling durch (teil-)automatisierte Entscheidungssysteme Bewertungen über die Persönlichkeit getroffen, Ressourcen verteilt oder Karrierewege ausgeschlossen werden. Eine wichtige Rolle spielen außerdem die technischen Infrastrukturen und Software-Lösungen und ihre Ausgestaltung.

Selbstbestimmung lernen in einer datafizierten Gesellschaft

Aufgrund der besonderen (verletzlichen) Situation lernender Person und den oft asymmetrischen Machtstrukturen in (schulischen) Lernzusammenhängen stellen sich hier viele ethische Fragen. Es zeigt sich eine deutliche Spannung zwischen der besonderen Schutzwürdigkeit personenbezogener Daten von Kindern und Jugendlichen und der Nützlichkeit des daraus generierten Wissens für ihre gute Förderung und Begleitung. Des Weiteren sind Stigmatisierungsvorgänge möglich, etwa dadurch, dass Informationen über Kinder auch bereits im Umfeld eines erweiterten Begriffs von Kriminalprävention genutzt werden können. Aber auch im Bereich der universitären und beruflichen Bildung sowie der Erwachsenenbildung ergeben sich Fragestellungen aus dem Spannungsfeld zwischen Berücksichtigung und Förderung der Individualität von Lernprozessen einerseits und der repressiven Wirkung von Beobachtung und Datenerfassung andererseits. Besonders relevant sind darüber hinaus die Folgen der Überwachung für die Schule als Lebens- und Erfahrungsraum, für die Vertrauen zwischen Lernenden und Lehrenden zentral ist, sowie insbesondere für Schule als demokratischen Lernort, in dem ein erzieherisches Ideal zur Hinführung zu Mündigkeit, gesellschaftlicher Verantwortung und Freiheit im Vordergrund steht.

Dass bei den meisten der genannten Anwendungen Daten anfallen, die viel über die Heranwachsenden aussagen, erscheint in freiheitlichen Demokratien daher besonders problembehaftet. Bildung und Erziehung sind eine Kernaufgabe einer modernen Gesellschaft. Vor allem heranwachsende Menschen sollen nicht nur ausgebildet, sondern als (zukünftige) mündige Bürger*innen zur Teilhabe und gesellschaftlich verantwortlichen Selbstbestimmung in einer freien und demokratischen Gesellschaft befähigt werden.

Die Nutzung von Online-Diensten, die Beteiligung an sozialen Medien und das Leben in intelligenten Umgebungen ist also auch schon für Kinder damit verbunden, dass sie im Alltag einer zumindest potenziell permanenten Überwachungssituation ausgesetzt sind (vgl. hierzu Heesen/Stapf 2021 i.E.). Durch die Auswertung z. B. von digitalen Plattformen (Clickstream, Metadaten, Social Graphs usw.) und komplexen Big Data-Analysen können mehr und mehr Informationen über das Verhalten und die Kommunikation der Nutzer*innen gewonnen werden. Digitale Medientechniken ermöglichen insofern Informationsverbreitung in zwei Richtungen: *durch* ihre Nutzer*innen und *über* ihre Nutzer*innen (Heesen 2016: 56f.). Die Unsicherheit über die mögliche Erfassung personenbezogener Daten kann damit auch ein (individuelles und kollektives) Gefühl der Überwachung erzeugen. Aus der Überwachung bzw. dem bloßen Gefühl der Überwachung können eine Veränderung des Verhaltens und gegebenenfalls eine Selbstdisziplinierung resultieren (Turow/Hennessy/Draper 2015), die in sublimierter Weise Eingang in System und Bewusstsein einer ganzen Gesellschaft finden kann (Foucault 1977: 258). Auswirkungen einer angenommenen oder realen Überwachung auf politische Aktivitäten oder den Prozess der Meinungsbildung werden in der Literatur auch als „Chilling-Effekte“ oder als Prozesse der Selbstzensur beschrieben (Staben 2016).

Das Recht auf eine offene Zukunft und demokratische Teilhabe

Im Kern sollen demokratische Freiheits- und Gleichheitsrechte aber auch und gerade Kindern das Recht auf eine offene Zukunft und demokratische Teilhabe ermöglichen (vgl. White Paper des Forum Privatheit, i.e. Stapf et al. sowie Stapf in diesem Band). So ist auch in Artikel 16 der Kinderrechtskonvention der Vereinten Nationen verbrieft, dass „kein Kind (…) willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden“ darf. Den durch das Grundgesetz, die EU-Grundrechtecharta und die Europäische

Menschenrechtskonvention verbrieften Rechten von Kindern sollte aber zu stärkerer Durchsetzung und praktischer Relevanz im Bereich der Nutzung digitaler Technik verholfen werden (vgl. Stapf et al. in diesem Band). Damit verknüpfte Forderungen sind beispielsweise, dass Kinder grundsätzlich von personalisierter Werbung und Tracking ausgenommen werden sollten, dass die Profilbildung bei Kindern auszuschließen ist und dass stärkere Forderungen an die Datenminimierung (z.B. auch im Rahmen einer Bildungs-App) gestellt werden. Ein systematischer Datenschutz für Kinder fehlt bisher in der Datenschutz-Grundverordnung (vgl. Roßnagel in diesem Band).

Da Kindheit eine besonders verletzliche Entwicklungsphase ist und sich wichtige Fähigkeiten erst noch ausbilden, bedürfen Kinder eines umfassenden Schutzes durch Fürsorgetragende und den Staat. Sie sollen gleichzeitig aber auch als handelnde Subjekte ihre Selbstbestimmung erproben können. Hierzu werden Befähigungsmaßnahmen wesentlich, welche die Mündigkeit von Kindern in der Demokratie (und im „digitalen Gemeinwesen“) zum Ziel haben. Medienmündigkeit ist somit eine zentrale gesellschaftliche Aufgabe, die jedoch nicht singulär den Individuen aufgegeben ist, sondern deren Ermöglichung durch Design- und Infrastrukturvorgaben, interdisziplinäre Problemlösungen und politische, gemeinwohlorientiere Entscheidungen auf den Weg gebracht werden sollte (Heesen/Stapf 2021 i.E.).

Das Thema Privatheit von Kindern in digitalen Umwelten weist dabei ein ethisch relevantes Spannungsfeld auf: einerseits als fürsorglicher Schutz im Interesse des Kindes, andererseits aber auch als paternalistische Überwachungspraktiken, die kindliche Selbstbestimmungsansprüche in Frage stellen. Aus der fortschreitenden Mediatisierung von Kindheit resultiert Handlungsbedarf mit Blick auf damit verbundene Risiken und Gefahren sowie eine grundsätzliche Erörterung möglicher Potenziale und Chancen. Diese Auseinandersetzung erscheint besonders gesellschaftlich relevant, da Kinder und Jugendliche bis 18 Jahren rund ein Drittel der weltweiten Internetnutzer*innen ausmachen (Livingstone et al. 2016).

Dieser Band füllt eine bestehende Forschungslücke im deutschsprachigen Raum, da die Privatheit von Kindern in digitalen Kontexten bislang kaum wissenschaftlich differenziert untersucht wurde. Dies kann aufgrund der Komplexität des Themenfeldes nur interdisziplinär erfolgen. Eine hierzu weiterführende und dies bündelnde Perspektive ist der kinderrechtliche Ansatz. Kinderrechte wurden – ergänzend zu den allgemeinen Menschenrechten – 1989 völkerrechtlich in der UN-Kinderrechtskonvention (UN-KRK) verankert und gelten seit 1992 als einfaches Recht in Deutschland. Die Rechte von Kindern werden zudem in Artikel 24 der EU-Grundrechte-

charta verbrieft. Die UN-KRK betont die Rolle von Kindern als subjektive Handlungsträger mit eigenen Rechten und etabliert in 54 Artikeln das beste Interesse von Kindern als leitendes Prinzip im Zusammenspiel von Schutz-, Förderungs- und Beteiligungsrechten. Gerade mit Blick auf das in Artikel 16 UN-KRK verbriefte Recht auf „Schutz der Privatsphäre und Ehre" ergeben sich im digitalen Umfeld von Kindern und Jugendlichen in Familie, Bildungseinrichtungen, aber auch in den medialen Angeboten selbst dringend zu adressierende Fragen (vgl. Roßnagel in diesem Band).

Mit dem Aufkommen überwachungsbasierter Medientechnologien von Smart Toys, Babysitter-Kameras im Teddybär bis hin zu Home-Robotern wie Alexa, individualisierter Lernsoftware, Tracking-Apps oder Videoüberwachung in der Kita sind dies Fragen danach, was die Privatheit von Kindern heute (neuartig) bedroht, aber auch was sie, im Vergleich zu Erwachsenen eigentlich ausmacht: Bedarf es bei Kindern anderer Konzepte als bei Erwachsenen? Wie können sie den Schutz ihrer Daten im Altersverlauf steuern lernen? Was müssen Eltern, Erzieher*innen, Bildungseinrichtungen oder mediale Anbieter dabei beachten? Wer trägt hierbei wofür die Verantwortung? Und welche Kompetenzen sind für digitale Mündigkeit wesentlich?

Zentrale Kernthesen und aktuelle Forschungsaufgaben

Die Jahrestagung des Forum Privatheit im November 2019 hat das Thema „Aufwachsen in überwachten Umgebungen" in Deutschland erstmals interdisziplinär aufgegriffen. Dabei zeigte sich eine Diskrepanz zwischen dem bestehenden gesellschaftlichen und politischen Orientierungs- und Steuerungsbedarf einerseits und der noch ausstehenden wissenschaftlichen Forschung an der Schnittstelle von Theorie und Praxis andererseits. Auch wurde deutlich, dass es einen Bedarf an interdisziplinär ausgerichteten Zugängen zu diesem komplexen Forschungsgebiet gibt, das derzeit erst noch am Anfang steht und sich mit der Evolution neuer Techniken zunehmend weiter wandeln wird. Dies möchte der vorliegende Tagungsband im deutschsprachigen Raum anregen und erste Grundlagen in der Theorie und mit Blick auf die Praxis der Regulierung, Bildung, Erziehung und technische Gestaltung schaffen.

Die Kernthese des in der Folge der Jahrestagung 2019 entstandenen White Papers „Kinderrechte und Privatheit" ist, dass die Rechte von Kindern im Digitalen stärker durchgesetzt und berücksichtigt werden sollten. Dazu gehören explizit das Recht auf informationelle Selbstbestimmung und Privatheit und die freie Entfaltung der Persönlichkeit

(vgl. Stapf et al. in diesem Band). Das White Paper verfolgt das Ziel, einen gesellschaftlich-politischen Diskurs anzustoßen, erste Anforderungen für die Praxis zu formulieren sowie den Forschungsbedarf bezogen auf das Thema aufzuzeigen. Die Forderungen und Thesen darin dürfen auch als ein Fazit des Tagungsbandes verstanden werden. Aus der Kernthese folgt aber auch ein neuartiger Forschungsbedarf: So empfiehlt das Forum Privatheit einen ganzheitlichen Ansatz zur Integration von Kinderrechten, z.B. durch mehr interdisziplinäre empirische Forschung, da momentan die besondere Perspektive der Kinder selbst noch zu wenig untersucht und auch verstanden wird. Es fehlen vor allem Langzeitstudien und partizipative Formate, in denen die Anregungen von Kindern und Jugendlichen direkt in die technische Entwicklung aufgenommen werden können (vgl. Stapf et al. sowie Meiner/Yannic/Krämer in diesem Band).

Aus dem genannten Themenspektrum ergibt sich eine Vielzahl von Fragestellungen und Forschungszielen, die dem Band zugrunde liegen:

- **Probleme, Risiken und Nutzen** – Welche Probleme ergeben sich für die Lernsituation (in einer überwachten Umgebung)? Wie sind Programme zur Digitalisierung des Klassenzimmers unter diesen Aspekten zu bewerten? In welchem Umfang nutzen und schützen interaktive Lernprogramme *personenbezogene Daten*? Wie stark nehmen Nutzer*innen in diesem Umfeld eine Gefährdung von Privatheit überhaupt wahr und inwieweit ist eine *Abwägung von Nutzen und Risiken* zu beobachten?
- **Juristische Herausforderungen** – Welche juristischen Herausforderungen stellen sich in diesem speziellen Umfeld? Welche Rolle spielt hier die UN-Kinderrechtskonvention? Wie können individualisierte Lernprogramme auf detaillierten Lernprofilen einzelner Nutzer*innen aufbauen und dabei die *Missbrauchsrisiken solcher Lernprofile* vermeiden? Wie sind die Lernprozesse der Lernprogramme zu gestalten, um *Diskriminierung zu vermeiden*? Welche Anwendungsszenarien fördern oder gefährden die freie Entfaltung der Persönlichkeit? Welche technischen und organisatorischen Maßnahmen sind notwendig, um die Rechte der betroffenen Personen zu schützen und die Prinzipien des Datenschutzrechts wie etwa Datensparsamkeit umzusetzen?
- **Ökonomische Aspekte und technische Infrastruktur** – Welche Rolle spielen ökonomische Aspekte hierbei, was passiert z. B. unter dem Aspekt der *Private-Public-Partnerships* zur Ausstattung mit Hard- und Software im Bildungsbereich oder wie können *digitale Geschäftsmodelle* privatheitswahrend gestaltet werden? Welche Rolle und Bedeutung haben

die *technischen Infrastrukturen* und schnellen Innovationszyklen in diesem Bereich?

- **Privatheit aus der Sicht von Heranwachsenden** – Inwiefern verändern sich *Konzepte von Kindheit* durch Überwachung? Welche Arten von Privatheit können und wollen Kinder für sich in Anspruch nehmen? Was ist *Privatsphäre aus Kindersicht*? Wie unterscheiden sich möglicherweise Vorstellungen und Bedürfnisse von Kindern und Erwachsenen und wie werden Privatheitsinteressen intergenerationell verhandelt? Welche *Normen* bilden sich unter Heranwachsenden heraus in Bezug auf Privatheit, Medienkonsum, Selbstdarstellung und digitales Self-Fashioning? *Welche neuen Spaltungen* entstehen zwischen Kindern unterschiedlicher Herkunft und Bildungskarriere in Fragen der Privatheit und des (mündigen) Umgangs mit digitalen Technologien?
- **Privatheit und Medienkompetenz** – Darüber hinaus stellen sich nicht nur Fragen zur Bedeutung von Privatheit und Datenschutz im Bildungsbereich, auch die *Bedeutung von Bildung und Medienkompetenz für Datenschutz, Privatheit* und einen mündigen Umgang mit digitalen Technologien und Lebenswelten ist wichtig. Von vielen Seiten werden Bildung/Medienkompetenz als vielversprechendste Mittel zu verbessertem Datenschutz und Privatheit angesehen. Von anderer Seite werden derartige Konzepte wiederum im Hinblick auf eine *Individualisierung gesellschaftlicher Schutzverantwortung* kritisiert. Wie kann dieses Spannungsfeld angemessen adressiert werden? Wie können mögliche Konflikte zwischen Kalkülen der *Datenökonomie* und dem umfassenden *gesellschaftlichen Bildungsauftrag* von Schulen und anderen Bildungseinrichtungen vermieden oder gelöst werden? Wie können Bildungsangebote praktisch gestaltet werden, um nötige Medienkompetenzen effektiv zu vermitteln?
- **Praktische Erfahrungen** – Welche Erfahrungen haben Praktiker*innen in der Bildungsarbeit in Schule, Hochschulen und anderen Umgebungen mit datenbasierten Lernanwendungen gemacht? Welche Probleme und Herausforderungen treten dabei auf?

Der Band gliedert sich in sechs Teile, die unterschiedliche Aspekte aus dem Themenspektrum aufgreifen, so theoretische Grundlagen aus kulturgeschichtlicher, medienpsychologischer und medienethischer Perspektive (vgl. die Beiträge von Ammicht Quinn, Meinert/Meier/Krämer, Stapf), das Aufwachsen in überwachten Umgebungen und sich daraus ergebende Fragen von Privatheit in Kita, Schule und Familie (vgl. die Beiträge von Croll/Frense, Pfaff-Rüdiger/Oberlinner/Eggert/Drexl, Reimer/Flückinger), Datenschutz und Privatheit als Thema der Gesetzgebung und Medienregulie-

rung (vgl. die Beiträge von Dreyer, Roßnagel, Nebel), Medienbildung, Kompetenzen sowie die Frage nach digitaler Mündigkeit (vgl. die Beiträge von Livingstone/Stoilova/Nandagiri, Schulze-Tammena, Janson/Kreidel/Schöbel/Hornung/Söllner/Leihmeister) und schließlich auch Erfahrungsberichte und Hinweise zur praktischen Umsetzung in unterschiedlichen Kontexten (vgl. Beiträge von Persson, Hansen, Zorn/Murmann/Harrach-Lasfaghi sowie Stapf et al.).

Der Band strebt es an, erste interdisziplinäre Ansätze vorzulegen und aufeinander zu beziehen und damit hoffentlich Impulse für die weitere Forschungsarbeit und Gestaltung und Regulierung der Praxis geben zu können.

Literatur

Foucault, Michel (1977): *Überwachen und Strafen. Die Geburt des Gefängnisses*. Suhrkamp: Frankfurt a. M.

Heesen, Jessica (2016): *Einleitung*. In: Jessica Heesen (Hg.): Handbuch Medien- und Informationsethik. Metzler: Stuttgart, S. 1-8.

Heesen, Jessica / Stapf, Ingrid (2021): *Digitale Kommunikation: Medienethik, Medienkompetenz.* In: Monika Bobbert / Jochen Sautermeister (Hg.): Handbuch Psychologie und Ethik. New York/Heidelberg: Springer (im Erscheinen).

Livingstone, Sonia / Carr, John / Byrne, Jasmina (2016*): One in Three: Internet Governance and Children´s Rights*. Florenz: UNICEF Innocenti.

Staben, Julian (2016): *Der Abschreckungseffekt auf die Grundrechtsausübung*. Tübingen: Mohr/Siebeck.

Stapf, Ingrid / Judith Meinert / Jessica Heesen / Nicole Krämer / Regina Ammicht Quinn / Felix Bieker / Michael Friedewald / Christian Geminn / Nicholas Martin / Maxi Nebel / Carsten Ochs (2020): *Privatheit und Kinderrechte, White Paper Forum Privatheit.* Schriftenreihe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Creative Commons 2020. Online verfügbar unter: https://www.forum-privatheit.de/publikationen/white-paper-policy-paper/ / (Abruf am: 10.10.2020).

Stapf, Ingrid (2019): *„Ich sehe was, was Du auch siehst." Wie wir die Privatsphäre von Kindern im Netz neu denken sollten und was Kinder möglicherweise dabei stärkt – ein kinderrechtlicher Impuls.* In: frühe Kindheit 2(19), S. 12-25.

Stapf, Ingrid (2020): *Kindliche Selbstbestimmung in digitalen Kontexten – medienethische Überlegungen zur Privatsphäre von Heranwachsenden.* In: Buck, Fabian / Drerup, Johannes / Schweiger, Gottfried (Hg.): Neue Technologien – neue Kindheiten? Ethische und bildungsphilosophische Perspektiven, S. 31-54.

Steinberg, Stacey (2017): *Sharenting: Children's Privacy in the Age of Social Media* (March 8, 2016). 66 Emory Law Journal 839. University of Florida Levin College of Law Research Paper No. 16-41.

Turow, Joseph / Hennessy, Michael / Draper, Nora (2015): *The Tradeoff Fallacy. How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*. A Report from the Annenberg School for Communication, Philadelphia, Pennsylvania, USA.

Teil I –
Grundlagen: Kulturgeschichtliche, medienpsychologische, -ethische und -rechtliche Zugänge

Vom Märchen zur App: Kindheiten im historischen Wandel

Regina Ammicht Quinn

Abstract

Während die Vorstellung von Kindheit als eigener Lebensphase historisch relativ neu ist, hat der Medienwissenschaftler Neil Postman schon für das Ende des 20. Jahrhunderts das Ende der Kindheit vorhergesagt. Dieses Ende der Kindheit ist für ihn an die Medialisierung von Kindheiten gebunden und ein „disaster of the first order".

Nun sind Kindheiten heute nicht zu Ende. Aber kontinuierliche Veränderungen machen es nötig, auch einen historischen Blick auf Kinder und Kindheiten zu werfen. Dabei wird deutlich, dass historische Phänomene nicht verschwunden sind, sondern neu gemischt werden und an unterschiedlichen Stellen und in veränderter Form wieder zutage treten. Dieser kulturelle Wandel macht deutlich, dass Kindheiten kein naturgegebenes Phänomen, sondern Zuschreibungen sind – ähnlich wie Zuschreibungen zu Geschlechterrollen oder ethnischen Zugehörigkeiten. Kindheit als Zuschreibung aber bedeutet, dass kontinuierlich nach den Werten dieser Zuschreibung und der Hierarchisierung dieser Werte gefragt werden muss. Diese Hierarchisierungen von Werten dürfen nicht einfach YouTube, Google Classroom oder einer auf Kinder zielende Werbung überlassen werden. Denn an diesen Hierarchisierungen entscheidet sich, ob Kindheiten in gerechter und einer demokratischen Gesellschaft angemessener Weise ermöglicht werden können.

1. Vom Ende der Kindheit

Kindheiten verändern sich momentan in rasantem Tempo. Manche Kinder und Jugendliche bewohnen Welten, die ihre Großeltern, aber auch ihre Eltern noch nicht kannten – eine Welt der Online Spiele, des kontinuierlichen und unmittelbaren schriftlichen, gesprochenen oder bildlichen Kontakts zu anderen, eine Welt des einfachen Zugangs zu Wissen und Fehlinformationen, zu Phänomenen, die nur im Virtuellen existieren und

zu virtuellen Phänomenen, die erheblichen Einfluss auf das Selbstbewusstsein, die Entwicklung und das Selbstwertgefühl von Kindern und Jugendlichen haben.

Kindheiten aber haben sich schon immer verändert. Kindheiten waren schon immer plural, unterschiedlich an unterschiedlichen Standorten, in unterschiedlichen sozialen Schichten, Bildungskontexten und politischen Situationen.

Mit Blick auf Mitteleuropa waren in den letzten drei Jahrzehnten vor allem zwei Phänomene die Treiber der rasanten Veränderungen: neue Vorstellungen von Elternschaft und damit auch neue Familienstrukturen, und die Entwicklung hin zu einer digitalisierten Gesellschaft.

Das Wort „Neue Beelterung" war eines der Kandidaten für das Unwort des Jahres 1997, ein Jahr, nachdem mit „Dolly" das erste Hausschaf geklont wurde. Beides, der Fortschritt in der Genforschung und der Versuch, eine Sprache für neue soziale Lebensformen zu finden, gehören zusammen. Neue Formen der Elternschaft können biomedizinisch hergestellt werden, und damit wandeln sich die Bilder- und Symbolwelten dessen, was ein Kind ist, welche Rolle und welche Räume ihm zugeschrieben werden. Wenn diese Bilder- und Symbolwelten, aber auch die Räume digitalisiert werden, multiplizieren sie sich. Neue Sichtbarkeiten, Orientierungen und Machtverhältnisse entstehen.

Daher ist es sinnvoll, die aktuellen Fragen von Überwachung und Privatheit von Kindern auch in einen historischen Kontext zu stellen. Es gab Zeiten, in denen Privatheit oder Überwachung keine oder eine andere Bedeutung hatten.

Erik Erikson beschreibt in „Childhood and Society" (1950) die Abhängigkeit individueller Erziehung von historischen Wandlungsprozessen. Kontext und Kultur sind treibende Faktoren für die Konstitution der Lebensphasen, in denen ein Kind den Sinn für das Selbst und die eigene Identität entwickelt. 35 Jahre später nimmt Neil Postman Erikson beim Wort: Kindheit ist geprägt durch die neue mediale Umgebung. Und diese mediale Umgebung führt zum Verschwinden der Kindheit:

> „…a new media environment, with television in its center, is leading to a rapid disappearance of childhood in North America. [… C]hildhood will probably not survive the end of this century; and […] such a state of affairs represents a social disaster of the first order." (Postman 1985: 286)

Postmans Diskussion bezieht sich in den 1980er Jahren insbesondere auf die Rolle des Fernsehens in der Gesellschaft und für die Familien. Was aus heutiger Sicht noch fast nostalgische Vorstellungen weckt, ist für Postman

Anzeichen einer Kultur, die sich der Technologie unterwirft; Technik sei nicht mehr die Unterstützung des Menschlichen, sondern werde zur kulturprägenden Handlungsmacht (Postman 1992).

Die Vorstellung der Kindheit als eigener Lebensphase ist relativ neu (Winkler 2019). Folgen wir Postman, ist sie aber auch schon wieder zu Ende. Falls das so ist: Welche Kindheit wäre das gewesen? Und gibt es in der Folge neue Kindheiten?

2. Der Schutz von Kindern: Freiheit und Sicherheit

Die Art und Weise, wie Kinder geschützt werden, welcher Schutz für sie als notwendig und welche Mittel als angemessen geachtet werden, sind ein Anzeichen dafür, wie Kindheiten wahrgenommen und gestaltet werden.

In manchen Kindheiten mussten Kinder vom Spielen nach Hause kommen, wenn die Straßenlampen angingen. In anderen Kindheiten haben Eltern die Möglichkeit, ihre Kinder mit Hilfe von Tracking-Technologien kontinuierlich zu „begleiten".

Die Prothelis AG verkauft Tracking Devices für „Hunde, Kinder, Sport und Wertsachen" (www.prothelis.de). Für Kinder ist die „GRETA App" gedacht, eine Tracking Software mit einem Ortungsgerät, das sich „in der kleinsten Hosentasche" verstauen lässt. Damit werden „Zäune unsichtbar" (ebd.), ein Spielgebiet lässt sich individuell festlegen, und die Eltern werden benachrichtigt, wenn das Kind den Bereich verlässt. Die Eltern können auch, so die Website, mit Anrufen „frühzeitig bei unerwarteten Bewegungen des Kindes" gewarnt werden (ebd.).

Was auch immer für erwartbare Bewegungen in die Technologie eingeschrieben sind: Die App macht – repräsentativ – deutlich, dass Kindheiten heute auf vielen Ebenen über das Gewähren von Freiheit und das Fordern von Sicherheit verhandelt werden. Mit der GRETA App soll Freiheit durch Sicherheit hergestellt werden. In den technischen und nicht-technischen Diskursen zu Freiheit und Sicherheit aber wird häufig nicht berücksichtigt, dass eine Güterabwägung zwischen Freiheit und Sicherheit nicht und nie ausreichend ist; hier müssen auch andere Güter, Prinzipien und unterschiedliche Kontexte berücksichtigt werden, für Kindheiten beispielsweise die Fragen nach Sicherheit und Privatheit, Sicherheit und der Herausbildung von Individualität, Sicherheit und Wachstumschancen und anderes.

Die Geschichten, die als Werbung für die GRETA App erzählt werden, unterscheiden sich deutlich von den Geschichten, in denen Gretel (und ihr Bruder Hänsel) eine Rolle spielen. Das Märchen ist eine der ältesten Erzählformen und transportiert damit Bilder, Emotionen und die Fantasie

früherer Zeitalter mit. Dies geschieht in einem der berühmtesten Märchen Europas in der Besetzung von zwei unschuldigen Kindern, zwei bösen Frauen ((Stief)Mutter und Hexe) und einem schwachen Vater vor dem Hintergrund einer Hungersnot.

Im 19. Jahrhundert hat dieses Märchen Konjunktur:

Die Gebrüder Grimm (Grimm/Grimm 1812-1858) bringen das Märchen in die erste schriftliche Form. In der ersten Fassung 1812 schickt die Mutter die Kinder in den Wald, weil das Essen nicht mehr für alle reicht. Sie treffen auf die Hexe, die Hänsel mästen und essen will, Gretel tötet die Hexe, und die Kinder finden wieder nach Hause, wo die Mutter inzwischen gestorben ist. Die zweite Fassung 1819 malt den Rückweg der Kinder und die Re-Integration in eine Normalität breiter aus. In der Fassung von 1840 ist es nicht mehr die Mutter, die die Kinder los werden will, sondern die Stiefmutter (vgl. dazu Bluhm 2012).

1893 wird Humperdincks Oper „Hänsel und Gretel" (Libretto: Adelheid Wette) in Weimar uraufgeführt – bis heute eines der am häufigsten gespielten Stücke im Opernrepertoire. In dieser spätromantischen Form (und mit Rücksicht auf das deutlich sensiblere Weimarer Publikum) verändern sich die familiären Verhältnisse und mit ihnen das Verständnis von Kindheit. Zwar sind Mutter und Vater keineswegs Rollenvorbilder – die Mutter jähzornig, der Vater betrunken; beides ist mit einer eindeutigen Klassenzugehörigkeit verbunden. Die Liebe der Eltern zu den Kindern aber wird nicht in Frage gestellt. Die Oper zeigt, wie die Mutter die Kinder zum Beerensuchen in den Wald schickt. Die Kinder finden nicht zurück. Die Eltern suchen überall nach ihnen. Und die Kinder, die nun im dunklen Wald übernachten müssen, singen den Abendsegen, dessen 14 Englein auch dramaturgisch auf der Bühne erscheinen:

Abends will ich schlafen gehn,
Vierzehn Engel um mich stehn:
Zwei zu meinen Häupten,
Zwei zu meinen Füßen,
Zwei zu meiner Rechten,
Zwei zu meiner Linken,
Zweie, die mich decken,
Zweie, die mich wecken,
Zweie, die mich weisen,
Zu Himmels-Paradeisen.
(2. Akt)

Alleine im Wald zu übernachten scheint für die Geschwister Humperdinck und Wette und das Weimarer Publikum problematisch zu sein –

darum gibt es schützendes Personal: eine ganze Schutzmauer aus Engeln. Spätestens seit Norbert Elias die Privatisierung und Intimisierung des Schlafes als eines der Kennzeichen des Zivilisationsprozesses beschrieben hat (Elias 1976: 219-230), erscheint diese Situation ziemlich beengt: ein Engel oder auch zwei sehr gerne. Aber vierzehn davon? Diese Überzahl an Schutzpersonal bringt in der Beengtheit eine eigene Freiheit hervor: die Freiheit, sicher im Wald zu schlafen.

Und die Hexe selbst wird am Ende in Lebkuchen verwandelt.

Dieselbe Geschichte – Eltern, zwei Kinder, Not, Gefahr und Überwindung der Gefahr – zeigt in kleinen Verschiebungen der Grundelemente, wie sich innerhalb eines Jahrhunderts die Vorstellung von Kindheit verändert hat: In der 1812 veröffentlichten Version sind die Kinder eine Last, in der nächsten Version wird der Rückweg und damit die Wiederaufnahme in die Familie länger und aufregender. Dann, 1840, ändert sich der Blick auf die Mutterliebe: Keine „richtige" Mutter würde ihre Kinder in die Gefahr schicken; sie wird also zur Stiefmutter. Und im Ausgang des 19. Jahrhunderts ist dann der Blick auf die Kinder ein anderer: Die Erwachsenen sind zuständig für die Sicherheit der Kinder, religiöse Vorstellungen (und das heißt auch: Vorstellungen von transzendentem, herbeirufbarem Schutz) helfen dabei, und alles wird gut – auch weil es zu Beginn nie so schlecht war. Die GRETA App, die ebenfalls einen Schutzraum für Kinder herstellt, ist ein logischer (über)nächster Schritt.

3. Kindheitskonzepte im Widerstreit

Wenn die Geschichte der Kindheit erzählt wird, stößt man auf zwei etablierte, aber widersprüchliche Narrative: Philippe Ariès zeichnet in seiner Geschichte der Kindheit 1960 (D 1975) die Zeit vom 11. bis zum 17. Jahrhundert und den darauffolgenden Wandlungsprozess nach. Ariès, ein enger Freund Foucaults, interessiert sich dafür, wie Mentalitäten rekonstruiert werden können. Bis zum 17. Jahrhundert findet er im Material, das er bearbeitet – vor allem Malerei und Traktate – keine aus der Erwachsenenwelt abgegrenzten und herausgehobenen Kinder. Das gilt auch für das am meisten gezeigte Kind, das Jesuskind, das häufig Gesicht und Gestus eines Erwachsenen hat, auch dort, wo in den Madonnendarstellungen deutlich erotische Motive vorhanden sind. Kinder, so Ariès, waren, sobald sie laufen konnten, in den gemeinsamen Haushalt und dessen Aufgaben integriert. Es gab keine Sonderbereiche des Kindseins: keine spezifische Kleidung, Nahrung oder Unterhaltung. Das gemeinschaftliche Leben zog alle Stände und Altersstufen in einen Sog, mit einem gefühlsmäßig lockeren

Band zwischen Eltern und Kindern. Die Kinder, beschreibt Ariès, waren frei, ohne vernachlässigt oder verachtet zu werden. Im Übergang zur Neuzeit, in der Renaissance, wird das Kind aus der Gesellschaft der Erwachsenen gerissen. Nun wird strenge Kontrolle zur Grundlage jeder Erziehung, die auf Disziplinierung und Standardisierung des Körpers zielt: „Die Leidenszeit der Kinder beginnt mit der Erfindung der Kindheit." (Ariès 1975: 82)

Die Gegengeschichte wird von Psychohistoriker Lloyd deMause erzählt. 1974 erscheint sein Buch „The History of Childhood", das in Deutschland, provokativ, „Hört ihr die Kinder weinen" (deMause 1980) heißt. Die Geschichte, die deMause über die Kindheit erzählt, ist ein „Alptraum, aus dem wir gerade erst erwachen. Je weiter wir in der Geschichte der Kindheit zurückgehen, desto unzureichender wird die Pflege der Kinder, die Fürsorge für sie, und desto größer wird die Wahrscheinlichkeit, daß Kinder getötet, ausgesetzt, geschlagen, gequält und sexuell mißbraucht wurden" (deMause 1980: 12). Erst heute gelingt es, so deMause, eine Beziehungsform der Unterstützung zu entwickeln, in der akzeptiert wird, dass das Kind „besser als seine Eltern weiß, was es braucht" (deMause 1980: 84).

Beide Positionen und Deutungen sind grundlegend kritisiert worden. Es sind zwei unterschiedlich idealisierte Konzepte. Denn es gab mit großer Sicherheit keine Epoche, die Kindern gegenüber völlig gleichgültig war. Der historische Wandel ab dem 17. Jahrhundert war ein diskontinuierlicher Wandel über lange Zeiträume hinweg und voller Brüche; es war ein Wandel, der sich entlang vielfältiger Praktiken von Klasse, Schicht, Geschlecht, Nationalität, regionaler Verankerung und kulturellen Überlieferungen bis heute erstreckt. Während dieser Zeit haben sich spezifische Vorstellungen von Kindheiten herausgebildet, symbolisch gekennzeichnet durch eigene Kleidung, eigene Räume, eigens wahrgenommene Bedürfnisse und die Abtrennung von Sexualität.

Ariès' Einzelanalysen aber liegt eine entscheidende Erkenntnis zugrunde: Kindheit ist kein natürliches, sondern ein historisches Phänomen. Es gibt in allen Gesellschaften Kinder – aber nicht jede Gesellschaft hat eine Vorstellung von Kindheit oder gar ähnliche Vorstellungen von Kindheit (vgl. im Überblick Winkler 2019). Damit ist sein Werk auch politisch zu lesen – als Kritik an der in den 1950er Jahren verbreiteten traditionalistischen These vom Zerfall der Familie (Winkler 2017: 23). Kinder, Kindsein und Kindheit werden in dem langen Übergang hin zur Moderne in neuer Weise in den Blick genommen und reflektiert. Zugleich wird die Geschichte der Kindheit historisch fast ohne Ausnahme als Geschichte der wohlsituierten und weißen Kinder erzählt.

4. Das Kind: schuldig/unschuldig; das Kind: öffentlich/privat

Inmitten dieser historischen Entwicklungen zeigen sich zwei relevante Veränderungen:

Das Kind wird allmählich rein und unschuldig; und dem Kind wird statt der öffentlichen allmählich eine private Rolle zugeschrieben.

Die „Unschuld" des Kindes ist seit Augustinus ein umkämpftes Terrain. Für ihn ist das Neugeborene von der Erbsünde befleckt, die die Eltern durch Geschlechtsakt und Zeugung an das Kind weitergeben. Die menschliche Natur ist per se sündig (z.B. Augustinus 1888, 1.Buch, 7. Kap.: 5f.). In der mittelalterlichen Vermischung von vorchristlichem und christlichem Dämonenglauben werden dann immer wieder „Wechselbälger" identifiziert. Wechselbälger werden vom Teufel gezeugt oder von Hexen in der Wiege ausgetauscht – was man manchmal direkt (wenn ein Kind fehlgebildet ist), manchmal erst später merkt (wenn ein Kind kontinuierlich ungehorsam ist). Für Descartes und dessen frühneuzeitlichen Rationalismus wird dann die Sünde zur Sünde der Unvernunft: Alle menschlichen Irrtümer rühren daher, dass ein Mensch Kind gewesen ist. Man(n) muss sich daher von der Kindheit befreien, so wie man sich von einem Übel befreit (Descartes 1955: 253; zit. n. Badinter 1999: 42f.).

Am Übergang von der Aufklärung zur Romantik aber tritt die Unschuld der Kinder in den Vordergrund. Rousseau ist einer der Protagonisten, für den Kinder nicht durch Sünde, sondern durch Unschuld und Reinheit bestimmt sind (als durchgehendes Motiv in Rousseau [1762] 2013). Die Vorstellung von Unschuld und Reinheit des Kindes hat zwei Konsequenzen, die miteinander verwoben sind:

Als erste Konsequenz entwickelt sich eine emotionale Ökonomie in Bezug auf das Kind. In das Kind wird emotional investiert, und damit wird auch eine (vor allem) emotionale Rendite erwartet. Im 19. Jahrhundert wird Mutterliebe zu einem beherrschenden Thema (Badinter 1994), oft verknüpft mit der Opferbereitschaft der Mütter. Bei Vätern findet sich als Zeichen der emotionalen Ökonomie oft eine Sakralisierung des Kindes. „Child is the Father of Man", so schreibt William Wordsworth (1802; vgl. dazu Winkler 2016). Für ihn ist das (männliche) Kind tief verbunden mit der Natur, die auch als moralischer Richtwert gilt. Das Kind gibt diese Natur-Bindung an den Mann weiter, sodass (zumindest in der englischen Romantik) eine mutterlose Reproduktion des Guten konzipiert wird. Über die englische Romantik hinaus reicht dies bis zu Peter Handke, der 1981 in seiner „Kindergeschichte" das Kind zum moralischen „Lehrherr[n]" macht:

„Er war überzeugt, dass das Kind da ein großes Gesetz verkörperte, welches er selber entweder vergessen oder nie gehabt hatte. War es ihm denn nicht im ersten Monat schon erschienen als sein persönlicher Lehrherr? […] Das-es-war gab dem Erwachsenen das Wahrheitsmaß an; für ein Leben, wie es sein sollte." (Handtke 1981: 63)

Anders als bei Handke, bei dem das bloße Dasein des Kindes genug ist, entwickelt sich in prominenten Teilen der Geistesgeschichte die Vorstellung von Unschuld und Reinheit des Kindes. Aus der Reinheit wird dann die Idee der Formbarkeit des Kindes: Das Kind ist ein unbeschriebenes Blatt und verlangt nach Erziehung. Es ist dann nicht der „Lehrherr" der Erwachsenen, sondern die Erwachsenen werden zu Lehrherren und das Kind zum Objekt gesellschaftlichen Gestaltungswillens (Winkler 2016, Rose 1999). Parallel dazu, manchmal komplementär, manchmal widersprüchlich, wird die „glückliche Kindheit" zum „Selbstdarstellungsprojekt des aufstrebenden Bürgertums. Anders als der seine Kinder in ihrer Entwicklung beschränkende Adel, anders auch als das bildungsferne Proletariat, schien nur der Bürger mit seinem Verständnis von Bildung, Arbeit und Moral eine für seine eigenen Kinder und die Kinder einer ganzen Nation richtige Erziehung gewährleisten zu können" (Winkler 2016; vgl. auch Budde 1994).

Neben dem Wandel hin zur Vorstellung von Unschuld und Reinheit des Kindes ist das Kind eingespannt in das Spannungsfeld von „privat" und „öffentlich" (Ammicht Quinn 2016: 607f.).

Mit einer unklaren Trennung von Öffentlichkeit und Privatheit sind Kinder vor der Renaissance in gewisser Weise „öffentlich". In ihnen schreibt sich eine Ahnenreihe fort, sie sind Bausteine des Fortbestands von Familie und Sippe oder der (vorstaatlichen) Nation, auch notwendige Teile der politischen und der ökonomischen Funktion der Familie, die ja Geburtsstätte ständischer Herrschaft und Ort produktiver Arbeit ist. Im Alltag zeigt sich im „ganzen Haus" auch größte Nähe mit Nicht-Familienangehörigen.

Die allmählich entstehende Spaltung zwischen einem öffentlichen und einem privaten Bereich vor allem ab dem 18. Jahrhundert bringt eine neue Geschlechterordnung und eine neue Generationenordnung hervor, innerhalb derer die Frau zum Privatbereich des Mannes gehört. Kinder gehören zur Frau, mit je nach Geschlecht unterschiedlicher Teilhabe an Öffentlichkeiten des Mannes – bei gleichzeitiger stetiger Institutionalisierung der Bildung. Aufklärerische Freiheit und Gleichheit enden an der Haustürschwelle, wobei im Haus durchaus komplizierte und gegenseitige Abhängigkeitsverhältnisse entstehen können und Männer sich nicht selten in der Rolle eines zusätzlichen Kindes befinden (ebd.).

Dort, wo Beruf und Familie voneinander getrennt werden, regeln Höflichkeitskonzepte Nähe und Distanz und damit auch das Respektieren der Intimität. Dabei wird – über lange Zeiträume und in unterschiedlichen historischen und kulturellen Bewegungen – das unschuldige Kind zum privaten Kind.

Im 19. Jahrhundert und bis in die Gegenwart führt dies zu einer Idealisierung und gleichzeitigen Entmachtung des Kindes. Das Kind wird niedlich (Winkler 2019: 13). Um niedlich zu sein, muss es aber bestimmten ästhetischen und auch intellektuellen Maßstäben genügen. In den USA wird dann – wie im nationalsozialistischen Deutschland – das als „rassisch anders" wahrgenommene Kind aus der Kindheit herausgeschrieben. Jüdische, schwarze oder andere als „unpassend" empfundene Kinder sind nicht „niedlich", sondern (ver)stören die gegenwärtige Gesellschaft und deren wünschbare Zukunft und passen damit nicht in das herrschende Konzept der Kindheit.

5. Erfolgreiche Kindheiten?

Ein Verständnis von Kindheit als eigener Lebensphase mit den dazugehörigen eigenen Kinder-Räumen ist heute Konsens. Diese Lebensphase ist zugleich kommerzialisiert und in zunehmendem Maß digitalisiert. Durch die Vervielfältigung der Bilder werden Idealvorstellungen von Kindheit und Kindsein homogenisiert, während zugleich die jeweiligen empirischen Ausgestaltungen plural sind.

Kinder sind „Privatsache"; das wird beispielsweise im Impfstreit und dem damit geforderten Recht der Verfügung der Eltern über den Kinderkörper deutlich. Zugleich werden Kindheiten veröffentlicht – von den Ultraschallbildern Ungeborener über die Abbildung „niedlicher" Fehler und Peinlichkeiten bis hin zu Lernprogrammen, mit denen, oft unwissend, auch die Lernschwierigkeiten für künftige Profilbildungen relevant werden können.

Die Schutzräume des Privaten waren für Abhängige schon immer ambivalent: Es konnten Räume sein wie Fröbels imaginierter Kinder-Garten, eine Entsprechung des Paradies-Gartens. Fröbel bezieht sich hier auf den Raum einer Zeit der Unschuld, in dem den Kindern die Kindheit geschenkt wird (Fröbel 1848; zit. n. Winkler 2016). Die abgegrenzten Räume aber konnten immer schon zu Räumen der Gewalt werden – im Sinn unmittelbarer, immer wieder auch sexualisierter Gewalt und im Sinn der Gewalt der Marginalisierung, Ausgrenzung, mangelnder Teilhabe oder auch extrem normierter Lebensform und Leistung. In digitalisierten Kinder-

Welten zeigt sich hier beides: Das Durchbrechen oder die Zerstörung des Schutzraumes erscheint hier als ein Vorgang, der nicht immer bei Ariès' idealisierter Freiheit der Kinder unter Erwachsenen endet; das Durchbrechen des Schutzraumes kann problematisch oder bedrohlich sein, etwa dort, wo Informationen, Bilder und Videos nachhaltig verstörend wirken können oder wo die Kontaktaufnahme mit der „realen" Welt jenseits des geschützten Raums gefährlich sein kann. Gleichzeitig aber kann die Digitalisierung der Kindheit eine große Chance sein: die Chance, die Sicht- und Hörbarkeit von Kindern in all ihrer Diversität zu erhöhen.

Der Rückgang der Kinderzahl und der Mortalitätsrate bei Kindern ist eine der Voraussetzungen für die Entstehung einer emotionalen Ökonomie, genauso aber die durch Medialisierung vorangetriebene neue Schätzung des Werts eines Kindes: Kinder sind *economically useless*, *emotionally priceless* (Zelizer 1985, Postman 1985). Dies ist zunächst eine menschenfreundliche Entwicklung, die ihre Wurzeln in der Vorstellung der Unschuld des Kindes hat. Die weniger menschenfreundliche Unterseite zeigt sich in Situationen, in denen Kinder für das Lebensglück der Eltern sorgen müssen und damit mit hohen Hypotheken belastet sind, die sie nie zurückzahlen können. Allerdings sind nicht alle Kinder *economically useless*. Es gibt YouTube-Stars, denen man beim Spielen mit bestellbarem Kinderspielzeug zusehen kann, während sie sehr viel Geld verdienen. Ryan Kaji, 2011 geboren, ist seit 2015 im YouTube-Geschäft mit Videos zum Thema Spielzeug. Für die Jahre 2018 und 2019 gilt er als der bestbezahlte YouTuber, der 22 Millionen US Dollar über die Videos und zusätzliche 26 Millionen US Dollar durch seinen Vertrag mit Walmart verdient.[1] Man mag Kinder wie ihn niedlich finden, aber sie sind mit einem Mal, wie bereits in der Vormoderne, die ökonomische Versicherung ihrer Eltern.

Das heißt: Historische Einzelphänomene sind nicht verschwunden, sondern werden neu gemischt und treten an unterschiedlichen Stellen und in veränderter Form wieder zutage. Beide Bereiche des historischen Wandels – die Schuld oder Unschuld und die Öffentlichkeit oder Privatheit des Kindes – zeigen sich dort in ihrer Ambivalenz und in einer Ausweitung auf das „System Kindheit", wo Kindheiten „erfolgreich" sein müssen.

Noch vor zwei Generationen – in manchen Gegenden und sozialen Schichten viel länger – war die Biografie eines Menschen von Geburt an häufig durch drei Faktoren bestimmt: Genealogie, Geografie, Geschlecht (Ammicht Quinn 2006: 37).

1 https://www.youtube.com/channel/UChGJGhZ9SOOHvBB0Y4DOO_w.

Die Genealogie bestimmte den Ort in einer Familie, in einem Stand oder einer sozialen Klasse, häufig in einem Beruf oder einer Berufsgruppe, in und auf einem bestimmten Niveau des materiellen und geistigen Lebens: der Sohn des Taglöhners und seiner Frau, des Lehrers und seiner Frau. Die Geografie zeigte die Unterschiede zwischen dem Lehrersohn im Schwarzwalddorf oder in Hamburg. Und das Geschlecht zeichnete jeweils einen von zwei möglichen biographischen Wegen vor: Der Lehrersohn wird wieder Lehrer, die Lehrerstochter heiratet einen.

Bis heute ist für Schul- und Berufserfolg der biografische Einfluss durch den sozialen Status der Familie nicht ausreichend ausgeglichen worden. Dennoch haben diese Faktoren heute ihre absolute Prägekraft verloren. In vieler Hinsicht ist aus Schicksal Wahl geworden. Jede*r ist ihres und seines Glückes Schmied, und wem das Schmieden nicht gelingt, ist nicht nur unglücklich, sondern an seinem Unglück auch selber schuld. Und genau hier werden Kindheiten zu Folien für Machbarkeitsdenken (Winkler 2019: 12). So böse das klingt, so verständlich ist es. Die Freiheit, die eigene Biografie zu gestalten, wird zu einer Last. Die Last wird besonders schwer, wenn es um Kinder geht. Die *glückliche Kindheit* als Zielvorstellung des aufstrebenden Bürgertums des 19. Jahrhunderts bekommt dabei die Form der *erfolgreichen Kindheit*. Kinder (und Eltern) werden an öffentlichen Maßstäben gemessen, und wenn die Maßstäbe nicht erreicht werden, kommt für alle, die mit dem „System Kindheit" befasst sind, die Schuldfrage zurück.

Digitale Technologien sind dann Hilfen für die „richtige" Entwicklung und das „angemessene" Lernen; sie demokratisieren den Zugang zu Öffentlichkeiten und das damit verbundene Erfolgsversprechen. Zugleich sind sie Bausteine für die Biografiegestaltung. Dies birgt Chancen und Risiken: Chancen dort, wo hier Kapazitäten der Familien und anderer Beteiligter im „System Kindheit" ergänzt und verstärkt werden können; Risiken dort, wo sich eine neue Möglichkeit des „childhood engineering" (Winkler 2016) auftut, die einem Erziehungsziel von Mündigkeit und (auch demokratischer) Freiheit diametral entgegensteht.

6. Ein Ende der Kindheit?

Neil Postman war sich sicher, dass das Ende der Kindheit droht, falls die industrialisierten Gesellschaften nicht den Hebel umlegen und die kulturdominierende Wirkung der Medien nicht nur kontrollieren, sondern beenden können. Das ist nicht geschehen. Ein Stück weit sehen wir heute Elemente dieses Endes der Kindheit. Etwa dort, wo die Idee der Gestaltung und Formbarkeit von Kindern und der Gestaltungswille von Erwachsenen

mit digitaler Hilfe zum „childhood engineering“ wird; dort, wo aufgeweckte Kinder Zugriff auf alles haben, von allen Formen der Sexualität bis zu allen Formen der Gewalt; oder dort, wo der Schonraum als Raum temporärer Entlastung und Freiheit den Kindern geraubt wird, indem durch digitale Analysen individueller Fehler und Talente in Lernprogrammen Kindern eine offene Zukunft verstellt wird.

Zugleich sind die Kindheiten der Kinder heute natürlich nicht zu Ende. Denn es geht nicht darum, dass Kinder heute eine Kindheit haben sollten, die so schön ist wie sie früher auch nicht war. Der nostalgische Anteil in allen kulturpessimistischen Standpunkten benennt häufig einen Teil der Wahrheit – aber eben nur einen Teil.

Die kulturellen Veränderungen zeigen, was Kindheiten sind: kein naturgegebenes Phänomen, sondern eine Zuschreibung. Kindsein und Kindheit sind Zuschreibungen, in denen Vorstellungen von Natur und Kultur eng verwoben sind ähnlich wie in Zuschreibungen von Geschlechterrollen oder ethnischen Zugehörigkeiten. Dies bedeutet, dass solche Zuschreibungen durchaus miteinander konkurrieren können. Vorstellungen von „Kindheit“ können hinter andere Zuschreibungen – wie „Rasse“ oder Klasse – zurücktreten. So werden diese Zuschreibungen auch Aussagen über Strukturen, Machtvorstellungen und Autoritäten einer Gesellschaft: etwa dann, wenn geflüchtete Kinder nicht zuallererst schutzbedürftige Kinder, sondern „Geflüchtete“ sind, oder dort, wo nicht-weiße Kinder zuallererst „Probleme“ sind und nicht Kinder mit einer offenen Zukunft.

Wenn Kindheit eine Zuschreibung ist, dann ist eine Gesellschaft zur Selbstüberprüfung und zum Handeln aufgefordert. Dies gilt auch und gerade dort, wo sich durch digitale Medien, sei es YouTube, Google Classroom oder auf Kinder zielende Werbung bestimmte normative Vorstellungen von „guter“ oder „erfolgreicher“ Kindheit verfestigen.

Kindheiten sind nicht zu Ende. Sie sind neu und anders mit jeder Generation. Sie sind nicht mehr in einer Weise privat, wie sie es möglicherweise eine relativ kurze Zeit in der Geschichte waren. Kindheiten spielen sich an den vielen Schnittstellen zwischen „öffentlich“ und „privat“ ab; es sind Schnittstellen, an denen die Normen der jeweiligen Bereiche immer wieder, manchmal mühsam, ausgehandelt werden. Die Kinderrechtskonvention der Vereinten Nationen ist hier eine notwendige legale Grundlage. Diese Legalität wird mit Hilfe ethischer Überlegungen zu ihrer konkreten Umsetzung je neu ergänzt.

Wenn Kindheiten grundlegend an Gewährung (oder dem Einfordern) von Freiheiten und dem Herstellen (oder dem Infragestellen) von Sicherheiten für Kinder ihre Formen finden, dann ist es eine gesamtgesellschaftliche Aufgabe, Schutzräume als Ermöglichungsräume zur Verfügung zu

stellen. Es gibt kein allgemeines Rezept dafür, wann, wie und in welchen Mengen und Mischungen Schutz, Fürsorge und Kontrolle in einer digitalisierten Kindheit sinnvoll sind. Dies wird zum einen kleinteilig und individuell, zum anderen politisch und gesellschaftlich ausgehandelt.

Ob Kinder, wie die GRETA App suggeriert, schützenswerte Wertsachen sind, und ob dieser Schutz von imaginierten Engeln oder der Technik kommt: Die Werte, die hier zum Tragen kommen, sind unterschiedlich. Die Fragen, welche Werte essentiell sind, um Kindheiten und das „System Kindheit" zu unterstützen, und wie diese Werte hierarchisiert werden, müssen in den Vordergrund rücken. Denn es muss ständig und ständig neu geklärt werden, wo Sicherheit welchen Freiheiten vorzuziehen ist, ob angestrebter schulischer Erfolg wichtiger ist als Privatheitserwägungen und ob öffentliche Akzeptanz den Vorrang hat vor welchen individuellen Neigungen. Diese Hierarchisierungen von Werten dürfen nicht YouTube, Google Classroom oder einer auf Kinder zielende Werbung überlassen werden. Denn an diesen Hierarchisierungen entscheidet sich, welchen Wert Mündigkeit als Zielvorstellung der gestaltbaren Kindheiten einnimmt und ob Kindheit als Zuschreibung in gerechter und einer demokratischen Gesellschaft angemessener Weise ermöglicht werden kann.

Literatur

Ammicht Quinn, Regina (2006): *Glück – der Ernst des Lebens*. Freiburg: Herder.

Ammicht Quinn, Regina (2016): *Gender - Aufregung um eine Analysekategorie*. In: Stimmen der Zeit 9, S. 600-610.

Ariès, Philippe (1975 [1960]): *Geschichte der Kindheit.* München: Hanser.

Aurelius Augustinus (1888 u.ö.): *Bekenntnisse des heiligen Augustinus*. Übersetzung von Otto F. Lachmann. Leipzig: Reclam.

Badinter, Elisabeth (1991): *Mutterliebe. Geschichte eines Gefühls vom 17. Jahrhundert bis heute*. München: Pieper.

Bluhm, Lothar (2012): *Die „Kinder- und Hausmärchen" der Brüder Grimm. Eine literatur- und kulturwissenschaftliche Einordnung eines ‚Bestsellers'*. Online verfügbar unter: https://literaturkritik.de/id/17417 (Abfrage am: 22.7.2020).

Budde, Gunilla (1994): *Auf dem Weg ins Bürgerleben: Kindheit und Erziehung in deutschen und englischen Bürgerfamilien 1840-1914.* Göttingen: Vandehoeck & Ruprecht. Online verfügbar unter: http://digi20.digitale-sammlungen.de/de/fs1/object/display/bsb00049951_00001.html (Abfrage am: 22.7.2020).

Descartes, René (1955 [1644]): *Die Prinzipien der Philosophie*. Hamburg: Meiner.

DeMause, Lloyd (1980): *Evolution der Kindheit*. In: Ders. (Hg.): Hört ihr die Kinder weinen. Eine psychogenetische Geschichte der Kindheit. Frankfurt a. M.: Suhrkamp, S. 12–112 [(1974): *The History of Childhood.* New York: Harper & Row].

Elias, Norbert (1979 [1939]): *Über den Prozess der Zivilisation*. *Soziogenetische und psychogenetische Untersuchungen.* Erster Band: Wandlungen des Verhaltens in den westlichen Oberschichten des Abendlands. Frankfurt a. M.: Suhrkamp.

Erikson, Erik (1950): *Childhood and Society*. W.W. New York: Norton & Company.

Fröbel, Friedrich (1848) an Luise Levin in Rendsburg v. 11.11./14.11.1848 (Dresden), Bibliothek für Bildungsgeschichtliche Forschung. Online verfügbar unter: http://bbf.dipf.de/editionen/froebel/fb1848-11-11-01.html (Abfrage am: 22.7.2020).

Grimm, Jacob / Grimm, Wilhelm [1812-1857] (1982): *Kinder- und Hausmärchen.* Ausgabe letzter Hand. Mit den Originalanmerkungen der Brüder Grimm. Mit einem Anhang sämtlicher, nicht in allen Auflagen veröffentlichter Märchen und Herkunftsnachweisen, hg. von Heinz Rölleke. 3 Bände. Stuttgart: Reclam.

Handtke, Peter (1981): *Kindergeschichte.* Frankfurt a. M.: Suhrkamp.

Postman, Neil (1985): *The Disappearance of Childhood.* In: Childhood Education 61 (4), S. 286-293.

Postman, Neil (1992): *Technopoly: The Surrender of Culture to Technology*. New York: Vintage Books.

Rose, Nikolas S. (1999): *Governing the Soul. The Shaping of the Private Self*. London: Routledge.

Rousseau, Jean-Jacques (2013 [1762]): *Emile oder über die Erziehung*. Berlin: Edition Holzinger.

Winkler, Martina (2016): *Kindheitsgeschichte*, Version: 1.0. In: Docupedia-Zeitgeschichte, 17.10.2016. Online verfügbar unter: http://docupedia.de/zg/Winkler_kindheitsgeschichte_v1_de_2016 (Abfrage am: 22.7.2020).

Winkler, Martina (2017): *Kindheitsgeschichte. Eine Einführung.* Göttingen: Vandenhoek & Ruprecht.

Winkler, Martina (2019): *Kindheit als Konzept aus historischer Perspektive.* In: Drerup, Johannes / Schweiger, Gottfried (Hg.): Handbuch Philosophie der Kindheit. Berlin: Metzler, S. 9-17.

Wordworth, William (1802): My Heart Leaps Up. Online verfügbar unter: https://poets.org/poem/my-heart-leaps (Abfrage am: 22.07.2020).

Zelizer, Viviana A. (1985): *Pricing the Priceless Child. The Changing Social Value of Children*. New York: Basic Books.

Privatheit aus medienpsychologischer Perspektive: Folgen der zunehmenden Digitalisierung für Kinder und Jugendliche

Judith Meinert, Yannic Meier und Nicole C. Krämer

Abstract

Die Nutzung digitaler Medien, Programme und Systeme ist heute fester Bestandteil des Lebens, sowohl im Alltag als auch zur Kontaktpflege und zum Ausstauch in Schule und Freizeit sowie für Lernzwecke. Dabei werden sowohl explizit als auch implizit zahlreiche persönliche und personenbezogene Informationen gesammelt und gespeichert, was zu Datenschutzrisiken hinsichtlich der Verletzung der horizontalen (durch andere Nutzer*innen) oder vertikalen (durch Unternehmen oder Regierungen) Privatheit führen kann. Insbesondere Kinder und Jugendliche sind als vulnerable Nutzergruppe zu verstehen, die die Risiken, die sich für ihre persönlichen Daten ergeben, nicht vollumfänglich erfassen und ihren Handlungsspielraum bezüglich der Kontrolle ihrer Daten nicht kennen. Die besondere Herausforderung besteht darin, praktikable Lösungsansätze zu finden, die sich nicht auf die binäre Unterscheidung zwischen Nutzung und Nicht-Nutzung beziehen, sondern Kinder und Jugendliche darin unterstützt, effektive Strategien zu erlernen, mit denen sie ihre Daten bei der Nutzung von Medien und Software schützen können (Livingstone/Stoilova/Nandagiri 2019: 4-45). Unter dieser Prämisse beleuchtet der folgende Beitrag potenzielle Risiken der Privatheit von Kindern und Jugendlichen aus entwicklungspsychologischer Perspektive ebenso wie in privaten sowie schulischen Nutzungskontexten und schließt mit der Vorstellung verschiedener Lösungsansätze.

1. Problemstellung

Noch immer verändern digitale Technologien unseren Alltag zusehends. Die Digitalisierung führt zu neuen Möglichkeiten der Kommunikation und der Aufgabenbewältigung im privaten wie im beruflichen Kontext. Doch nicht nur der Alltag der Erwachsenen ändert sich; auch oder viel-

leicht sogar insbesondere der der jungen Generation. Im Lernkontext werden sowohl in der Schule als auch Zuhause Tools eingesetzt, um den Lernfortschritt der Schüler*innen optimal zu unterstützen, aber auch einsehbar und nachvollziehbar zu machen (Romero/Ventura 2020: 1-21, Pardo/Siemens 2014: 438-450). Im privaten Bereich sind Kinder und Jugendliche miteinander über Smartphones vernetzt, treten in Online-Games gegeneinander an, schicken sich per WhatsApp Fotos und Sprachnachrichten und folgen sich gegenseitig auf sozialen Netzwerkseiten (Hajok 2019: 6-8, Rathgeb/Behrens 2018b: 2-88). Auch in den privaten Haushalten, die eigentlich einen Rückzugsort darstellen, halten immer mehr „intelligente" Geräte Einzug, die Daten über die Haushaltsmitglieder und somit auch über Kinder aufzeichnen. Tatsächlich geben zwischen 93 und 97% der 12 bis 19-Jährigen an, ein Smartphone zu besitzen (Engels 2018: 3-26, Rathgeb/Behrens 2018a: 2-80) und 98% berichten, dass ein PC oder Laptop im Haushalt existiert und somit Zugang zum Internet besteht (Rathgeb/Behrens 2018a: 2-80). Auch sogenannte smarte Technologien sind auf dem Vormarsch: 31% der 12-19-jährigen Jugendlichen sagten, dass ein Wearable (ein am Körper getragenes System, das Nutzer- und Interaktionsdaten aufzeichnet) im Haushalt existiert und 16% gaben an, dass ein digitaler Sprachassistent im Haushalt vorhanden ist (Rathgeb/Schmid 2019: 2-60).

Bei allen Vorteilen und Erleichterungen, die diese Technologien mit sich bringen, darf auf der anderen Seite die Tatsache nicht vergessen werden, dass gleichzeitig die Wahrscheinlichkeit von Verletzungen der Privatheit steigt. Besonders bei jungen Menschen scheinen Privatheitsgefährdungen durch andere Personen besonders hoch zu sein (Drachsler/Greller 2016: 89-98). Cyber-Mobbing, Scham durch das unumkehrbare Veröffentlichen intimer Informationen, die für das restliche Leben online abrufbar sein können, aber auch physische Treffen mit Personen, die ihre wahre Identität verschleiern, können die Folge sein. Privatheitsverletzungen können aber nicht nur durch Gleichaltrige oder unbekannte Personen entstehen, sondern auch Eltern wird es erleichtert, viel tiefer in private Bereiche ihres Kindes vorzudringen als es ohne Technologie möglich ist (Pardo/Siemens 2014: 438-450). Zusätzlich sammeln auch Unternehmen unbehelligt Informationen von Kindern und Jugendlichen und legen Persönlichkeitsprofile an (Ifenthaler/Schumacher 2016: 176-181). Je weiter die Technisierung und Digitalisierung voranschreitet, desto einfacher können sensible Daten gesammelt werden, da die Heranwachsenden – häufig unbewusst und lediglich auf Basis ihres Verhaltens – viele Daten von sich preisgeben.

Auf der Basis von einschlägiger Literatur kann zwischen einer horizontalen und einer vertikalen Dimension der Privatheit unterschieden werden

(Masur 2018: 446-465). Dabei ist der vertikalen Privatheit zuzuordnen, dass Technologieanbieter und Internetfirmen Daten sammeln, um sie im Rahmen der Datenökonomie für sich finanziell nutzbar zu machen. Mit horizontaler Privatheit wird angesprochen, dass gleichaltrige Kontaktpersonen Daten erhalten, die zum Beispiel bei Cyber-Mobbing zum Nachteil der Person eingesetzt werden können. Eine Zwischenform, die weder komplett dem vertikalen noch dem horizontalen Bereich zuzuordnen ist, stellen Verletzungen der Privatheit dar, die durch Eltern und Lehrer*innen geschehen. So haben beispielsweise Eltern die Möglichkeit, regelrechte Überwachungs-Apps auf den Geräten ihrer Kinder zu installieren oder Sensoren am Schulranzen anzubringen, die den Weg zur Schule überwachen. Durch Anwendungen wie Google Family Link und Apple Screen Time erhalten Eltern die Kontrolle über zahlreiche Aspekte, wie das Sperren von als ungeeignet empfundenen Internetseiten, die Limitierung der Nutzungszeiten des Geräts, die Ortung des Gerätes, die Entscheidung über den Download von Apps, Nutzungsstatistiken, bis hin zum Mithören von Telefonaten oder Mitlesen von Nachrichten. Allerdings sind auch weitere Elemente der Privatheitsverletzung durch Eltern dokumentiert: über Sharenting (ein Begriff, der sich aus sharing und parenting zusammensetzt und die weitreichende Veröffentlichung von Bildmaterial der eigenen Kinder bezeichnet) werden Fotos oder Videos mit den Kindern als Protagonisten geteilt, ohne dass sie dem zugestimmt haben. Auch die Anschaffung von Geräten wie Sprachassistenten setzt Kinder einem Privatheitsrisiko aus, das sie selbst weder gewählt haben noch überblicken können. Die Möglichkeiten der Überwachung durch Lehrer*innen gestalten sich etwas subtiler. Die Nutzung von Lernsoftware ist beispielsweise dabei behilflich, wesentlich lückenloser als durch die herkömmliche Erteilung von Aufgaben und deren Kontrolle, nicht nur die Lernergebnisse zu prüfen, sondern auch jeglichen Nutzungsfortschritt, Log-in Zeiten und detaillierte Aspekte der Lernkurve nachzuvollziehen (Ifenthaler/Schumacher 2016: 176-181). Die Tatsache, dass dies zu – für manche Schüler*innen nachteilige – Inferenzen über ihre Intelligenz, Leistungsbereitschaft und Tagesabläufe führen kann, wird allerdings bislang kaum diskutiert (Biehl/Hug 2019: 6-96). Auch Überwachungstechnologien auf dem Schulhof oder gar im Klassenraum sind zwar momentan in Deutschland noch undenkbar, werden aber beispielsweise in Australien als Mittel diskutiert, um Bullying zu vermeiden (McKeith 2019).

Im folgenden Beitrag werden diese unterschiedlichen Szenarien aus psychologischer Sicht diskutiert. Dabei wird zunächst aufgezeigt, inwiefern man vor dem Hintergrund entwicklungspsychologischer Erkenntnisse davon ausgehen kann, dass Kinder und Jugendliche tatsächlich besonders ge-

fährdet sind. Dann werden potenzielle Privatheitsverletzungen im privaten Raum analysiert und herausgehoben, welche Aspekte hemmend oder fördernd auf das Privatheitsverhalten von Kindern und Jugendlichen wirken. In einem weiteren Kapitel wird dann der schulische Kontext beleuchtet und reflektiert, welche Gefahren und Chancen dort identifizierbar sind. Abschließend werden mögliche Maßnahmen vorgeschlagen. Die vielschichtige und zentrale Rolle von Eltern und Lehrer*innen werden aufgrund ihrer Bedeutung besonders betont.

2. *Privatheit in entwicklungspsychologischen Zusammenhängen*

Privatheit scheint für die kindliche und jugendliche Entwicklung unerlässlich zu sein. So ist Privatheit zum Beispiel bedeutend für die Entwicklung eines selbstständigen, unabhängigen Selbstkonzeptes. Der wachsende Sinn für das eigene Selbst geht einher mit einem Verständnis von Kontrolle über Informationen, die das eigene Selbst betreffen (Piaget 1966: 528-528). Die Entdeckung, dass Privates, Geheimnisse oder sogar Lügen solange verdeckt bleiben, bis sich das Kind dazu entscheidet, diese Dinge zu enthüllen, führen zum Gefühl eines autonomen Selbstkonzeptes (Kupfer 1987: 81-89). Selbstbestimmung kann beschrieben werden als Kontrolle darüber, welche Aspekte der eigenen physischen oder psychologischen Existenz Teil der Erfahrung einer anderen Person werden oder nicht (Kupfer 1987: 81-89). Privatheit schafft hier also einen Rückzugsort, an dem das eigene Selbst erprobt werden kann, und an dem auch verschiedene Rollen studiert und – ohne Bewertung von anderen – eingenommen oder wieder verworfen werden können.

Entwicklungstheoretikern zufolge gibt es mindestens vier wichtige Entwicklungsziele bei Heranwachsenden: Autonomie, Identität, Intimität und die Entwicklung der sexuellen Persönlichkeit (z.B. Bukatko 2008: 1-577, Steinberg 2008: 78-106). Diese vier Entwicklungsziele scheinen sich stark mit vier von Westin (1967: 166-170) definierten Funktionen der Privatheit zu überschneiden. Diese vier Funktionen der Privatheit sind persönliche Autonomie, Selbstbewertung, begrenzte und geschützte Kommunikation sowie das Ausleben der eigenen Emotionen. Peter und Valkenburg (2011: 221-234) schlussfolgern, dass die Erreichung dieser Entwicklungsziele ohne Privatheit gar nicht oder nur eingeschränkt möglich ist. Sie gehen beispielsweise davon aus, dass Autonomie nur erreicht werden kann, wenn durch die Wahl und Kontrolle des Alleinseins ausreichende Unabhängigkeit geschafft werden kann. Identität und Intimität kann insbesondere in geschützten (Online-)Räumen entwickelt werden, in denen Selbstdarstel-

lung und Kommunikation erprobt werden kann. Außerdem erleichtere die Privatheit die sexuelle Selbstentdeckung, da sie von moralischem Druck befreit (Peter/Valkenburg 2011: 221-234).

2.1 Warum gelten Kinder als besonders vulnerable Gruppe?

Stapf und Kollegen (2020: 3-18) plädieren für einen verstärkten Schutz von Kindern und Jugendlichen in digitalen Kontexten und argumentieren, dass besonders Kinder vulnerabel sind. Es lassen sich drei Bereiche feststellen, hinsichtlich derer sich Kinder von Erwachsenen unterscheiden: der Stand der kognitiven Entwicklung, Unterschiede im Erfahrungshorizont sowie Gepflogenheiten im Umgang mit Medien.

Hinsichtlich der kognitiven Voraussetzungen lässt sich feststellen, dass Kinder unter 11 Jahren nicht nur Konzepte wie ‚Privatheit' nicht vollumfänglich begreifen, sondern vor allem die hinter vielen Digitalangeboten stehende Datenökonomie nicht erfassen sowie kaum verstehen können, dass ihre eigenen Daten von Unternehmen genutzt werden, um Geld zu verdienen (Livingstone/Stoilova /Nandagiri 2019: 4-45). Hier fehlt bei Kindern vor der Adoleszenz das so genannte formal-operationale Denken (Piaget 1972: 1-12), mit dessen Hilfe abstraktes Denken und das Erkennen von (intransparenten) Zusammenhängen gelingen kann. Hinzu kommt, dass in der Pubertät das Funktionieren mancher neuronaler Verschaltungen temporär eingeschränkt feststellbar ist (Powell 2006: 865-867). Dies erschwert das Verständnis potenzieller negativer Konsequenzen von riskantem Verhalten – was vermutlich auch für riskante Selbstdarstellung in sozialen Medien gilt. Vor dem Hintergrund ihrer noch nicht vollständig abgeschlossenen Entwicklung sind Kinder und Jugendliche daher auch besonders anfällig für Online-Dienste, die auf kurzfristige Erfolgserlebnisse und Belohnungsanreize setzen (vgl. Abschnitt 3.1).

Neben den Einschränkungen, die sich aus den kognitiven Fähigkeiten ergeben, spielt ein fehlender Erfahrungshintergrund eine Rolle. Dies wirkt sich beispielsweise so aus, dass Kinder und Jugendliche sich der Gefahren für Privatheit und Datenschutz und den potenziellen Folgen eher wenig bewusst sind (Heeg/Genner/Steiner/Schmid/Suter/Süss 2018, Naplavova/Ludík/Hruza/Bozek 2014: 3552-3555). Dennoch macht sich vor allem die Medienberichterstattung bemerkbar, die Eltern und Kinder hinsichtlich potenzieller Risiken sensibilisiert hat: Werden Kinder direkter befragt, welche Gefahren sie im Internet vermuten, werden vor allem horizontale Privatheitsbedrohungen genannt (zum Beispiel Online-Mobbing oder Cyber-Grooming). Somit beziehen sich die Befürchtungen von Kindern und

Jugendlichen in Bezug auf eine Verletzung ihrer Online-Privatheit vor allem auf andere Nutzer*innen und somit horizontale Privatheitsbedrohungen. Dies wird durch Beschränkungen des Zugriffs auf einzelne Beiträge oder das gesamte Profil zu verhindern versucht (Borgstedt/Roden/Borchard/Rätz/Ernst 2014: 1-175). Ein vergleichsweise hohes Bewusstsein findet sich auch hinsichtlich der Gefahren des Cyber-Grooming im Sinne der Kontaktanbahnung durch Fremde (Mascheroni/Jorge/Farrugia 2014: 2). Über die Hintergründe und potenziellen Gefahren der Datenökonomie besteht dagegen kaum Bewusstsein (Livingstone/Stoilova/Nandagiri 2019: 4-45), was offensichtlich nicht nur daran liegt, dass Kinder und Jugendliche dies kognitiv kaum verarbeiten können, sondern dass zu diesen Themen auch wesentlich weniger Informationen an Kinder (und Eltern) gerichtet werden.

Ein dritter Grund, warum Kinder und Jugendliche als besonders vulnerable Gruppe gelten können, liegt darin begründet, dass diese anders an Medien herangehen als Erwachsene. So werden durch den selbstverständlichen Gebrauch von neuen Technologien, bestimmte Nudging- oder Persuasionsmechanismen nicht hinterfragt und als „normale" Aspekte des Internets empfunden (Wang/Shi/Kim/Oh/Yang/Zhang/Yu: 2019: 1-9). Auch die Tatsache, dass Kinder und Jugendliche sich neuen Spielen und Funktionen eher durch Ausprobieren nähern – statt zum Beispiel Testberichte oder Bedienungsanleitungen zu lesen – kann dazu führen, dass Gefahren nicht rechtzeitig erkannt werden (Borgstedt/Roden/Borchard/Rätz/Ernst 2014: 1-175). Hinzu kommt, dass Nutzungsbedingungen und Anleitungen sich auch eher primär an Eltern wenden. Eine informierte Entscheidung, die aus datenschutzrechtlicher Sicht auch von minderjährigen Nutzer*innen im Sinne einer wirksamen Einwilligung erforderlich ist, kann daher eigentlich nicht gegeben werden (vgl. Roßnagel/Bile/Nebel/Geminn/Karaboga/Ebbers/Bremert/Stapf/Teebken/Thürmel/Ochs/Uhlmann/Krämer/Meier/Kreutzer/Schreiber/Simo 2020: 5-32). Auf Basis der zu geringen Informationen über Risiken und Nachteile überwiegen in der Entscheidung, die Technologie zu nutzen, die unmittelbar transparenten Vorteile und weniger die nur indirekt erkennbaren Nachteile. Aus juristischer Sicht heißt es dazu in Erwägungsgrund 38 der Datenschutz-Grundverordnung (DSGVO):

> „[1]Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.[2] Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von

Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen.[3] Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein."

3. Probleme in privaten Nutzungskontexten

Wie bereits eingangs geschildert, nutzen Kinder und Jugendliche Technologien wie soziale Medien mittlerweile umfangreich, um mit anderen zu kommunizieren. Dabei verhalten sie sich im Schnitt sorgloser als Erwachsene dies tun: Im Zusammenhang mit sozialer Netzwerknutzung wurde beispielsweise herausgefunden, dass Kinder und Jugendliche (10 – 19 Jahre alt) mehr Informationen von sich preisgeben und ihre Privatheit schlechter durch mögliche Einstellungen schützen als Ältere (Walrave/Vanwesenbeeck/Heirman 2012). Außerdem wurde in dieser Studie gezeigt, dass jüngere Kinder ihre Privatheit schlechter schützten als ältere, dass aber gleichzeitig Kinder und Jugendliche, die besorgt um ihre privaten Informationen waren, dazu tendierten, ihre Daten auch besser zu schützen. Es scheint also lohnenswert, die Faktoren zu analysieren, die dazu beitragen, dass mehr oder weniger Informationen in privaten Kontexten geteilt werden. Betrachtet wird der Beitrag, den die Anwendungen selbst leisten (im Sinne des Angebotscharakters (Affordances) der Technik, der die Nutzenden zur Nutzung anregt), der Einfluss Gleichaltriger sowie der Einfluss der Eltern (vgl. Stapf/Meinert/Heesen/Krämer/Ammicht Quinn/Bieker/Friedewald/Geminn/Martin/Nebel/Ochs 2020: 3-18).

3.1 Der Einfluss von Affordances

Affordances können als fundamentale Objekteigenschaften beschrieben werden, die den potenziellen Gebrauch bestimmen (Livingstone/Stoilova/Nandagiri 2019: 4-45). Der Angebotscharakter zahlreicher Technologien ist dadurch charakterisiert, dass zur Nutzung geradezu aufgefordert wird. So bauen viele Social Media Programme (wie WhatsApp, Instagram, Facebook, Snapchat, Pokemon-Go oder TikTok) auf sozialen Belohnungssyste-

men auf. Dies geschieht entweder durch Push-Nachrichten oder Belohnungen für erreichte Ziele oder durch die soziale Vernetzung mit anderen Nutzenden und deren Förderung (zum Beispiel durch die Möglichkeit, sich niedrigschwellig soziale Belohnungen und Feedback wie Likes zu senden). Hinzu kommt, dass oft nicht ersichtlich wird, wer die Nachrichten sehen kann oder wie lange die Nachrichten gespeichert werden. So wird ein WhatsApp Chat zwischen zwei Personen als privat empfunden (Borgstedt/Roden/Borchard/Rätz/Ernst 2014: 1-175), obwohl die Inhalte an andere weitergesendet werden können.

Zusammengefasst besteht die spezifische Gefahr, die von den Affordances ausgeht, darin, dass sie auf der einen Seite mit Vorteilen einhergehen, die Kinder und Jugendliche für sich nutzen, dass dieselben Funktionen aber auch mit Gefahren verbunden sind. Dies lässt sich auch in empirischen Untersuchungen aufzeigen: Jugendliche nutzen manche Social Media Affordances (Persistenz, Reproduzierbarkeit, Skalierbarkeit und Durchsuchbarkeit bit-basierter Informationen) offenbar, um Entwicklungsziele zu erreichen (Peter/Valkenburg 2011: 221-234). Das bedeutet, dass einerseits Affordances die gesunde Entwicklung von Kindern und Jugendlichen unterstützen können. Andererseits existiert jedoch gleichzeitig die Gefahr, dass dieselben Affordances die Entwicklung gefährden können, indem sie zu negativen Erfahrungen wie Privatheitsverletzungen führen.

Kinder und Jugendliche könnten hier besonders gefährdet sein, da sie zum einen eine verminderte Einschätzung negativer Konsequenzen und zum anderen eine verringerte Selbstwirksamkeit, negative Konsequenzen vermeiden zu können, aufweisen (Cohn/Macfarlane/Yanez/Imai 1995: 217-222).

Durch die einfach zu erreichenden Belohnungen und die nicht oder nur unklar kommunizierten Risiken wird die Tragweite der vermeintlich harmlosen Informationsweitergabe nicht deutlich (Engels 2018: 3-26). Ähnliche Tendenzen werden bereits im sogenannten "Privacy Calculus" (Culnan/Armstrong 1999: 104-115) beschrieben, der aufzeigt, dass ein kurzfristiger Nutzen angestrebt wird und darüber die langfristigen Folgen in den Hintergrund geraten. Inwieweit diese Überlegungen tatsächlich im Sinne rationaler, bewusster Entscheidungen fallen, wird allerdings kritisch diskutiert und muss umso mehr für Kinder hinterfragt werden.

3.2 Gleichaltrige als Einflussfaktoren

In ganz ähnlicher Weise wie die Affordances der Technologien wirken auch Gleichaltrige in die Richtung, dass die positiven Seiten der Social Media Nutzung deutlicher wahrgenommen werden. Die sogenannte Peergroup verstärkt die Wahrnehmung der Vorteile der Social Media Nutzung, da es für Kinder und Jugendliche eine besonders hohe Wichtigkeit hat, dazuzugehören und Teil der Gemeinschaft zu sein. Da beispielsweise WhatsApp Gruppen häufig zur Kommunikation im Klassenverband genutzt werden, isolieren sich Kinder und Jugendliche durch fehlende Teilnahme (Engels 2018: 3-26, Rathgeb/Behrens 2018a: 2-80). Selbst wenn Privatheitsbedenken vorhanden sind, werden diese aufgrund des Wunsches nach Zugehörigkeit in den Hintergrund gedrängt.

3.3 Eltern als Einflussfaktoren

Neben den Gleichaltrigen sind aber auch die Eltern und gegebenenfalls ältere Geschwister einflussreich, wenngleich über andere Mechanismen als bei Gleichaltrigen. Basierend auf den Annahmen zum Modelllernen nach Bandura (1979: 193-236) kann angenommen werden, dass Kinder sich insbesondere an ihren Eltern orientieren. So kann sich etwa auch im Verhalten der Kinder abbilden, wenn die Eltern selbst sorglos Familienbilder auf Instagram und anderen sozialen Medien teilen (Sharenting). Ebenso wird der Umgang mit Sprachassistenten und Smart-Home-Steuerungs-Apps gelernt. Problematisch sind die natürlichen Lernvorgänge vor allem dann, wenn die Eltern aufgrund der hohen Komplexität selbst mit der Risikoeinschätzung überfordert sind (Kutscher/Bouillon 2018, Manske/Knobloch 2017: 1-97). Da diese Überforderung häufig auf sozioökonomische Unterschiede und einen mangelnden Wissensstand zurückzuführen ist, können sich Wissensklüfte auch auf nachfolgende Generationen auswirken (Paus-Hasebrink/Sinner/Prochazka/Kulterer 2018: 209-225).

Um Kindern und Jugendlichen die Entwicklung von kritischer Urteilskraft und einen reflektierten Umgang mit Technologien zu ermöglichen, sollte das Wissen über Erfahrungen in konkreten Kontexten vertieft werden (Stapf 2019: 12-25). Da Eltern oftmals überfordert sind, haben Bildungsinstitutionen, das heißt vorrangig Schule und Lehrer*innen, eine Verantwortung zur Vermittlung zentraler Kompetenzen. Dass aber Schule zunehmend auch selbst Fragen nach Privatheit im Bildungskontext beantworten muss, wird im nächsten Kapitel thematisiert.

4. Probleme im Bildungskontext

Der heute nahezu omnipräsente Zugriff auf Smartphones, Tablets und Laptops durch Kinder und Jugendliche hat neben der Nutzung privater Apps, Spiele und Softwareprogramme auch die Anwendung von Lernsoftware in der Schule stark befördert (Link/Schwarz/Huber/Fischer/Nuerk/Cress/Moeller 2014: 257-277). Einerseits ergibt sich durch den Einsatz digitaler Technologien zum Lernen die Möglichkeit innovative, kreative und individuell zugeschnittene Lernmethoden zur Wissensvermittlung und -vertiefung anzuwenden (Avella/Kebritchi/Nunn/Kanai 2016: 13-29). Insbesondere die im Jahr 2020 vorherrschende Covid-19 Pandemie, die zu einer deutschlandweiten Schulschließung führte, betonte die Relevanz und Notwendigkeit einer Digitalisierung in der Schule (Steinberg/Schmid 2020), da lediglich durch den Einsatz digitaler Lehr- und Lernmethoden der Unterricht weiter stattfinden konnte.

Andererseits ergeben sich aus dem Einsatz von Lernsoftware – sowohl in der Krise als auch abseits einer Pandemie – jedoch auch einige problematische Aspekte. Grundlegend bieten Lernsoftwarelösungen Lernunterstützung zu verschiedenen Themen und Fächern, die auf unterschiedliche Wissensstände und individuelle Lerntypen und -fortschritte abgestimmt sind (Ifenthaler/Schumacher 2016: 176-181). Das beinhaltet u.a. auch den reziproken Austausch mit anderen Lernenden und Lehrenden ebenso wie den Vergleich von Lernerfolgen und -ergebnissen (Pardo/Siemens 2014: 438-450). So können Lehrkräfte beispielsweise direkt innerhalb der Lern-App Feedback zum Lösungsansatz und -ergebnisse einer Aufgabe geben, um individuell zu unterstützen und anzuleiten. Zwangsläufig geht damit auch eine enorme Sammlung von persönlichen Daten einher. Dabei werden demografische Daten wie Geschlecht, Alter und Nationalität, administrative Informationen wie Schulform, Klasse, Stadt, Interaktionsdaten und Chatverläufe mit anderen Nutzer*innen und dem System als auch jegliche individuelle Eingaben des oder der Lernenden (z.B. Eingaben in Texte und Quizze, Beiträge in Foren und individuelle Daten wie das Vorwissen, Testergebnisse und teilweise sogar Motivationen oder Stimmungszustände) gespeichert (Ifenthaler/Schumacher 2016: 176-181, Romero/Ventura 2020: 1-21).

In Anlehnung an die im vorherigen Kapitel dargestellte Problematik in Bezug auf den Aufforderungscharakter von Apps, die zudem auf langfristige Nutzerbindung durch wiederholte Belohnung setzen (Engels 2018: 3-26), kommt erschwerend hinzu, dass die Funktionsweise sowie bestimmte Verarbeitungsmechanismen (z.B. der persönlichen Daten) von Lernsoftware intransparent und im Speziellen für die Schüler*innen unverständ-

lich gestaltet sind (Drachsler/Greller 2016: 89-98). Das bezieht sich beispielsweise darauf, dass die Schüler*innen oftmals nicht vollumfänglich wissen oder erfassen können, wer Einsicht in ihre Daten hat. Das kann der Fall sein, wenn Lehrkräfte Einblicke in Lernkurven und -fortschritte sowie die von den Schüler*innen gewählten Lösungswege haben. Auch kann es durch ein auf Basis aller Schüler*innen eines Klassenverbands erstelltes Scoring oder einen Leistungsvergleich zur Einsicht in die Daten anderer kommen.

Als Quintessenz daraus ergeben sich in diesem Kontext besonders starke Risiken für die Privatheit der Kinder und Jugendlichen. So existiert darüber hinaus die Gefahr einer kommerziellen Nutzung der Daten (Mühlhoff 2020, Tsai/Whitelock-Wainwright/Gašević 2020: 230-239). Dabei lässt sich von vertikalen Privatheitsbedrohungen (Masur 2018: 446-465, Masur/Teutsch/Dienlin 2019: 337-365) sprechen, die die Weitergabe von Daten an Unternehmen und Institutionen beschreiben. In diesem Zuge können aus den persönlichen Daten durch Analyse- und Prädiktionsverfahren personalisierte Werbeangebote, aber auch ganze Datenprofile, zum Beispiel auf Basis der eingegebenen Hintergrunddaten wie Geschlecht oder Nationalität generiert werden (Tsai/Whitelock-Wainwright/Gašević 2020: 230-239). Diese Datafizierung kann schwerwiegende Folgen haben (Tsai/Whitelock-Wainwright/Gašević 2020: 230-239): So kann die Prädiktion von Verhalten und Leistung zu Benachteiligungen in der Beurteilung von Schüler*innen (z.B. für die Empfehlung einer weiterführenden Schulform oder eines Studien- oder Ausbildungsplatzes) führen und in einer regelrecht systemischen Stigmatisierung gewisser (Nutzenden-)gruppen gipfeln (Knijnenburg/Raybourn 2019: 1-14). Die Tatsache, dass Kinder und Jugendliche sich in einem Entwicklungsstadium befinden, in dem sie noch Veränderungen in der Ausgestaltung ihrer Persönlichkeit und ihres Verhaltens unterliegen, erhöht die schwerwiegenden Konsequenzen einer solchen persistenten Stigmatisierung und macht ihre Daten besonders sensibel und schützenswert (Mühlhoff 2020).

Darüber hinaus besteht eine Bedrohung der horizontalen Privatheit. Diese bezieht sich auf den Zugriff auf die eigenen Daten durch andere Personen (Masur/Teutsch/Dienlin 2019: 337-365). Durch die Nutzung von Lernsoftware besteht die Möglichkeit, dass Lehrkräfte, Eltern und Mitschüler*innen Einblicke in die sensiblen Leistungs- und Lernfortschrittsdaten der Schüler*innen bekommen. Oftmals werden die individuellen Leistungsdaten (z.B. Lösungen von Aufgaben) automatisch im Klassenverband miteinander verknüpft und an Eltern und Lehrer*innen versandt (Pardo/Siemens 2014: 438-450). Das birgt nicht nur die Gefahr von Kontrolle und Überwachung durch Eltern und Lehrkräfte, sondern kann darüberhinaus-

gehend auch zu Mobbing bezüglich schlechter oder guter Leistungen durch andere Mitschüler*innen führen. Ein weiterer potenzieller Nachteil besteht in der unbewussten Beeinflussung von Lehrer*innen in ihrer Bewertung von Schüler*innen und deren Leistungen durch die Einsicht in die Herangehensweise an die Aufgabenlösung und eventuelle Fehlversuche, die im Rahmen der Lösungsfindung entstanden sind. Zudem haben die Nutzenden keinerlei Einfluss auf die automatischen Freigabeprozesse, können diese nicht stoppen oder verhindern und werden nicht nach ihrer Einwilligung gefragt. Auch sind sie nicht in der Lage in irgendeiner Form privatheitsregulierende Strategien zu ergreifen wie beispielsweise die Anonymisierung ihrer Inhalte oder die Einschränkung des Adressatenkreises (Masur/Teutsch/Dienlin 2019: 337-365).

Dementsprechend liegt insgesamt die Kontrolle über die eigenen Daten im Rahmen der Nutzung digitaler Lernsoftware nicht bei den jungen Nutzer*innen selbst. Oftmals mangelt es an Aufklärung, Sensibilisierung und Unterstützung über die Sammlung und Speicherung von Daten (und der dadurch möglichen Erstellung, Interpretation und Weitergabe von Datenprofilen). Das ist zum einen dem mangelnden Fachwissen und der Weiterbildung der Lehrkräfte (Kumar/Chetty/Clegg/Vitak 2019: 1-13) geschuldet. Jedoch gibt es auch von Seiten der Hersteller solcher Software nur wenig Informationen (z.B. im Rahmen von Datenschutz policies) und Anleitungen für spezifische Nutzereinstellungen (Boninger/Molnar/Saldaña 2019)

Im Zuge der Covid-19 Pandemie ist es im Bildungsbereich zu einer „Turbo-Digitalisierung" (Mühlhoff 2020) gekommen, da aufgrund der landesweiten Schulschließungen andernfalls kein Unterricht hätte stattfinden können. Dadurch sind neben der Erkennung der Notwendigkeit zum Ausbau digitaler Lernmethoden aber auch deren Schwachstellen und Probleme sichtbar geworden. So wurden zum Teil Applikationen wie Zoom oder WhatsApp aus der Not heraus zu Kommunikationszwecken aktiviert, trotz des Wissens wie wenig Datenschutz dort geboten ist (Mühlhoff 2020). Weiterhin hat sich offenbart, dass die Schulen zudem meistens von Privatanbietern abhängig sind, da die schulisch und staatlich geförderten Anbieter sich entweder nicht bewährt oder durchgesetzt haben (Schuknecht/Schleicher 2020: 68-70). Dabei spielt auch das Vertrauen der Schüler*innen (und deren Eltern) in Institutionen wie Schulen und damit einhergehend auch Lehrer*innen eine große Rolle. Wenn diese die Nutzung einer Software im Unterricht initiieren oder für vertiefende Übungen zu Hause empfehlen, vertrauen die Schüler*innen instinktiv darauf, dass die Nutzung ebendieser Applikationen ihnen nicht schaden wird (Tsai/Whitelock-Wainwright/Gašević 2020: 230-239). Konterkariert wird dies durch den Mangel an Fachwissen und Weiterbildungsmöglichkeiten der meisten

Lehrkräfte, die sich nicht in der Lage sehen, Datenschutzrisiken von Lernsoftware erkennen, vermitteln und aufheben zu können (Reinhardt 2020).

Insgesamt ist es in besonderer Weise erforderlich (geworden), praktikable Wege zu finden für den Einsatz digitaler Lernsoftware, ohne dass der Schutz der persönlichen Daten und der Privatheit der Schüler*innen vernachlässigt wird.

5. Lösungsansätze

Kindern und Jugendlichen ist Online-Privatheit keineswegs egal. Wie Livingstone und Kolleginnen (2019: 4-45) zeigen, wünschen sich Kinder aller Altersklassen, dass sie Kontrolle über das dauerhafte Löschen persönlicher Daten haben, dass persönliche Daten nicht mit Dritten geteilt werden, dass mehr Privatheitsschutz im Internet besteht und dass privatheits- und datenschutzrelevante Vorgänge besser verständlich sind. Außerdem gibt es für verschiedene Altersgruppen spezielle Wünsche, die an das altersbedingte Verständnis von Privatheit gekoppelt sind. So wünschen sich 11–12-Jährige, dass Online-Inhalte angemessener für Kinder und Jugendliche sind und dass Services für Kinder nutzbar sind, ohne dass dabei persönliche Daten gesammelt werden. In der Altersgruppe der 13 bis 14-Jährigen werden Wünsche nach bezahlbaren Angeboten, die privatheitsschützend sind, eine einfache Löschung und der Nicht-Weiterverkauf persönlicher Daten laut. 15 bis 16-Jährige geben an, dass persönliche Daten besser geschützt sein sollten, dass Unternehmen auf Datensparsamkeit setzen sollten und dass mehr Transparenz über die Sammlung und Verwendung persönlicher Informationen geben sollte.

Die Suche nach möglichen Lösungen, die oben beschriebenen Privatheitsprobleme zu minimieren, kann sich als sehr schwierig gestalten. Für unterschiedliche Privatheitsrisiken müssen unterschiedliche Lösungsansätze gefunden werden. Zum einen gehen verschiedene Risiken von unterschiedlichen Parteien, wie etwa Eltern, Lehrer*innen oder Mitschüler*innen oder aber Internetfirmen oder Fremden aus. Zum anderen hängt das Verständnis von Privatheit und das Bewusstsein für die digitale Datenverarbeitung stark vom Alter der Kinder ab (Livingstone/Stoilova/Nandagiri 2019: 4-45), wie in den vorherigen Abschnitten deutlich geworden ist. Dadurch sind die potenziellen Lösungsansätze an die jeweiligen Altersklassen gekoppelt.

5.1 Medienkompetenz als Grundlage eines sicheren Online-Verhaltens

Medienkompetenz im Allgemeinen ist sowohl für Kinder und Jugendliche als auch für Erwachsene eine wichtige Voraussetzung für einen verantwortungsvollen, bewussten und selbstbestimmten Umgang mit Medien (Aufderheide 1993: 1-44). Die Schaffung von Medienkompetenz und deren Subfacette Privatheitskompetenz sind wichtige Voraussetzungen dafür, einen autonomen und informierten Umgang mit den eigenen Daten zu erlernen und das Recht auf informationelle Selbstbestimmung ausüben zu können. Da die Privatheit von Kindern, wie die der Erwachsenen, sowohl auf horizontaler Ebene als auch auf vertikaler Ebene Angriffen ausgesetzt ist (Debatin 2011: 47-60), müssen auch hier verschiedene Lösungen gefunden werden. Online-Privatheitskompetenz setzt sich aus faktischem als auch aus prozeduralem Wissen, also theoretischem und praktischem Wissen über Privatheitsfragen zusammen (Trepte/Teutsch/Masur/Eicher/Fischer/Hennhöfer/Lind 2015: 333-365). Der theoretische Teil der Privatheitskompetenz beinhaltet beispielsweise Wissen über technische Aspekte der Datenverarbeitung und des -schutzes, potenzielle Privatheitsrisiken, die damit einhergehen als auch Kenntnisse über Gesetze, die die persönliche Privatheit regulieren. Praktisches Wissen sind Kenntnisse darüber, wie man die eigene Online-Privatheit mithilfe bestimmter Verhaltensweisen oder Technologien schützen kann. Allerdings sprechen sich Forscher*innen dafür aus, nicht allein Privatheitskompetenz, sondern Medien- oder digitale Kompetenzen im Allgemeinen zu vermitteln (Buckingham 2015: 21-35).

In einer kürzlich erschienenen Studie mit Kindern im Alter von 9 bis 13 Jahren wurde gezeigt, dass gezieltes Training das Wissen der Kinder über potenzielle Gefahren und entsprechenden Schutz vor diesen Gefahren signifikant verbessern kann (Desimpelaere/Hudders/Van de Sompel 2020: 1-12). Ein interessantes Ergebnis dieser Untersuchung bestand darin, dass der Lerneffekt für jüngere Kinder größer war als für ältere. Zudem konnte gezeigt werden, dass Kinder, die vorher über bestimmte Privatheitsrisiken aufgeklärt wurden, im Nachgang weniger dazu bereit waren, persönliche Informationen in einer bestimmten Situation zu teilen. In einem weiteren Versuch zeigten die Ergebnisse allerdings gegenteiliges: Privatheitskompetenz und Privatheitssorgen hingen negativ miteinander zusammen und letztere hingen wiederum negativ mit der allgemeinen Bereitschaft zusammen, persönliche Informationen im Netz preiszugeben. Somit hatte Privatheitskompetenz einen indirekten positiven Einfluss auf die Intention, Informationen zu teilen. Laut den Autor*innen der Studie zeigt sich an diesem Befund eine potenzielle Schattenseite der Privatheitskompetenz:

Obwohl Kinder, die sich auf Basis eines Privatheitskompetenz-Training eines hohen Privatheitsrisikos bewusst waren, weniger persönliche Informationen von sich teilen wollten, zeigte sich parallel, dass Kinder mit größerem Wissen über Online-Privatheit ein falsches Gefühl von Sicherheit oder eine gewisse laissez fair Attitüde entwickeln können und somit wieder potenziell höheren Risiken ausgesetzt wären (Desimpelaere/Hudders/Van de Sompel 2020: 1-12). Somit ist die Schaffung von Privatheitskompetenz bereits in jungen Jahren ein wichtiges Ziel, da generell davon auszugehen ist, dass diese den Umgang mit persönlichen Informationen und das Bewusstsein für Privatheitsrisiken verbessert. Es sollte allerdings nicht vernachlässigt werden, dass eine gesteigerte Schulung von Kompetenzen unter Umständen bei manchen Personen auch einen negativen Effekt haben kann.

Ein Beispiel für eine verständliche Übersicht von Privatheitsgefahren für Kinder und Jugendliche im Netz stellt das „Teaching Privacy Curriculum" dar (Egelman/Bernd/Friedland/Garcia 2016: 591-596). Diese englischsprachige Website bietet Informationen zu zehn von den Forscher*innen selbstentwickelten Prinzipien für Eltern, Lehrer*innen und Schüler*innen an. Diese Prinzipien werden sowohl durch kurze Beschreibungen der Gefahren und einer vorgeschlagenen Gegenmaßnahme als auch einer ausführlichen Beschreibung erklärt. Die zehn Punkte beschreiben verschiedene Gefahren im Netz, wie beispielsweise, dass Daten aus verschiedenen Quellen aggregiert werden und so Rückschlüsse auf persönliche Vorlieben und Eigenschaften gezogen werden können; dass die Online-Welt ebenso real ist, wie die physische Welt und man sich online so verhalten sollte wie offline; dass man online nicht anonym ist, auch wenn es sich so anfühlt; und dass Personen sich als jemand anderes ausgeben können. Somit werden unterschiedliche Bereiche abgedeckt, die sowohl die horizontale als auch die vertikale Privatheitsebene betreffen.

Ähnliche Websites existieren auch in Deutschland. Beim ZDFtivi Projekt „App On" (ZDF 2020) wird mit kurzen Videos und dazugehörigen aufklärenden Texten über potenzielle Gefahren im Netz informiert. Die Videos und Texte sind dabei gezielt auf ein jüngeres Zielpublikum zugeschnitten. Inhaltlich thematisieren die Videos verschiedene Security- und Privatheitsrisiken wie Cyber-Mobbing, Phishing oder die generelle Wichtigkeit des Datenschutzes und präsentieren jeweils Lösungsvorschläge. Darüber hinaus werden allerdings auch weitere Themen wie Fake News adressiert. Somit wird hier nicht nur die Privatheitskompetenz von Kindern und Jugendlichen, sondern die Medienkompetenz im Allgemeinen geschult. Eine weitere deutschsprachige Website zur Schulung der Medienkompetenz bietet die „Initiative klicksafe" (Europäischen Union für mehr Sicherheit im Internet 2020) an. Das Besondere an dieser Website ist,

dass hier nicht nur speziell Kinder und Jugendliche adressiert werden, sondern dass es auch eigene Bereiche für Eltern und für Pädagogen gibt. Außerdem ist der Kinder-Bereich der Webseite unterteilt in Angebote für jüngere und ältere Kinder.

Bei allen Vorteilen, die die Erhöhung der Medien- und Privatheitskompetenz mit sich bringt, sind auch diesem Ansatz natürliche Grenzen gesetzt. Zwar kann durch einen informierten und bewussten Umgang mit persönlichen Informationen im Netz und mit sicheren Privatheitseinstellungen die Eintrittswahrscheinlichkeit möglicher Risiken minimiert werden, allerdings bleibt immer ein gewisses Restrisiko bestehen und teilweise ist die Nutzung bestimmter Apps oder Services alternativlos.

5.2 Software-Lösungen

Neben der Eigenverantwortung der Kinder und Jugendlichen und der Notwendigkeit, dass Eltern bei Privatheitsangelegenheiten Unterstützung leisten müssen, sollte – auch aus ethischen Überlegungen heraus – zumindest diskutiert werden, ob alle Verantwortlichkeiten bei den Betroffenen liegen sollten. Die Probleme, die sich daraus ergeben, dass Eltern die Verantwortung für das datenschutzkonforme Verhalten ihrer Kinder übernehmen, wurde oben bereits geschildert: Zum einen müssen Eltern unterstützend die Internetnutzung ihrer Kinder regulieren, um sie vor potenziellen Privatheitsrisiken schützen zu können. Zum anderen ist aber auch das Internet- und App-Nutzungsverhalten der Kinder als ein privates Verhalten einzustufen, das nicht gänzlich offengelegt werden sollte, da es (vgl. Abschnitt 2) zur kindlichen Entwicklung von Autonomie und einem Selbst-Gefühl ein Bewusstsein über die eigene Person und Persönlichkeit) beiträgt. Außerdem sollte es Kindern in gewissem Ausmaß selbst überlassen sein, welchen Inhalten sie sich zuwenden möchten, da dies zur Entwicklung von Persönlichkeit und zum eigenen Lernfortschritt beiträgt. Folglich entsteht ein Spannungsfeld zwischen der elterlichen Fürsorgepflicht und der kindlichen Privatheit. Hier könnten verschiedene Softwarelösungen Abhilfe schaffen, die bestimmte Bereiche des Internets für das Kind unzugänglich machen. Somit können sich Kinder nach wie vor den individuell ansprechenden Bereichen zuwenden, ohne dabei auf potenziell ungeeignetes Material zu stoßen, wie beispielsweise Propaganda, Pornographie oder Gewalt.

Neben dem generellen Schutz vor unangebrachten Inhalten können auch Spiele, Software und Apps für Kinder und Jugendliche so gestaltet werden, dass sie per Voreinstellung datenschutzfreundlicher sind (Bieker/

Hansen 2017: 165-170). Das bezieht sich auf die Prinzipien ‚Privacy by Default' und ‚Privacy by Design' und beschreibt, dass Software in ihrer grundsätzlichen Funktionsweise protektiv bezüglich der Freigabe der persönlichen Daten ist und jede weitere Freigabe, Nutzung oder Weiterleitung von Daten explizit autorisiert und bewilligt werden muss. Darüber hinaus besagen die Prinzipien, dass nicht alle Daten der Nutzenden gesammelt werden sollten, sondern eine auf die/den Nutzer*in und Anwendungskontext zugeschnittener Datenschutz implementiert werden (Knijnenburg/Raybourn 2019: 1-14). Das würde auch beinhalten, dass nicht das System die Datenweitergabe ungefragt initiiert, sondern die Nutzenden selbst. Für die Nutzung von Lernsoftware könnte das beispielsweise bedeuten, dass die Schüler*innen auswählen können, mit welchen Mitschüler*innen sie ihre Ergebnisse und Fortschritte teilen und vergleichen möchten und wann und mit welchen Zwischenschritten ihre Ergebnisse an die Lehrer*innen übersandt werden.

5.3 Umgang mit Affordances

Ein weiterer relevanter Aspekt betrifft die oben beschriebenen Media Affordances. Im Internet und speziell in der interpersonellen Kommunikation in sozialen Medien existiert eine Reihe verschiedener Affordances, die die Interaktion zwischen Individuen prägen. Zum einen gibt es Affordances, die die Privatheit von Nutzenden potenziell gefährden können. Zum anderen können bestimmte Affordances aber auch zu einer Erhöhung der Online-Privatheit beitragen. Zum Beispiel kann Anonymität die Eigenschaft beschreiben, dass Nachrichten versendet werden können, ohne die eigene Identität preiszugeben, was potenziell privatheitsfördernd ist. Die Affordance der Persistenz kann andererseits privatheitsreduzierend sein, da Inhalt, der einmal geteilt wurde, viele Jahre oder gar Jahrzehnte später noch von anderen Personen eingesehen, geteilt oder von Firmen genutzt werden kann (vgl. Trepte 2020: 1-22).

Ein bewusster Umgang mit und Kenntnisse über Affordances sollten daher sowohl Kindern als auch Erwachsenen vermittelt werden. Dieses Wissen und die entsprechenden Fähigkeiten lassen sich sicherlich auch unter die allgemeine Medien- bzw. Privatheitskompetenz fassen; allerdings ist es hier wichtig, diesen Aspekt gesondert zu betrachten, da Kinder von einigen Affordances besonders profitieren, was sie in besonderem Maße verwundbar macht (Peter/Valkenburg 2011: 221-234). Weiterhin müssten Funktions- und Verarbeitungsmechanismen transparenter gestaltet werden, so dass Kinder und Jugendliche ein besseres Verständnis z.B. über die

Abhängigkeit von Belohnungssystemen erhalten. Auch transparente Informationen darüber, welche Daten zu welchem Zweck gesammelt werden, würde weitere Aufklärung schaffen. Als eine besonders auf die Zielgruppe abgestimmte Maßnahme, wäre z.B. eine kindgerechte Darstellung durch Bilder und Icons denkbar (Holtz/Nocun/Hansen 2011: 338-348).

6. *Fazit*

Die Omnipräsenz von Smartphones und Tablets beginnt heutzutage bereits im Kindesalter und ermöglicht auch den Zugang zu Applikationen, die von Kindern und Jugendlichen zum Spielen, Chatten und Kommunizieren ebenso wie zum Lernen und Vertiefen von Schulinhalten genutzt werden. Neben den Vorteilen einer vernetzten, innovativen Integration digitaler Anwendungen und Software im Freizeit- und Schulbereich, kommt es allerdings auch zur Sammlung enormer Datenmengen. Dabei führt die Verwendung vernetzter, digitaler Software dazu, dass sowohl andere Nutzende als auch Unternehmen und Institutionen Zugriff auf die persönlichen Daten bekommen können, sodass sich in vielfacher Hinsicht Privatheitsbedrohungen ergeben.

Als Nutzergruppe sind Heranwachsende dabei als besonders schützenswert zu sehen, da sie sich einerseits noch in der Entwicklung befinden, was auch die Veränderung von Persönlichkeit und Verhalten umfasst, und andererseits oftmals kognitiv noch nicht in der Lage sind, komplexe und intransparente Funktions- und Verarbeitungsmechanismen zu erfassen.

Mögliche Lösungsansätze beziehen sich zum einen auf das Design von Software, das schon in den Grundeinstellungen den Schutz der Privatheit und der persönlichen Daten stärker berücksichtigen sollte. Darüberhinausgehend sollte auch die Medienerziehung generell und bezüglich des Datenschutzes sowohl zu Hause als auch in der Schule ausgebaut werden. Indem Kindern und Jugendlichen Herangehensweisen und Lösungsansätze für den Umgang mit Privatheitsrisiken (sowohl horizontal als auch vertikal) gezeigt werden, wird ihre Selbstwirksamkeit in Bezug auf den Schutz und die Weitergabe ihrer persönlichen Daten gestärkt (Youn 2009: 389-418). Das würde auch der verbreiteten Wahrnehmung entgegenwirken, dass Datenschutz ein binäres Konstrukt ist, in dem man sich nur für (zu Lasten des Datenschutzes) oder gegen (um die eigenen Daten zu schützen) die Nutzung von Apps und Software entscheiden kann.

Basierend auf diesen Erkenntnissen plädieren wir für einen „kollektiven Datenschutz“ (vgl. Mühlhoff 2020), der insbesondere die Auswertung und Datafizierung der Daten Heranwachsender aus vernetzten digitalen Umge-

bungen, in denen Kinder und Jugendliche ihre Freizeit und Schulzeit verbringen, auf gesetzlicher und edukativer Ebene ebenso wie hinsichtlich der Gestaltung von Software protektiver regelt.

Literatur

Aufderheide, Patricia (1993*): Media literacy. A report of the National Leadership Conference on Media Literacy*. Queenstown, Maryland: The Aspen Institute.

Avella, John. T. / Kebritchi, Mansureh / Nunn, Sandra G. / Kanai, Therese (2016): *Learning analytics methods, benefits, and challenges in higher education: A systematic literature review*. In: Online Learning 20 (2), S. 13-29.

Bandura, Albert (1979): *The social learning perspective: Mechanisms of aggression*. In: Toch, Hans (Hg.): Psychology of crime and criminal justice. Prospect Heights, IL: Waveland Press, S. 193-236.

Biehl, Christopher Julien (2019): *Entwicklung einer Unterrichtsreihe zu dem Thema Datenschutz mit Fokus auf den mathematischen Relationen in Sozialen Netzwerken*. Masterarbeit. Universität Koblenz: Koblenz-Landau.

Bieker, Felix / Hansen, Marit (2017): *Datenschutz "by Design" und "by Default" nach der neuen europäischen Datenschutz-Grundverordnung*. RDV, 4, S. 165-170.

Boninger, Faith / Molnar, Alex / Saldaña, Christopher M. (2019): *Personalized learning and the digital privatization of curriculum and teaching*. Whitepaper. National Educational Policy Center. Online verfügbar unter: https://nepc.colorado.edu/publication/personalized-learning (Abfrage am: 7.10.2020).

Borgstedt, Silke / Roden, Ingo / Borchard, Inga / Rätz, Beate / Ernst, Susanne (2014): *DIVSI U25-Studie: Kinder, Jugendliche und junge Erwachsene in der digitalen Welt*. SINUS Institut Heidelberg, S. 1-175.

Buckingham, David (2015): *Defining digital literacy – What do young people need to know about digital media?* In: Nordic Journal of Digital Literacy 10, S. 21-35.

Bukatko, David (2008): *Child and adolescent development: A chronological approach.* Boston: Houghton Mifflin Company.

Cohn, Lawrence D. / Macfarlane, Susan / Yanez, Claudia / Imai, Walter K. (1995): *Risk perception: differences between adolescents and adults.* In: Health Psychology 14 (3), S. 217-222.

Culnan, Mary. J. / Armstrong, Pamela K. (1999): *Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation*. In: Organization Science 10 (1), S. 104-115.

Debatin, Bernhard (2011*): Ethics, privacy, and self-restraint in social networking.* In: Trepte, Sabine / Reinecke, Leonard (Hg.): Privacy online. Perspectives on privacy and self-disclosure in the social web. Berlin / Heidelberg: Springer, S. 47-60.

Desimpelaere, Laurien / Hudders, Liselot / Van de Sompel, Dieneke (2020): *Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behaviour.* In: Computers in Human Behavior 110, S. 1-12.

Drachsler, Hendrik / Greller, Wolfgang (2016): *Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics*. In: Proceedings of the Sixth International Conference on Learning Analytics & Knowledge, S. 89-98.

Egelman, Serge / Bernd, Julia / Friedland, Gerald / Garcia, Dan (2016): *The teaching privacy curriculum.* In: Proceedings of the 47th ACM Technical Symposium on Computing Science Education, S. 591-596.

Engels, Barbara (2018): *Datenschutzpräferenzen von Jugendlichen in Deutschland: Ergebnisse einer Schülerbefragung.* In: IW-Trends-Vierteljahresschrift zur empirischen Wirtschaftsforschung, 45 (2), S. 3-26.

Europäische Union (2020): Die EU-Initiative für mehr Sicherheit im Netz. Online verfügbar unter: https://www.klicksafe.de/impressum (Abfrage am: 20.08.2020).

Hajok, Daniel (2019): Der veränderte Medienumgang von Kindern. Tendenzen aus 19 Jahren KIM-Studie. JMS Jugend Medien Schutz-Report 42 (3), S. 6-8.

Heeg, Rahel / Genner, Sarah / Steiner, Olivier / Schmid, Magdalene / Suter, Lillian / Süss, Daniel (2018): Generation Smartphone. Ein partizipatives Forschungsprojekt mit Jugendlichen. Online verfügbar unter: http://www.generationsmartphone.ch./ (Abfrage am: 20.08.2020).

Holtz, Leif-Erik / Nocun, Katharina / Hansen, Marit (2010): *Towards displaying privacy information with icons*. IFIP PrimeLife International Summer School on Privacy and Identity Management for Life, S. 338-348.

Ifenthaler, Dirk / Schumacher, Clara (2016): *Learning analytics im Hochschulkontext*. WiSt-Wirtschaftswissenschaftliches Studium 45 (4), S. 176-181.

Knijnenburg, Bart P / Raybourn, Elaine M. (2019): *Learner privacy*. Sandia National Lab. Albuquerque, NM.

Kumar, Priya C. / Chetty, Marshini / Clegg, Tamara L. / Vitak, Jessica (2019): *Privacy and security considerations for digital technology use in elementary schools.* In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, S. 1-13.

Kupfer, Joseph (1987): *Privacy, autonomy, and self-concept*. In: American Philosophical Quarterly, 24 (1), S. 81-89.

Kutscher, Nadia / Bouillon, Ramona (2018): *Kinder. Bilder. Rechte. Persönlichkeitsrechte von Kindern im Kontext der digitalen Mediennutzung in der Familie*. Schriftenreihe Deutsches Kinderhilfswerk.

Link, Tanja / Schwarz, Eva J. / Huber, Stefan / Fischer, Ursula / Nuerk, Hans-Christoph / Cress, Ulrike / Moeller, Korbinian (2014): *Mathe mit der Matte – Verkörperlichtes Training basisnumerischer Kompetenzen.* In: Zeitschrift für Erziehungswissenschaft 17(2), S. 257-277.

Livingstone, Sonia / Stoilova, Mariya / Nandagiri, Rishita (2019): *Children's data and privacy online: Growing up in a digital age: An evidence review.* London School of Economics and Political Science: London.

Manske, Julia / Knobloch, Tobias (2017): *Datenpolitik jenseits von Datenschutz*. Stiftung Neue Verantwortung, S. 1-97.

Mascheroni, Giovanna / Jorge, Ana / Farrugia, Lorleen (2014): *Media representations and children's discourses on online risks: Findings from qualitative research in nine European countries*. In: Cyberpsychology: Journal of Psychosocial Research on Cyberspace 8(2), S. 27-34.

Masur, Philipp K. (2018): *Mehr als Bewusstsein für Privatheitsrisiken. Eine Rekonzeptualisierung der Online-Privatheitskompetenz als Kombination aus Wissen, Fähig-und Fertigkeiten.* In: M&K Medien & Kommunikationswissenschaft 66 (4), S. 446-465.

Masur, Philipp K. / Teutsch, Doris / Dienlin, Tobias (2019): *Privatheit in der Online Kommunikation.* In: Schweiger, Wolfgang / Beck, Klaus (Hg.): Handbuch Online-Kommunikation. Wiesbaden: Springer, S. 337-365.

McKeith, W. (2019): *CCTV is watching students and teachers, but how much surveillance do schools need?* In: The Syndey Morning Herald, 14.07.2019. Online verfügbar unter: https://www.smh.com.au/national/cctv-is-watching-students-and-teachers-but-how-much-surveillance-do-schools-need-20190712-p526o9.html (Abfrage am: 25.08.2020).

Mühlhoff, Rainer (2020): *We need to think data protection beyond privacy: Turbo Digitalization after COVID-19 and the biopolitical shift of digital capitalism.* In: Netzpolitik.org, 23.06.2020. Online verfügbar unter: https://netzpolitik.org/2020/warum-wir-gerade-jetzt-eine-debatte-ueber-datenschutz-brauchen/ (Abfrage am: 20.08.2020).

Naplavova, Magdalena / Ludík, Tomás / Hruza, Petr / Bozek, Frantisek (2014): *General awareness of teenagers in information security*. In: International Journal of Information and Communication Engineering 8 (11), S. 3552-3555.

Pardo, Abelardo / Siemens, George (2014): *Ethical and privacy principles for learning analytics.* In: British Journal of Educational Technology 45(3), S. 438-450.

Paus-Hasebrink, Ingrid / Sinner, Philip / Prochazka, Fabian / Kulterer, Jasmin (2018): *Auswertungsstrategien für qualitative Langzeitdaten: Das Beispiel einer Langzeitstudie zur Rolle von Medien in der Sozialisation Heranwachsender.* In: Scheu, Andreas M. (Hg.): Auswertung qualitativer Daten. Wiesbaden: Springer, S. 209-225.

Peter, Jochen / Valkenburg, Patti M. (2011): *Adolescents' online privacy: Toward a developmental perspective.* In: Trepte, Sabine / Reinecke, Leonard (Hg.): Privacy online. Perspectives on privacy and self-disclosure in the social web. Berlin / Heidelberg: Springer, S. 221-234.

Piaget, Jean (1966): *The psychology of intelligence and education.* In: Childhood Education 42(9), S. 528-528.

Piaget, Jean (1972): *Intellectual evolution from adolescence to adulthood.* In: Human Development 15 (1), S. 1-12.

Powell, Kendall (2006): *Neurodevelopment: How does the teenage brain work?* In: Nature 442, S. 865-867.

Rathgeb, Thomas / Behrens, Peter (2018a): *JIM-Studie 2018. Jugendliche, Information, Medien. Basisuntersuchung zum Medienumgang Zwölf-bis 19-Jähriger.* Medienpädagogischer Forschungsverbund Südwest, S. 2-80.

Rathgeb, Thomas / Behrens, Peter (2018b): *KIM-Studie 2018. Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang Sechs-bis 13-Jähriger.* Medienpädagogischer Forschungsverbund Südwest, S. 2-88.

Rathgeb, Thomas / Schmid, Thomas (2019): *JIM-Studie 2019. Jugend, Information, Medien. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger.* Medienpädagogischer Forschungsverbund Südwest, S. 2-60.

Reinhardt, Michael (2020): *Das digitale Bildungssystem offenbart seine Mängel*. In: Gründerszene. Online verfügbar unter: https://www.gruenderszene.de/technologie/digitalisierung-schulen-corona?interstitial (Abfrage am: 20.08.2020).

Romero, Cristobal / Ventura, Sebastian (2020): *Educational data mining and learning analytics: An updated survey.* In: Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 10 (3), S. 1-21.

Roßnagel, Alexander / Bile, Tamer / Nebel, Maxi/ Geminn, Christian / Karaboga, Murat / Ebbers, Frank / Bremert, Benjamin / Stapf, Ingrid / Teebken, Mena / Thürmel, Verena / Ochs, Carsten / Uhlmann, Markus / Krämer, Nicole / Meier, Yannic / Kreutzer, Michael / Schreiber, Linda / Simo, Hervais (2020): *EINWILLIGUNG. Möglichkeiten und Fallstricke aus der Konsumentenperspektive.* Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.

Schuknecht, Ludger / Schleicher, Andreas (2020): *Digitale Herausforderungen für Schulen und Bildung.* In: ifo Schnelldienst 73 (5), S. 68-70.

Stapf, Ingrid (2019): *„Ich sehe was, was Du auch siehst." Wie wir die Privatsphäre von Kindern im Netz neu denken sollten und was Kinder möglicherweise dabei stärkt – ein kinderrechtlicher Impuls.* In: Frühe Kindheit 2 (19), S. 12-25.

Stapf, Ingrid / Meinert, Judith / Heesen, Jessica / Krämer, Nicole C. / Ammicht Quinn, Regina / Bieker, Felix / Friedewald, Michael / Geminn, Christian / Martin, Nicholas / Nebel, Maxi / Ochs, Carsten (2020): *Privatheit und Kinderrechte*. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.

Steinberg, Laurence (2008): *A social neuroscience perspective on adolescent risk-taking.* In: Developmental Review 28(1), S. 78-106.

Steinberg, Mario / Schmid, Yannick (2020): *Digitalisierung in der Krise: COVID-19 und das Bildungswesen. Soziologiemagazin, Blogreihe# 8: Soziologische Impulse während Corona.* Online verfügbar unter: https://soziologieblog.hypotheses.org/13571 (Abfrage am: 20.08.2020).

Trepte, Sabine (2020): *The social media privacy model: Privacy and communication in the light of social media affordances.* In: Communication Theory, S. 1-22.

Trepte, Sabine / Teutsch, Doris / Masur, Philipp K. / Eicher, Carolin / Fischer, Mona / Hennhöfer, Alisa / Lind, Fabienne (2015): *Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS).* In: Gutwirth, Serge / Leenes, Ronald / De Hert, Paul (Hg.): Reforming European data protection law. Dordrecht: Springer, S. 333-365.

Tsai, Yi-Shan / Whitelock-Wainwright, Alexander / Gašević, Dragan (2020): *The privacy paradox and its implications for learning analytics.* In: Proceedings of the Tenth International Conference on Learning Analytics & Knowledge, S. 230-239.

Walrave, Michel / Vanwesenbeeck, Ini / Heirman, Wannes (2012): *Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults.* In: Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6 (1).

Wang, Xuewei / Shi, Weiyan / Kim, Richard / Oh, Yoojung / Yang, Sijia / Zhang, Jingwen / Yu, Zhou (2019): *Persuasion for Good: Towards a Personalized Persuasive Dialogue System for Social Good.* In: arXivLabs. Online verfügbar unter: https://arxiv.org/abs/1906.06725 (Abfrage am: 7.10.2020).

Westin, Alan F. (1967): *Privacy and freedom.* In: Washington and Lee Law Review 25(1), S. 166-170.

Youn, Seounmi (2009): *Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents.* In: Journal of Consumer Affairs 43 (3), S. 389-418.

ZDF (2020): *App +on – Sicher ins Netz mit Handy und Co.* Online verfügbar unter: https://www.zdf.de/kinder/app-und-on (Abfrage am: 20.08.2020).

Aufwachsen in überwachten Umgebungen: Medienethische Überlegungen zum Kinderrecht auf Privatheit im Zeitalter des Digitalen

Ingrid Stapf

Abstract

Mit dem Aufkommen überwachungsbasierter Medientechnologien von Smart Toys, Babysitter-Kameras in Teddybären bis hin zu Sprachassistenzsystemen wie Alexa, individualisierter Lernsoftware, Tracking-Apps oder Videoüberwachung in der Kita, ist die Frage aufgeworfen, was Privatheit von Kindern heute ausmacht: Bedarf es bei Kindern anderer Konzepte als bei Erwachsenen? Wie können sie den Schutz ihrer Daten im Altersverlauf steuern lernen? Und wer sind hierfür Verantwortungsträger? Der Beitrag untersucht aus medienethischer Perspektive das Kinderrecht auf Privatheit im Zeitalter des Digitalen. Von einem Beispielfall ausgehend wird erarbeitet, was die erhöhte Verletzlichkeit von Kindern begründet, wie das Kinderrecht auf Privatheit mit Blick auf personale Selbstbestimmung umgesetzt werden kann, was den Wert von Privatheit für Kinder ausmacht sowie was daraus für ein Recht auf Privatheit in digitalen Kontexten folgt. Hierzu wird eine kinderrechtliche Perspektive eingenommen, indem Kinder als handelnde Subjekte verstanden werden, die im Zuge ihrer sich noch entwickelnden Fähigkeiten verbriefte Rechte auf Schutz, Befähigung und Beteiligung haben. Um das Zusammenspiel dieser Rechte zu ergründen werden aktuelle empirische Daten und Rahmenbedingungen aufgegriffen und argumentiert, dass die Rechte von Kindern auch im Digitalen gelten und besser durchgesetzt werden sollten, dass sie dabei aber mit Blick auf die konkrete Lebenswelt relational und kontextbezogen aufzugreifen sind. Kindliche Rechte auf Privatheit bedürfen aus menschenrechtlicher Sicht folglich pädagogischer, technischer und regulatorischer Bedingungen dafür, dass Kinder sie kennen, konkret erfahren und in der Folge aktiv selbst ausüben lernen.

1. Mediatisierte Kindheit und Privatheit – einführende medienethische Überlegungen

In einem Interview mit einer 4.-Klässlerin berichtet ein Mädchen von einer Puppe, der sie im Vertrauen ihre Geheimnisse erzählt hatte. Und wie sie sich schämte, als sie erst später erfuhr, dass die Puppe alle Gespräche aufgezeichnet und gespeichert hatte. Es seien doch *ihre* Geheimnisse gewesen und jetzt wisse sie gar nicht, wer sie alles hören könne.[1]

Beispiele wie diese legen nahe, dass sich die Frage der Privatheit mit Blick auf Kinder anders als bei Erwachsenen stellt, da Kindheit eine besonders verletzliche Entwicklungsphase ist. Ausgehend von diesem Beispiel soll im Folgenden eine medienethische Perspektive auf die Frage der Privatheit von Kindern[2] in überwachten Umgebungen erarbeitet werden, die in aktuelle Kontexte und Problemlagen rund um mediatisierte Kindheit eingebettet wird. Denn durch das Aufkommen überwachungsbasierter Medientechnologien, wie Smart Dolls, Babysitter-Kameras in Teddybären bis hin zu Home-Robotern wie Alexa, individualisierte Lernsoftware, Tracking-Apps oder Videoüberwachung in der Kita, ist heutige Kindheit in besonderem Maße von privatheitsgefährdenden Techniken betroffen. Was können wir dabei über den Wunsch von Kindern nach Privatsphäre wissen? Bedarf es bei Kindern anderer Konzepte als bei Erwachsenen? Und wie können Kinder den Schutz ihrer Daten steuern lernen? Und was verändert daran vielleicht auch Kindheit selbst?

Kindheit ist heute *mediatisierte Kindheit* (Krotz 2001, Tillmann/Hugger 2014). Dass Medien Einzug in das heutige Leben von Kindern halten, legen empirische Daten offen. Sie zeigen eine stärkere Verfügbarkeit und wachsende Nutzungszahlen von Medien bei immer jüngeren Kindern. So stellt die aktuelle *KIM-Studie* (MPFS 2019a) fest, dass fast alle Kinder zwischen sechs und 13 Jahren (98 %) zuhause das Internet nutzen können und die Hälfte der Kinder ein eigenes Smartphone hat. Sie recherchieren über Suchmaschinen (65 %), verschicken *WhatsApp*-Nachrichten (62 %) oder

1 Das Interview mit einer 4.-Klässlerin an einer Berliner Grundschule entstand im Rahmen eines medienpädagogischen Projekts von Martin Riemer und wurde auf dem Netzfest der re:publica 2019 diskutiert (vgl. https://19.netzfest.de/de/session/wo-stimmen-kindern-netzpolitik-was-es-gibt-was-es-braucht).

2 Den Begriff „Kinder" benutze ich hier mit der UN-Kinderrechtskonvention, die Kindheit als Phase zwischen der Geburt und bis zum vollendeten 18. Lebensjahr (und de facto bis zur Volljährigkeit) versteht. Damit wird im Folgenden nicht zwischen Kindern und Jugendlichen unterschieden, es sei denn, die Begriffe werden beispielsweise in Gesetzestexten wie dem „Jugendmedienschutz" verwendet.

schauen *YouTube*-Videos (56 %). Beliebteste soziale Medien der 14- bis 24-Jährigen sind laut *DIVSI-Studie* (DIVSI 2018) *WhatsApp*, *YouTube* und *Instagram*. Heranwachsende verabreden sich über soziale Medien oder verhandeln Identitätsfragen über ihre Postings auf *Snapchat* oder *Instagram*. Schüler*innen recherchieren Hausaufgaben im Internet und schauen sich *YouTube*-Erklärvideos an. Sie sitzen in ihren Kinderzimmern und spielen vernetzte Computerspiele mit Freunden. All dies hat sich in der Folge des Digitalisierungsschubs im Zuge der Corona-Pandemie verstärkt.

Gerade weil Kinder digitale Medien schon stückweise *selbst bestimmt* nutzen, können sie aber auch viel früher schon Erfahrungen machen, die nicht altersgerecht oder gar verstörend sind. Mit dem ersten internetfähigen Smartphone haben Kinder Zugang zum globalen Netz, das derzeit weitgehend unreguliert ist. So gibt jeder fünfte Jugendliche an, dass schon einmal falsche oder beleidigende Inhalte über die eigene Person online oder über das Smartphone verbreitet wurden (MPFS 2019b: 49). Ein stringenter Jugendmedienschutz kann nicht mehr, wie früher, durch eine Eingangskontrolle im Kino, erreicht werden. So haben Anbieter von Pornographie wie *YouPorn* ihren Sitz im Ausland und können nicht ausreichend national reguliert werden. Dies hat beispielsweise zur Folge, dass Kinder pornographische Inhalte über *Pornhub* im Instagram-Feed abonnieren können. Und dass sie dabei auswertbare Spuren im Netz hinterlassen. Mit der „Mediatisierung sozialer Welten" (Krotz et al. 2014) lassen sich analoge und digitale Lebenswelten nicht mehr trennscharf voneinander unterscheiden. Das betrifft Kinder wie Erwachsene gleichermaßen. In der gelebten Praxis ihrer Lebenswelt sind beide Bereiche – gerade mit Blick auf die Spuren ihrer Daten – ineinander verwoben.

Aktuell zeigt sich vor allem eine große Verunsicherung. Mediale und öffentliche Diskurse fokussieren schnell auf extreme Beispiele (wie Computerspielesucht oder „digitale Demenz") und verbreiten „Moralpanik". Auf diese folgen oft strikte Verbote oder Rückzugsforderungen. Viele Eltern fühlen sich überlastet und orientieren sich selbst noch in diesen Veränderungen. Die Medienforschung und die Medienregulierung kommen mit der Geschwindigkeit der Entwicklungen kaum mit. Im Bereich digitale Medien und Kindheit liegt damit ein großer gesellschaftlicher Orientierungsbedarf.

Dies ist nicht zu unterschätzen, wenn man bedenkt, dass, laut einer *UNICEF-Studie*, ein Drittel der weltweiten Internetnutzer*innen mittlerweile Kinder unter 18 Jahren sind (Livingstone/Carr/Byrne 2016: 7): „An estimated one in three of all Internet users in the world today is below the age of 18." Kinder sind also *medial mittendrin*.

Dass Kindheit heute mediatisiert ist, meint dabei nicht nur einen technischen, sondern auch einen kulturellen und sozialen Wandel ihrer Lebenswelt. Diese ist eben auch eine *datafizierte Lebenswelt*, in der alle kindlichen Zugriffe, Tätigkeiten und Kontakte in der Welt der Codes und von Big Data abgebildet und ausgewertet werden. Aktuell gefährdet auch Online-Überwachung kindliche Privatheit, indem Massenüberwachungstechnologien von Regierungen und Firmen eingesetzt werden können, „to track, store, and analyse children´s actions with a level of detail previously unattainable" (Brown/Pecora 2014).

All diese Themenaspekte betreffen grundlegende Fragen der Ethik. Auch wenn es bereits erste ethische Auseinandersetzungen mit mediatisierter Kindheit und Jugend (Stapf/Prinzing/Köberer 2019) gibt, so wurde die Frage nach Privatheit mit Blick auf Heranwachsende im deutschsprachigen Raum bislang kaum wissenschaftlich bearbeitet. Heutige Kindheit ist nicht nur „mediatisierte Kindheit" (Tillman/Hugger 2014), sondern auch datafizierte Kindheit (vgl. Lupton/Williamson 2017). Ob in der Schule oder im Kindergarten, in der Familie oder in der Freizeit: Kinder wachsen heute in zunehmend überwachten Umgebungen auf, in denen Daten über sie gesammelt, ausgewertet, Profile erstellt und damit Sichtweisen auf sie manifestiert werden, die ihre Zukunft über die Gegenwart hinaus betreffen (Stapf 2020).

Je differenzierter dabei die Techniken selbst, ihre Vernetzung untereinander, vor allem aber ihre kommerzielle Auswertbarkeit werden, desto stärker kann die Privatheit von Kindern über neue Formen der Datensammlung und Überwachung durch Unternehmen, Eltern und Staat, aber auch Schulen, bedroht werden. „Die Rechte von Kindern in digitalen Handlungswelten", so Stapf et al. (2020: 3), sollten in der Folge „stärker durchgesetzt und berücksichtigt werden. Dazu gehören explizit das Recht auf informationelle Selbstbestimmung, der Datenschutz, die freie Entfaltung der Persönlichkeit und ein geschützter Privatbereich."

Mit Blick auf Daten entstehen in diesen Kontexten asymmetrische Machtverhältnisse (Rieger 2013), die besonders für jüngere Kinder schwer einschätzbar sind: „The complexity of the current digital ecology makes it particularly hard, for children and adults alike to anticipate the long-term consequences of growing up in the digital age" (Stoilova et al. 2019: 4).

Ethisch bedeutsam sind diese Entwicklungen vor allem mit Blick auf demokratische Freiheitsrechte, welche individuelle Selbstbestimmung und subjektives Wohlergehen aktuell, aber auch nachhaltig ermöglichen sollen. Medien- und Informationsethik, verstanden mit Heesen (2016: 3), erfasst die Auseinandersetzung „mit der Bewertung und Steuerung individuellen, gesellschaftlichen und institutionellen Handelns für eine sozialver-

trägliche Gestaltung von Informations- und Kommunikationstechniken wie auch mit der Verantwortung des und der Einzelnen bei ihrer Entwicklung, Verbreitung und Anwendung." Gerade mit Blick auf Kindheit als besonders verletzliche Lebensphase lassen sich vielfältige Fragen nach der Verantwortung für die Fürsorge gegenüber Kindern, aber auch ihrer Befähigung und gar Beteiligung stellen.

Diese Aspekte markieren die Grundidee auch einer kinderrechtlichen Perspektive. Ausgehend vom Eingangsbeispiel wird diese, nun folgend, mit Blick auf ein *Kinderrecht auf Privatheit im Zeitalter des Digitalen* medienethisch untersucht.

2. *Was macht die Besonderheit von Kindheit mit Blick auf Privatheit aus?*

Das Eingangsbeispiel zeigt *erstens*, dass *Kinder anders in der Welt sind als die meisten Erwachsenen*. Kindheit ist eine verletzliche Entwicklungsphase, in der sich viele Fähigkeiten und Fertigkeiten erst noch ausbilden, in der Kinder abhängig von für sie Sorgetragenden sind; und auch noch nicht über die Vielfalt an Erfahrungen und Informationen verfügen, die es braucht, um selbstbestimmt entscheiden zu können (vgl. Stapf 2018, 2019a, 2020).

Diese besondere Verletzlichkeit von Kindern ist der Entwicklungsdimension geschuldet, indem Kindheit eine Phase biologischer – und damit psychischer, kognitiver und physischer – Entwicklung ist. Die kindliche Vulnerabilität gründet darin, dass Kinder sich hinsichtlich ihrer kognitiven Voraussetzungen von Erwachsenen unterscheiden, dass sie weniger Vorwissen und Erfahrungen zu bestimmten gesellschaftlichen Prozessen haben sowie, dass sie, auch in der Folge davon, eine für ihre Altersgruppe spezifische Herangehensweise an Medien pflegen (Stapf et al. 2020: 7).

Berücksichtigt man diese Entwicklungsprozesse im Kindheitsverlauf, so zeigt sich die Schwierigkeit, „allgemein" über „Kinder" zu sprechen, da es große Unterschiede nicht nur zwischen Entwicklungsphasen (wie der frühen Kindheit und der Adoleszenz), sondern auch geschlechtliche sowie individuelle Unterschiede gibt. So ist von sensiblen Phasen[3] im Kindheitsverlauf ebenso auszugehen wie von persönlichkeitsbezogenen Besonderheiten und genetische Anlagen. Hieraus folgt, dass zwar über *allgemeine* Aspekte

3 In der Entwicklungspsychologie werden sensible Perioden als „jene Entwicklungsabschnitte definiert, in denen spezifische Erfahrungen maximale Wirkung haben (= Perioden höchster Plastizität). Sensible Phasen sind Zeitabschnitte, in denen spezifische Lernerfahrungen maximale Wirkung zeigen, wobei viele sensible Phasen auch durch Stadien der Hirnreifung bedingt sind" (Stangl 2020).

von Kindheit gesprochen werden kann, dabei aber gleichzeitig ausreichend *differenziert* und eine Diversität von Kindheit(en) berücksichtigt werden sollte.

Abseits biologischer und entwicklungspsychologische Aspekte verweist der Kulturhistoriker Philippe Ariès (2003) darauf, dass der Begriff Kindheit historisch und sozial immer schon im Wandel war (vgl. Ammicht Quinn in diesem Band). Auch die neuere Kindheitsforschung (vgl. Prout/James 1997) versteht Kindheit als ein soziales und kulturelles Konstrukt, das *Erfahrungen von und Sichtweisen auf Kindheit immer auch erst (unterschiedlich)* herstellt. Kindheit ist damit einerseits eine biologische Entwicklungsphase und basiert andererseits auf einem kulturell fundierten sozialen Konstrukt, aus dem heraus Sichtweisen auf Kinder erfolgen. Diese kulturell variierenden Sichtweisen definieren dann auch, was an Kindheit „schützenswert" ist oder was eine gute und gelingende Kindheit ausmacht.

Entwicklungspsychologisch betrachtet haben Erfahrungen in der Kindheit teils langfristige Auswirkungen über die Kindheit hinaus ins Erwachsenenalter. Welche (auch problematischen) Erfahrungen Kinder machen und welche grundlegenden Informationen, Fürsorgeangebote und Bewältigungsstrategien ihnen zur Verfügung stehen, ist demnach mitentscheidend für die überhaupt *möglich werdende Zukunft von Kindern*, d. h. für ihre Handlungs- und Gestaltungsmöglichkeiten als Erwachsene. Aus diesem Spannungsfeld folgert der Philosoph Joel Feinberg (1980) das *Recht auf eine offene Zukunft*. Als sich noch entwickelnde Personen bilden Kinder demnach bestimmte Fähigkeiten und Erfahrungen erst noch aus. So implizieren die Grundfreiheiten für Kinder – anders als für Erwachsene – nicht nur die Abwesenheit externer Hindernisse (indem Kinder beispielsweise eine Schul*pflicht* haben); Einschränkungen in kindliche Freiheiten werden vielmehr dadurch gerechtfertigt, was sie eigentlich ermöglichen sollen – nämlich „the sense of being a person, meaning being responsible, having reasons, acting with intentions and purposes. We want a society that enhances the liberty of a person to develop (creatively) in the fullest sense possible" (ebd. 199).

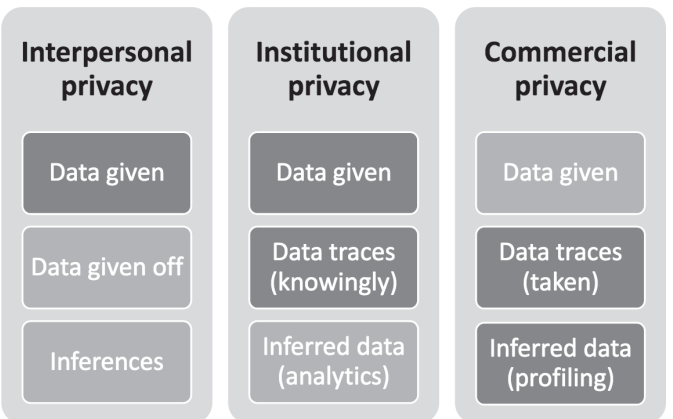
Um eine offene Zukunft zu gewährleisten, ist folglich schon *während der Kindheit* die Ermöglichung eigener, informierter Entscheidungen des Kindes zentral. Und da Autonomie auch ein oberstes Bildungsziel in Demokratien ist, sollten Kinder diese Entscheidungen möglichst selbstbestimmt treffen lernen.

Wird in der Ethik also vom „informed consent" gesprochen – dass erst dann autonome Entscheidungen getroffen werden können, wenn das dazu verfügbare Wissen und die relevanten Informationen vorliegen und in der Folge informiert eingewilligt werden kann –, dann gilt es zu berücksichti-

gen, dass eine informierte Einwilligung sich für Kinder anders gestaltet als für Erwachsene. Um eine informierte Einwilligung zu ermöglichen, müsste die Information kindgerecht erfolgen und es müssten Überlegungen vorausgehen, was (bei wem) vorausgesetzt werden kann und welche Unterstützung möglicherweise notwendig wird. Genau dies variiert im Entwicklungsverlauf, vor allem aber *von Kind zu Kind*: Was hierzu notwendig wird, hängt ab von kognitiven und emotionalen Fähigkeiten, situativen und kulturellen Kontexten, dem Bildungshintergrund der Familie sowie auch Persönlichkeitsfaktoren.

So unterscheiden sich nicht nur der Umgang von vier- und 14-jährigen mit Smart Toys, sondern möglicherweise auch das Wissen darum, was dabei an Daten erhoben wird und wie Privatsphäre-Einstellungen verändert werden können. Zudem unterscheidet sich, welche Rolle Privatheit überhaupt für die einzelne Person spielt oder spielen kann. Damit Fragen der Privatheit also überhaupt entscheidungsrelevant werden, brauchen Kinder für sie nachvollziehbare Informationen, um dann – soweit möglich und sinnvoll – selbst ihre Einwilligung geben zu können.

Abbildung 1: Kontexte der Privatheit (Livingstone et al. 2019: 16)



Eine aktuelle Studie von Sonia Livingstone zeigt, dass Kinder beim Thema Privatsphäre nur gering informiert sind und zunächst sehr stark vertrauen, da sie Privatheit primär als interpersonal verstehen (Stoilova/Livingstone/Nandagiri 2019: 3, 17, 24). Sie wollen bestimmte Informationen oder Bilder beispielsweise eher vor anderen Kindern oder den eigenen Eltern schützen als vor Firmen, die sie kommerziell auswerten. Selbst Unterneh-

men wie *Instagram* oder *Snapchat* verstehen Kinder in ihrer Wahrnehmung oft wie Personen:

> „[…] children give considerable thought to interpersonal privacy, although they may struggle with how to negotiate sharing or withholding personal information in networked contexts which demand they trade privacy for opportunities for participation, self-expression and belonging" (Livingstone in diesem Band).

In der Folge achten sie weniger stark auf institutionelle Kontexte wie ihre Schule oder gar auf kommerzielle Kontexte wie das Interesse globaler Firmen an ihren Daten. Die Preisgabe ihrer Daten erfolgt dabei hauptsächlich, wenn Kinder aktiv über Interaktionen auf ihren sozialen Medien Fotos, Daten oder andere Informationen mit anderen Nutzenden austauschen. Neben dem Risiko, „dass Gleichaltrige diese zum Beispiel für Cybermobbing-Angriffe nutzen (horizontale Privatheitsbedrohung), ist auch die passive Sammlung, Analyse und der Verkauf von Daten durch Unternehmen eine Gefahr, der sich Kinder und Jugendliche nicht vollständig bewusst sind (vertikale Privatheitsbedrohung)." (Stapf et al. 2020: 4)

Während Kinder also bei den verschiedensten Anwendungen, die digital konfiguriert sind, ständig Spuren hinterlassen, haben sie vor allem in der frühen Kindheit keine Vorstellung von ihrem „growing digital footprint" (Stoilova et al. 2019: 21). Genau dies wäre aber die Bedingung dafür, dass ihr Recht auf Privatheit eine Rolle auch mit Blick auf kindliche Selbstbestimmung spielen könnte.

3. Wie lassen sich Rechte von Kindern auf Privatheit umsetzen?

Das Eingangsbeispiel zeigt *zweitens*, dass Kinder moralische Gefühle und Bedürfnisse schon früh artikulieren (vgl. Eisenberg 1992) und durchaus – auch hier wieder entwicklungsabhängig – wissen, was sie fair und unfair, gerecht oder ungerecht finden. *Kinder wünschen sich, auch wenn sie es vielleicht noch nicht genau so benennen, Räume für sich, d.h. für ihre eigene Privatheit.* Obwohl sie selbst noch aushandeln, was Privatheit für sie bedeutet, belegt auch die Studie von Livingstone, dass „children care about their privacy online, and they want to be able to decide what information is shared and with whom" (Stoilova/Livingstone/Nandagiri 2019: 3). Grundlegende Fairness fordern Kinder auch über die Altersspannen hinweg von Unternehmen: „companies *should* explain better, improve services, be age-appropriate, provide options that users want, respond to users' concerns, and treat users well" (Livingstone in diesem Band).

Privatheit[4] fungiert allgemein als „Sammelbegriff für bestimmte zu schützende Positionen" und umfasst verschiedene Teilaspekte und auch Rechte, wie das Recht auf informationelle Selbstbestimmung, das Recht auf Schutz des Privaten und das Recht auf Datenschutz sowie das Persönlichkeitsrecht, das Post- und Fernmeldegeheimnis, die Unverletzlichkeit der Wohnung und das sogenannte IT-Grundrecht, das die Vertraulichkeit und Integrität informationstechnischer Systeme zum Schutzzweck hat (Stapf et al. 2020: 4). Privatheit hat unterschiedliche Bezugsdimensionen: Diese reichen von körperlichen Zonen, mentalen Vorgängen, über persönliche Entscheidungen, lokale Räume, den Schutz privater Daten bis hin zu institutionellen Bereichen, die sich zwar analytisch unterscheiden lassen, die aber – gerade bei Kindern – in der Praxis zutiefst ineinander verwoben sind; denn Privatheit tritt „relational innerhalb sozialer Konstellationen" auf (Ochs 2019: 15).

Gerade in „mediatisierten Welten" (Krotz/Hepp 2012) erleben Kinder interaktive Techniken aus ihrer konkreten Lebenswelt heraus. So titelte der Tagesspiegel im August 2019, dass viele Kinder *Siri* als ihre beste Freundin bezeichneten.[5] Dies verwundert nicht, da Kinder bei den wichtigsten Tätigkeiten das Thema Freundschaft an oberster Stelle nennen: 93 Prozent der sechs bis 13-jährigen Kinder interessieren sich, laut KIM-Studie (MPFS 2019a: 5), für das Thema Freunde und Freundschaft.[6] Es spielt für Kinder also eine zentrale Rolle bei der Nutzung digitaler Medien, es prägt aber auch ihre Wahrnehmung von digitalen Anwendungen. Denn fast alle Kinder haben in Deutschland aktuell Zugang zu Fernsehen, Internet und Smartphone (MPFS 2019a: 9).

---

4 Im vorliegenden Text wird vorwiegend der Begriff der Privatheit verwendet, der, anders als der eher „paternalistische Ansatz der Bestimmung eines schützenswerten Bereiches von außen („Privatsphäre")" durch staatliche Behörden, Justiz oder Rechtswissenschaften, die Selbstbestimmung des Einzelnen zum Maßstab erhebt (vgl. Stapf et al. 2020: 4, vgl. auch Geminn/Roßnagel 2015, Nebel 2015). Der Begriff Privatheit ist damit besser mit einem freiheitsorientierten Ansatz kompatibel. Der Begriff Privatsphäre wird im Text vor allem dann verwendet, wenn er sich auf diese Begriffsverwendung in bestimmten Dokumenten bezieht, z.B. der UN-Kinderrechtskonvention.

5 Quelle: https://www.tagesspiegel.de/wirtschaft/abhoererin-von-sprachassistent-viele-kinder-bezeichnen-siri-als-ihre-beste-freundin/24878764.html [Zugriff am 30.12.2019].

6 Gut zwei Drittel zeigen weiterhin Interesse an den Themen „Sport", „Handy/Smartphone" sowie „Schule". Gut drei von fünf Kindern begeistern sich für „Internet/Computer/Laptop", „Musik" und „Computer-/Konsolen-/Onlinespiele".

Digitale Technologien sind damit in unterschiedlichster Gestalt mit kindlichen Lebenswelten verwoben, vor allem indem sie eine wichtige Rolle für die kindliche Beziehungspflege spielen. Sie werden evident in der Kommunikation mit anderen Kindern, so bei vernetzten Computerspielen, der Nutzung von Social Media oder im Spiel mit Smart Toys. Sie strukturieren aber auch die kindliche Kommunikation mit Erwachsenen, ob in Familienchats oder in Bildungseinrichtungen. Und dass Kinder nicht mehr – wie nur eine Generation zuvor – zwischen „analogen" und „digitalen" Lebenswelten unterscheiden, wirkt sich auf die (schwieriger abschätzbaren und auch kontrollierbaren) Konsequenzen ihres Handelns aus, indem sie nämlich – anders als in klassisch analogen Handlungskontexten – vermehrt Datenspuren hinterlassen.

Um diese Fragen verhandeln zu können, bedarf es einer kinderrechtlichen Perspektive. Denn selbst bestimmen zu dürfen, welche Räume andere betreten oder welche Informationen sie einsehen oder verwenden dürfen, gilt nicht als ein „Luxusgut", sondern ein für Demokratien wesentliches Freiheitsrecht. Folgerichtig ist auch in Artikel 16 der UN-Kinderrechtskonvention (UN-KRK)[7] verbrieft, dass

> „kein Kind […] willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden" (darf).

Aus Sicht der Kinderrechte sind Fragen der Privatheit damit auf das *Wohlergehen* von Kindern ausgelegt und mit weiteren kindlichen Grundrechten, z.B. auf Bildung, Schutz und Partizipation, verknüpft. So bedarf ein umgesetztes Recht auf Privatheit Bildungsmaßnahmen darüber, wie diese gesteuert und definiert werden kann und da Kinder noch besonders verletzlich sind, folgt auch ein erhöhter Schutzbedarf. Und soll langfristig daraus ebenfalls Selbstschutz als autonomes Handeln erfolgen, ist Partizipation in all diesen Prozessen wesentlich. Die Förderung des Wohlergehens umfasst damit auch das Ziel, Kindern selbstbestimmtes Handeln, faire Chancen und wichtige Fähigkeiten für ihr Leben zu eröffnen. Hierzu versteht Art. 3 UN-KRK das Kindeswohl oder das beste Interesse (englisch „best interest") von Kindern als übergeordnet. Es wird als eine Art „Querschnittsrecht" gesetzt, das sich auf alle anderen Kinderrechte bezieht, und an dem sich alle auf das Kind bezogene Verfahren und Maßnahmen ausrichten sollen:

---

7 Online abrufbar unter: https://www.bmfsfj.de/blob/jump/93140/uebereinkommen-ueber-die-rechte-des-kindes-data.pdf [Zugriff: 30.3.2020].

> „Bei allen Maßnahmen, die Kinder betreffen, gleichviel ob sie von öffentlichen oder privaten Einrichtungen der sozialen Fürsorge, Gerichten, Verwaltungsbehörden oder Gesetzgebungsorganen getroffen werden, ist das *Wohl des Kindes* ein Gesichtspunkt, der vorrangig zu berücksichtigen ist."

Auch bei einem kinderrechtlichen Ansatz werden folglich immer schon Wertannahmen vorausgesetzt. Denn Kindheitsbilder prägen sowohl im Bildungsbereich als auch im Elternhaus oder in der Medienregulierung Vorstellungen darüber, was eine *gute Kindheit* ausmacht und was diese ermöglicht. Gesellschaftliche Vorstellungen von einer guten Kindheit nähren sich, so Fuhs (2004: 277), aus dem zugrunde liegenden Kindheitsbild sowie der „Gesamtheit aller gesellschaftlichen Bedingungen des Kinderalters." Und, laut Bühler-Niederberger (2011: 13 ff., 42) basiert das, was Kindern in Deutschland zugetraut und zugemutet werden dürfe, auf der Vorstellung einer langen und behüteten Kindheit, die den bewahrenden Schutzgedanken betont.

Aus kinderrechtlicher Sicht sind Kinder also nicht wie in vielen philosophischen Diskursen „noch-nicht-autonome" oder gar „Mängelwesen", denen zentrale Fähigkeiten fehlen, sondern agieren als *handelnde Subjekte*.[8] Kinder gelten folglich nicht nur als zukünftige Erwachsene, die einmal – nämlich mit 18 – autonom sein werden, sondern die bereits *als Kinder* Rechte haben und schon während ihrer Kindheit mit- und selbst bestimmen dürfen und damit nicht nur Objekt der Entscheidungen Sorgeberechtigter sind.[9] Der kinderrechtliche Rahmen strebt „children´s civil, political, protection, social economic and cultural rights" an: Diese sehen, so Third et al. (2019: 376), „children as active agents in the exercise of their rights" und leiten „the particular rights of children to ensure they develop to their full potential" daraus ab. Ähnlich betont Maywald (2012: 16), dass Kinderrechte weder „Erwachsenenrechte" noch „Sonderrechte" für Kinder sind, sondern dass Kinder einen „auf ihre spezielle Situation zugeschnittenen Menschenrechtsschutz benötigen". Dabei ist der Schutz ihrer Privat-

8 Für einen Überblick der philosophischen Diskussion um Kinderrechte vgl. Archard 2016, Stapf 2019a.

9 In der philosophischen Diskussion existieren verschiedene Modelle, die Kindern entweder gar keine oder nur teilweise Rechte zuschreiben. Insgesamt ist das Kindheitsbild dabei aber vermehrt auf Kindheit als Transitorium zum Erwachsenenstadium bezogen, wobei Erwachsenen per se Autonomierechte zugeschrieben werden und Kinder als nicht oder begrenzt autonomiefähig gelten (vgl. Stapf 2018, 2019, 2020).

sphäre als wesentlich zu verstehen. Oder: für diesen Menschenrechtsschutz ist der Schutz ihrer Privatsphäre wesentlich.

4. *Ist Privatheit ein Zustand oder Teil des Prozesses sich entwickelnder Autonomie?*

Ein Großteil der philosophischen Autonomietheorien versteht Individuen erst dann als autonomiefähig, wenn bestimmte Fähigkeiten (wie rationales Handeln, Abwägen und Urteilen) bereits vorliegen. Daran haben vor allem die feministische Ethik und die Care-Ethik (vgl. Conradi 2001) kritisiert, dass dies wichtige gesellschaftliche Gruppen per se von Autonomiefähigkeit ausschließen würde, wie beispielsweise Menschen mit starken Behinderungen oder eben auch Kinder. Problematisiert wird überdies, dass unter diesen Bedingungen auch viele Erwachsene nicht (immer) autonomiefähig wären.

Versteht man Individuen dagegen als „inherently social beings" (Friedman 2000: 217f.), die sich lebenslang in Entwicklungsprozessen befinden, dann entfaltet sich personale Autonomie im Zuge sich entwickelnder Fähigkeiten und im Rahmen von Beziehungen. Um sie auszubilden werden zur Verfügung stehende Informationen und Wahlmöglichkeiten, wachsende Erfahrungen zu verschiedenen Formen innerer und äußerer Autonomie sowie Einsicht in mögliche Konsequenzen des eigenen Handelns notwendig. Kinder als handelnde Subjekte wahrzunehmen, obwohl sie noch nicht über alle (voran kognitiven) Fähigkeiten verfügen, die Autonomiefähigkeit begründen, wird mit *relationalen Selbstbestimmungskonzepten* möglich.[10] Relationale Autonomiekonzepte (vgl. Mackenzie/Stoljar 2000) postulieren, dass sich Prozesse der Autonomieentwicklung im Rahmen von sozialen Beziehungen und in konkreten Kontexten ereignen. Privatheit kann also sowohl im Lebensverlauf als auch in verschiedenen Kontexten und Kulturen oder in verschiedenen Beziehungen ganz Unterschiedliches bedeuten.

10 Selbstbestimmung wird verstanden als ein *Selbstverhältnis*, ein *Weltverhältnis* oder als eine *interaktionistische Beziehung* (Seidel 2016). Nach internalistischen Theorien hängt Autonomie von internen Bedingungen wie mentalen Zuständen, dem geistigen Vermögen oder ausgebildeten Fähigkeiten ab. Konträr dazu sind für externalistische Theorien externe Bedingungen, wie Freiheit von Zwang, soziale Umstände oder Möglichkeiten relevant für personale Autonomie. Interaktionalistische Theorien verstehen Selbstbestimmung dagegen als ein Sich-in-Beziehung-Setzen, das in einem Zusammenspiel von Selbst- und Weltverhältnis möglich wird.

Als eine Art kontextuelle Integrität hängt sie auch von Beziehungen und Kontexten ab. Sie ist auf etwas und auf andere Personen bezogen, und damit nicht nur individuell zu verstehen (Solove 2015, Hargreaves 2017). Über die eigene Privatheit selbst bestimmen zu können impliziert damit die Möglichkeit, die eigene Privatheit auch bewusst einzuschränken, um andere Ziele zu erreichen oder Privatheit unter bestimmten Umständen gar nicht schützen zu wollen.[11]

Kindliches Handeln ist folglich auch Teil von sozialen Aushandlungsprozessen im Rahmen der eigenen Persönlichkeitsentwicklung, die sich im Verlauf des Lebens vollzieht. Als Persönlichkeit wird „das einem Menschen spezifische Gefüge von Merkmalen, Eigenschaften, Einstellungen und Handlungskompetenzen bezeichnet, das sich auf der Grundlage der biologischen Ausstattung und als Ergebnis der Bewältigung von Lebensaufgaben ergibt"; damit gilt Persönlichkeitsentwicklung auch als „die Veränderung wesentlicher Elemente dieses Gefüges im Verlauf des Lebens" (Bründel/Hurrelmann 2017: 16).

Ein Kind muss also nicht schon über alle Fähigkeiten verfügen, um selbstbestimmt zu handeln. Ganz im Gegenteil braucht es zur Ausbildung dieser Fähigkeiten entsprechende Erfahrungen. So zeigt das Eingangsbeispiel *drittens*, dass Kinder in ihren konkreten Lebenswelten schon weitgehend *selbst*bestimmt handeln. Das Mädchen hat mit der Puppe gespielt, *ohne* dass sie wusste, dass ihre Gespräche gespeichert werden. Sie hat ihre Daten nicht fahrlässig aus der Hand gegeben, sondern es geschah, weil es ihr nicht transparent war, was in diesem Fall der Unterschied zwischen einer Puppe mit und ohne Informationstechnik war. Noch jüngere Kinder dagegen wären vielleicht noch nicht in der Lage, eine Folgenabschätzung zu leisten, selbst wenn sie wüssten, dass die Daten abgehört werden können. Das Gleiche könnte aber auch auf technisch nicht sehr kompetente oder daran nicht interessierte Erwachsene zutreffen.

---

11 Das Phänomen scheinbar widersprüchlichen Verhaltens durch die freiwillige Aufgabe von Privatheit wird in der Forschung als „privacy paradox" (Barnes 2006, Norberg/Horne/Horne 2007) bezeichnet und kritisch diskutiert (Baruh/Secinti/Cemalcilar 2017). Vermutet wird, dass Kinder im Internet einerseits freiwillig persönliche Informationen online teilen und dabei Risiken für ihre Sicherheit und ihre Privatheit in Kauf nehmen, obwohl sie andererseits ihre Privatheit schützen wollen. Der Widerspruch besteht mit Blick auf soziale Kontexte allerdings eigentlich darin, dass soziale Teilhabe nur bei Aufgabe herkömmlicher Privatheitsvorstellungen möglich wird. Kinder müssten hierbei, wie Erwachsene auch, eine wirkliche Wahl haben (White Paper Kinderrechte und Privatheit vgl. Stapf et al. 2020: 5).

Die Frage ist also nicht, *ob* Kinder *ein Recht auf Privatheit* im Digitalen haben, sondern, *wie ihnen Bedingungen geschaffen werden können*, durch die sie ihre Privatheit erleben und erfahren können. Und wie sie ihre Privatheit *selbst* bestimmen und regulieren lernen können. Dies erfordert aus kinderrechtlicher Sicht aber geradezu, dass Kinder *nicht nur als handelnde Subjekte gesehen, sondern auch als solche behandelt* werden.

Blickt man auf Beispiele des *Sharenting*, wenn Eltern teils intime Fotos ihrer noch Ungeborenen oder ihrer Babys auf sozialen Netzwerken posten, so zeigt sich, dass vor allem jüngere Kinder oft als „Extension des Selbst" wahrgenommen werden und weniger als Subjekte oder gar Rechteträger. Phänomene des elterlichen *Sharenting* als „habitual use of social media to share news, images, etc. of one´s children"[12] und *Oversharenting*, wenn dies exzessiv geschieht, verdeutlichen, dass es mit Blick auf Selbstbestimmungsrechte von Kindern offensichtliche Widersprüche gibt (Stapf 2018): So wird die Social-Media-Nutzung von *WhatsApp* von Kindern durch Eltern begrenzt und ist rechtlich zum Schutz der Kinder gar auf das Alter von 16 Jahren angehoben worden,[13] während

> „parents share information about their children online, they do so without their children´s consent. These parents act as both gatekeepers of their children´s personal information and as narrators of their children´s personal stories [...]. A conflict of interests exists as children might one day resent the disclosures made years earlier by their parents." (Steinberg 2017: 839)

Spy-Apps von Eltern oder andere digitale Tools zum Überwachen kindlicher Aktivitäten in der Schule können zwar dem Schutz des Kindes dienen und folgen auch aus dem verbrieften Kinderrecht (Art. 5 UN-KRK) zur elterlichen Fürsorgepflicht: Diese steht im Zusammenspiel – und oft im Konflikt – mit kindlichen Rechten, soll dabei aber ermöglichen, „das Kind bei der Ausübung der in diesem Übereinkommen anerkannten Rechte in einer seiner Entwicklung entsprechenden Weise angemessen zu leiten und zu führen." Werden elterliche Fürsorgepflichten vom Kind her gedacht, dann folgen aus der Frage nach Privatheit andere, kritische Nachfragen. Dann lässt sich beispielsweise hinterfragen, ob Maßnahmen, wie Spy-Apps,

12 vgl. Collins Dictionary „Sharenting", online unter: https://www.collinsdictionary.com/dictionary/english/sharenting [Zugriff: 1.4.2020].

13 So war das Mindestalter von 13 Jahren auf 16 Jahre angehoben worden und wird im Zuge der neuen Datenschutz-Grundverordnung jetzt auch von Kindern abgefragt (vgl. https://www.faz.net/aktuell/wirtschaft/unternehmen/whatsapp-setzt-mindestalter-auf-16-jahre-herauf-15558790.html [Zugriff: 17.12.2019]).

dazu führen können, dass Kinder sich als *verantwortliche Subjekte* erfahren und *sich selbst schützen* lernen oder ob Kinder diese Maßnahmen eher als Überwachung erleben, denen sie passiv ausgeliefert sind.

5. Was macht den Wert der Privatheit für Kinder aus?

An dem Eingangsbeispiel zeigt sich *viertens*, warum Privatheit in freiheitlichen Demokratien überhaupt so einen hohen Wert hat und mit grundlegenden demokratischen Freiheitsrechten verknüpft ist. Privacy umfasst, so Westin (1967), die individuelle Kontrolle über Informationen, die wissentlich gegeben oder mit anderen geteilt werden. Sie gilt, nach Nissenbaum (2010: 3), als „a right to appropriate flow of personal information".

Privatheit wird generell Erwachsenen zugeschrieben, bei Kindern treten dagegen grundlegende Fragen zutage: Haben beispielsweise schon Neugeborene, die noch gewickelt werden, ein Recht auf eine Privatsphäre? Wie können wir Personen eine Privatsphäre zuerkennen, die sie selbst noch nicht als solche wahrnehmen, artikulieren oder gar einfordern können? Wie bereits beschrieben gibt es zu diesem moralischen Problem unterschiedliche ethische Positionen, die sich auf unterschiedliche Autonomiekonzepte beziehen. Aus einer menschenrechtlichen Perspektive heraus, die hier eingenommen wird, erscheint es schwierig, Bedingungen daran zu knüpfen, welche Fähigkeiten jeweils schon *vorliegen* müssen, damit einer Person grundlegende Rechte zugeschrieben werden oder diese selbst bestimmen oder mitbestimmen darf. Unteilbare, unkündbare und universelle Menschenrechte sind, so *Bielefeld* (2008), vielmehr „inklusiv" zu denken.

Denn die Idee der Menschenrechte basiert auf dem Prinzip der Menschenwürde, die *allen* Menschen zukommt: Das altersübergreifende Gleichheitsprinzips (Art. 1 der Allgemeinen Erklärung der Menschenrechte; Art. 3 GG) impliziert, dass *Kinder* einen *eigenen moralischen Status* haben, der nicht Ableger des Status anderer, voran der Eltern, ist (vgl. Schickhardt 2012). Kinder haben also das fundamentale Recht, *als Gleiche behandelt* zu werden.

Versteht man Kinderrechte als „Menschenrechte für Kinder" (Maywald 2012), dann gilt es aber gleichermaßen, wesentliche *Differenzen* zwischen Kindern und Erwachsenen zu berücksichtigen, d.h. dass Kinder eben noch *in der Entwicklung* sind. Autonomie ist für das Aufwachsen ein wichtiger Zielbegriff, da Autonomie aus menschenrechtlicher Sicht überhaupt erst die Grundlage für moralische Verantwortungsübernahme, staatsbürgerliche Partizipation in Demokratien, die Grundlage weiterer Menschenrechte, aber auch für ein individuelles gelingendes Leben ist.

Autonomieentwicklung verstanden als ein *interaktiver Prozess*, der im Zuge der „evolving capacities" (Lansdown 2005) lebenslang wächst, erfordert damit, schon kleinsten Kindern ein Recht auf Privatsphäre zuzusprechen, auch wenn diese den Wunsch danach selbst noch nicht artikulieren können. Vielmehr rückt dann die Frage in den Vordergrund, was es *braucht*, damit Kinder ihre Selbstbestimmung *entfalten* und entfalten *lernen* können: Welche Prozesse und Interaktionen, welche Formen der Befähigung, des Schutzes, aber auch der Partizipation ermöglichen es Kindern, Privatheit zu erleben, sie einzufordern, für wichtig zu halten und sie selbst zu gestalten? Viele Eltern und Erziehende verfügen hier selbst nicht über alle Kompetenzen, um Kinder optimal zu begleiten. Kinder haben ihren Eltern gegenüber sogar oft Wissens- und Erfahrungsvorsprünge:

> „Children are often pioneers in exploring and experimenting with new digital technologies and services […]. Increasingly independent users of digital technologies and starting at a much younger age, children experience newly emerging risks often before adults know about their existence or are able to put mitigating strategies in place. In the contemporary digital environment, children's actions are particularly consequential as technologies transform their lives into data which can be recorded, tracked, aggregated, analysed and monetised – and which is durable, searchable and virtually undeletable." (Stoilova et al. 2019: 4)

Je jünger Kinder sind, desto verletzlicher können sie dabei noch sein. Selbst wenn sie Medien zwar schon (d.h. im deskriptiven Sinne) selbstbestimmt nutzen können, fehlen ihnen noch weitreichende Erfahrungen über mögliche Folgen ihres Handelns sowie Entscheidungskriterien, die sie moralisch gesehen (d.h. im normativen Sinne) leiten können. Beispielsweise zeigen Studien wie die von Livingstone et al. (2019), dass Kinder unter 11 Jahren in ihrer Entwicklung meist nicht weit genug vorangeschritten sind, um Konzepte wie „Privatheit" vollumfänglich zu begreifen:

> „Vor dem Hintergrund ihrer noch nicht vollständig abgeschlossenen Entwicklung sind Kinder und Jugendliche somit auch besonders anfällig für Online-Dienste, die auf kurzfristige Erfolgserlebnisse, Belohnungsanreize und soziale Honorierung setzen und im Gegenzug Datenprofile der Nutzenden sammeln" (Stapf et al. 2020: 7).

Privatheit ist folglich kein erreichbarer Zustand, sondern vielmehr *relational* zu verstehen (vgl. Livingstone et al. 2019). Sie ist bezogen auf den aktuellen Entwicklungsstand und die individuelle Persönlichkeit ebenso wie auf Beziehungen, Kontexte und Situationen. Gerade kindliche Praktiken hängen stark von der sozialen Umgebung ab. Somit geht es beim Schutz

der Privatheit zwar systemisch um eine Ökologie der Daten im Netz, aber in sozialen Kontexten und der Lebenswelt geht es auch um eine *gelebte Kultur der Privatsphäre* (Livingstone 2019 et al., Stapf 2019b). Damit ist der Wert der Privatheit für Kinder der *gleiche* Wert wie für Erwachsene, er ist aber stärker im Entwicklungsgeschehen der besonders verletzlichen Lebensphase Kindheit zu denken.

Die UN-Kinderrechtskonvention von 1989 artikuliert in 54 Artikeln *kindereigene Rechte*, die auf den vier Prinzipien Recht auf Gleichbehandlung, Vorrang des Kindeswohls, Recht auf Leben und Entwicklung und Achtung vor der Meinung des Kindes beruhen (Maywald 2012: 96). Die drei Säulen der Kinderrechte verbinden *Schutz-* (protection), *Versorgungs-* (provision) sowie *Beteiligungsrechte* (participation), die als eine Einheit zu verstehen sind, dem das *beste Interesse von Kindern* übergeordnet ist. Hierzu wird es notwendig, die Sichtweise und die *Perspektive von Kindern* auf das, was sie betrifft, angemessen einzubeziehen.[14] Genau das wäre als zentraler Bestandteil einer gelebten Kultur der Privatsphäre zu verstehen und folgt wesentlich aus der Entwicklungsdimension von Kindheit.

So mag das Kind im Eingangsbeispiel erlebt haben, dass es unangenehm ist, wenn man nicht weiß, *wer* die eigenen Geheimnisse anhören kann. Sie konnte es der Puppe nicht ansehen, wer alles auf die Daten Zugriff hat. Die Idee eines Geheimnisses, dass es – wenn überhaupt – nur ausgewählte Personen wie die beste Freundin, die ältere Schwester, oder eben nur die Puppe, mit der man eine besondere Beziehung hat, erfahren dürfen, ließ sich in diesem Fall nicht auf ein Smart Toy übertragen. Dabei spielt auch eine Rolle, dass das Mädchen diese Situation nicht vollumfänglich erkennen oder von der Puppe oder gar den Spieleherstellern fordern konnte, dass das Geheimnis geheim bleibt. Allerdings folgt daraus nicht, dass das Mädchen aufgrund dieser fehlenden Fähigkeiten oder Optionen kein Recht auf Privatheit hätte. Vielmehr sollte Privatheit für sie – auch als Kind – greifbarer werden, indem sie ein „lebendiges" Menschenrecht wird, das beispielsweise im Design voreingestellt ist und somit eine wirklich wählbare Option wird. Solange Kinder noch besonders verletzlich sind,

14 Der unbestimmte Rechtsbegriff des „Kindeswohls" („wellbeing of the child", „best interests of the child") vereint *subjektive* Aspekte des Willens und der Befindlichkeit des Kindes sowie *objektive* kindliche Interessen. Das Kindeswohl soll subjektiv gesichert werden, indem die *Sichtweise des Kindes als Betroffener* in Entscheidungsprozessen, das heißt, die *Kinderperspektive*, angemessen berücksichtigt wird. Und es soll objektiv gefördert werden, indem gesellschaftlich definiert wird, was ein gelingendes Leben für Kinder ausmacht, das heißt, welche Bedingungen, Möglichkeiten und Kompetenzen dafür wesentlich sind.

sollte Privatheit folglich bei digitalen Anwendungen vorkonfiguriert sein (i.S. von privacy-by-design).

6. *Was folgt für das Recht von Kindern auf Privatheit im Digitalen?*

Ein ethisches Kernproblem des Themas ist die *Objektivierung* der Nutzenden, die *Unsichtbarkeit* der Verknüpfung von Daten und deren Auswertung, sowie eine neuartige Form der *Nachhaltigkeit* von Datenspuren. Spuren, die Kinder im Netz hinterlassen, sind, metaphorisch gesprochen, nicht im Sand markiert, sondern in Beton gegossen (vgl. Stapf 2019b). Sie können spätere Optionen verhindern, wenn Unternehmen vor dem Vorstellungsgespräch Facebook-Einträge in Alkoholfeste in der Jugend einsehen können. Sie können zu Scham und Ohnmacht führen, wenn Kinder Cybermobbing erfahren. Oder sie können über die Erstellung von Dossiers oder das längerfristige Tracking von Kindern ihr Recht auf eine offene Zukunft einschränken.

Datenspuren können aber auch individuell auf Bedürfnisse von Kindern einwirken und auf ihre besonderen Interessen oder Fähigkeiten zugeschnitten werden, wie individualisierte Lernsoftware bei Kindern mit besonderen Fähigkeiten, Einschränkungen oder gar Behinderungen. Wesentlich wird also, was auch *positiv* erreicht und ermöglicht werden soll und wie dies gelingen kann. Und das heißt zu reflektieren, wie aus Herausforderungen möglichst Chancen werden.

Für Kinder geht es in erster Linie um Tätigkeiten und Interessen. Aber ebenso auch um Neugier, Langeweile, Trial & Error oder Lust auf Unterhaltung und Spiel – auch das *Recht auf Freizeit und Spiel* (Art. 31 UN-KRK) ist ein verbrieftes Kinderrecht. Was Chancen für ein gelingendes Leben, Aufwachsen und eine offene Zukunft ausmacht, hat folglich mit allgemein geteilten Vorstellungen von Wohlergehen ebenso zu tun wie mit subjektiven Besonderheiten. Entscheidend aus kinderrechtlicher Sicht ist die Wahrnehmung der Perspektive der Kinder selbst, die es zu berücksichtigen und die es auch sinnvoll einzubeziehen gilt. Und dazu ist es wesentlich, dass das *Kinderrecht auf Privatsphäre auch im Digitalen gilt.*

Mit Blick auf das Beispiel werden abschließend ein paar Forderungen aufgestellt[15]:

1. Die Privatsphäre von Kindern ist auch in digitalen Kontexten ein verbrieftes Kinderrecht. Die Kinderrechtskonvention ist seit 1992 ratifiziert und in einfaches Recht umzusetzen. Im Zuge der aktuellen Diskussion einer Aufnahme von Kinderrechten ins Grundgesetz hätte dies Auswirkungen auf unterschiedliche Lebensbereiche. Es sollte daher in digitalen Kontexten ausbuchstabiert werden, um die informationelle Selbstbestimmung schon von Kindern zu ermöglichen, wobei die besondere Verletzlichkeit von Kindern auch einen besonderen Schutz von Kindern begründet.
2. Mit der Sicherung kindlicher Privatsphäre ist das Recht des Kindes auf eine offene Zukunft verbunden. Aus Sicht der Kinderrechte sind Fragen der Privatsphäre auf das Wohlergehen von Kindern ausgelegt. Es geht darum, Kindern eine gelingende Kindheit und gute Chancen und wichtige Fähigkeiten mit Blick auf ihr Erwachsenenleben zu eröffnen. Dazu gehört das Recht auf eine offene Zukunft. Dies impliziert Sorgfalt im Umgang mit kindlichen Daten, das Recht auf Vergessen im Netz sowie auf Datensparsamkeit mit Blick auf Datenspuren, die Kinder im Netz hinterlassen.
3. Da Kinder noch in der Entwicklung sind und Fähigkeiten noch ausbilden, sollten Maßnahmen zum Schutz von Kindern immer auch Befähigungsmaßnahmen implizieren. Sowohl Schule als auch Eltern sollten Medienerziehung und Medienbildung vorantreiben, indem Kinder über ihre Rechte informiert werden und verschiedene Formen von Privatsphäre in digitalen Kontexten kennen und selbst regulieren lernen. Der *DigitalPakt Schule* der Bundesregierung[16] sollte neben Geräten und Infrastrukturen die digitalen Kompetenzen von Lernenden wie Lehrenden in Bildungskontexten fördern mit dem Ziel, dass Kinder selbst informierte Entscheidungen treffen lernen können.
4. Anreizsysteme für Datenschutz by Design & Default durch Unternehmen, Plattformbetreibern und Bildungseinrichtungen sollten gefördert werden. Privatheit im Digitalen sollte immer eine Möglichkeit sein und nicht erst aktiv eingestellt werden müssen. Es muss für Kinder selbst wählbar sein, in welchem Grad von Öffentlichkeit sie sich jeweils

15 Vertiefend hierzu vgl. White Paper Kinderrechte und Privatheit (Stapf et al. 2020: 16ff.).

16 Vgl. https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/digitalpakt-schule-1546598 [Zugriff: 25.7.2020].

befinden wollen. Und dies muss einfach im Design erkennbar sein, z.B. über auditive Ansagen oder visuelle Gestaltung („Wenn Du das abschickst, können es alle Menschen sehen, die das gleiche Angebot nutzen"). Die Privatsphäre von Kindern wird schon in der Konzeption von Angeboten, Software und Nutzungsmöglichkeiten vorkonfiguriert. Anbieter sollten in der Entwicklung, im Design und bei der Umsetzung von Angeboten Anreizsysteme hin zu „privacy-by-design" vorfinden. Sie sollten verpflichten werden, grundlegende Standards einzuhalten.

5. Privatsphäre ist ein die Demokratie sicherndes Menschenrecht. Hierzu bedarf es angesichts der rasanten technischen Entwicklung gesamtgesellschaftlicher, interdisziplinärer und kontextsensibler Ansätze. Die Möglichkeit zu entscheiden, welche Informationen in bestimmten Kontexten oder mit bestimmten Personen geteilt werden und welche nicht, ist grundlegend für personale Autonomie und damit ein Kernthema freiheitlicher Demokratien. Zu verstehen wie Heranwachsende Privatsphäre heute im Digitalen erleben und wie sich dies im Altersverlauf entwickelt, ist eine Forschungsaufgabe. Hierzu braucht es interdisziplinäre Langzeitstudien – auch unter Beteiligung von Heranwachsenden – innovative technische Ansätze, gesellschaftliche Diskurse und einen flexiblen Kinder- und Jugendmedienschutz.

Das Eingangsbeispiel hat aufgezeigt, wie verwoben das Netz an Herausforderungen mit Blick auf die Privatheit und den Datenschutz von Kindern im Digitalen sein kann. Dabei gilt es aus ethischer Sicht immer zu differenzieren: *Kindheit* ist weder eine einheitliche homogene Lebensphase, wie auch *digitale Medien* nicht gleichförmig sind. Zweijährige lassen sich mit 17-Jährigen ebenso wenig vergleichen wie Erklärvideos der NASA mit der Smart Barbie.

Was aber dringend gesellschaftlich diskutiert werden sollte, ist, was es jeweils braucht, damit sich Potenziale entfalten und Herausforderungen mit Blick auf die Privatheit von Kindern im Digitalen minimiert werden können. Denn es geht darum, dass möglichst viele Kinder frei und verantwortlich, aber auch mit Freude selbstbestimmt handeln lernen.

Literatur

Ariès, Philippe (2003): *Geschichte der Kindheit*. München: dtv.

Archard, David W. (2016): Children's Rights. In: *The Stanford Encyclopedia of Philosophy.* In: Zalta, E. N. (Hg.). Online unter: https://plato.stanford.edu/archives/sum2016/entries/rights-children/ [Zugriff: 1.4.2020].

Barnes, Susan B. (2006): *A privacy paradox: Social networking in the United States*. In: First Monday, 11(9). https://doi.org/10.5210/fm.v11i9.1394.

Baruh, Lemi / Secinti, Ekin / Cemalcilar, Zeynep (2017): *Online privacy concerns and privacy management: A meta-analytical review*. In: Journal of Communication, 67(1), S. 26-53.

Bielefeldt, Heiner (2008): *Menschenwürde. Der Grund der Menschenrechte*. Berlin: Deutsches Institut für Menschenrechte. Online unter: https://www.ssoar.info/ssoar/handle/document/31608.

Brown, Duncan H. / Pecora, Norma (2014): *Online Data Privacy as a Children´s Media Right: Toward Global Policy Principles.* In: Journal of Children and Media, vol. 8, no. 2, S. 201-207.

Bründel, Heidrun / Hurrelmann, Klaus (2017): *Kindheit heute. Lebenswelten der jungen Generation.* Weinheim/Basel: Beltz.

Bühler-Niederberger, Doris (2011): *Lebensphase Kindheit: Theoretische Ansätze, Akteure und Handlungsräume*. Weinheim: Beltz.

Conradi, Elisabeth (2001): *Take Care. Grundlagen einer Ethik der Achtsamkeit*. Frankfurt a. M.: Campus.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (2018): DIVSI U-25-Studie. *Euphorie war gestern. Die „Generation Internet" zwischen Glück und Abhängigkeit.* Hamburg.

Eisenberg, Nancy (1992): *The Caring Child*. Cambridge: Harvard University Press.

Feinberg, Joel (1980): *A Child´s Right to an Open Future.* In: Aiken, W. / LaFollette, H. (Hg.), Whose Child? Parental Rights, Parental Authority and State Power. Totowa, NJ: Littlefield, Adams & Co., S. 124-153.

Friedman, Marilyn (2000): *Feminism in Ethics: Conceptions of Autonomy.* In: The Cambridge Companion to Feminism in Philosophy, Cambridge: Cambridge University Press, S. 205–219.

Fuhs, Burkhard (2004): *Kindheit*. In: Krüger, H.-H. / Grunert, C. (Hg.): Wörterbuch Erziehungswissenschaft. Wiesbaden, S. 274-280.

Geminn, Christian / Roßnagel, Alexander (2015): *„Privatheit" und, „Privatsphäre" aus der Perspektive des Rechts – ein Überblick*. In: JuristenZeitung, 70(14); S. 703-708.

Hargreaves, Stuart (2017): *Relational privacy and tort.* In: William and Mary Journal of Women and the Law 23(3), S. 433-476.

Heesen, Jessica (2016): *Handbuch Medien- und Informationsethik*. Stuttgart: Metzler.

Krotz, Friedrich / Despotović, Cathrin / Kruse, Merle-Marie (Hg.) (2014): *Die Mediatisierung sozialer Welten. Synergien empirischer Forschung.* Wiesbaden: VS Springer.

Krotz, Friedrich / Hepp, Andreas (2012): *Mediatisierte Welten. Forschungsfelder und Beschreibungsansätze*. Wiesbaden: VS Springer.

Krotz, Friedrich (2001): *Die Mediatisierung kommunikativen Handels. Der Wandel von Alltag und sozialen Beziehungen, Kultur und Gesellschaft durch die Medien*. Wiesbaden: Westdeutscher Verlag.

Lansdown, Gerison (2005): *The Evolving Capacities of the Child*. Florenz: UNICEF.

Livingstone, Sonia / Stoilova, Mariya / Nandagiri, Rishita (2019): *Children's data and privacy online: Growing up in a digital age. An evidence review.* London: London School of Economics and Political Science.

Livingstone, Sonia / Carr, John / Byrne, Jasmina (2016*): One in Three: Internet Governance and Children´s Rights*. Florenz: UNICEF Innocenti.

Lupton, Deborah / Williamson, Ben (2017): *The datafied child: the dataveillance of children and implications for their rights.* In: New Media & Society 19(5), S. 780-794.

Mackenzie, Catriona / Stoljar, Natalie (2000): *Relational autonomy: feminist perspectives on autonomy, agency, and the social self*. New York: Oxford University Press.

Maywald, Jörg (2012): *Kinder haben Rechte! Kinderrechte kennen – umsetzen – wahren*. Weinheim/Basel: Beltz/Juventa.

Medienpädagogischer Forschungsverbund Südwest (MPFS) (2019a): *KIM 2018. Kindheit – Internet – Medien. Basisuntersuchung zum Medienumgang 6-13-Jähriger in Deutschland*. Stuttgart.

Medienpädagogischer Forschungsverbund Südwest (MPFS) (2019b): *JIM 2019. Jugend – Information – Medien. Basisuntersuchung zum Medienumgang 12-19-Jähriger in Deutschland*. Stuttgart.

Nebel, Maxi (2015): *Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung. Verfas- sungsrechtliche Zielsetzungen im deutschen und europäischen Recht.* Zeitschrift für Datenschutz, S. 517-522.

Nissenbaum, Helen (2010): *Privacy in Context. Technology, Policy, and the Integrity of Social Life.* Stanford: Stanford University Press.

Norberg, Patricia A./Horne, David/Horne, Dan (2007): *The privacy paradox: Personal information disclosure intentions versus behaviors*. Journal of consumer affairs, 41(1), S. 100-126.

Ochs, Carsten (2019): *Teilnahmebeschränkungen und Erfahrungsspielräume: Eine negative Akteur-Netzwerk-Theorie der Privatheit.* In: Behrendt, H. / Loh, W. / Matzner, T. / Misselhorn, C. (Hg.): Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter des Digitalen. Berlin: Metzler, S. 13-31.

Prout, Alan / James, Allison (1997): *A New Paradigm for the Sociology of Childhood?* Provenance, Promise and Problems. In: James, A. / Prout, A. (Hg.), Constructing and Reconstructing Childhood. London: Falmer Press, S. 7–34.

Rieger, Frank (2013): *Von Daten und Macht.* In: Aus Politik und Zeitgeschehen. 63. Jahrgang; 15-16-2013; S. 3-7: Online verfügbar unter: https://www.bpb.de/apuz/157536/transparenz-und-privatsphaere [Zugriff: 1.4.2020].

Schickhardt, Christoph (2012): *Kinderethik. Der moralische Status und die Rechte der Kinder*. Münster: Mentis.

Seidel, Christian (2016): *Selbst bestimmen: Eine philosophische Untersuchung personaler Autonomie*. Berlin: De Gruyter.

Solove, Daniel J. (2015): *The meaning and value of privacy*. In: Roessler, B. / Mokrosinska, D. (Hg.). Social dimensions of privacy: interdisciplinary perspectives. Cambridge: Cambridge University Press.

Stangl, Werner (2020): Stichwort: '*sensible Perioden'.* In: Online Lexikon für Psychologie und Pädagogik. Online verfügbar unter: https://lexikon.stangl.eu/1523/sensible-perioden-phasen/ [Zugriff: 26.5.2020].

Stapf, Ingrid / Prinzing, Marlis / Köberer, Nina (Hg.) (2019): *Aufwachsen mit Medien. Zur Ethik mediatisierter Kindheit und Jugend.* Baden-Baden: Nomos.

Stapf, Ingrid / Judith Meinert / Jessica Heesen / Nicole Krämer / Regina Ammicht Quinn / Felix Bieker / Michael Friedewald / Christian Geminn / Nicholas Martin / Maxi Nebel / Carsten Ochs (2020): *Privatheit und Kinderrechte, White Paper Forum Privatheit.* Schriftenreihe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Creative Commons 2020. Online verfügbar unter: https://www.forum-privatheit.de/publikationen/white-paper-policy-paper/.

Stapf, Ingrid (2020): *Kindliche Selbstbestimmung in digitalen Kontexten – medienethische Überlegungen zur Privatsphäre von Heranwachsenden.* In: Buck, F. / Drerup, J. / Schweiger, G. (Hg.): Neue Technologien – neue Kindheiten? Ethische und bildungsphilosophische Perspektiven. Stuttgart: J.B. Metzler, S. 31–54.

Stapf, Ingrid (2019a): *Zwischen Selbstbestimmung, Fürsorge und Befähigung. Kinderrechte im Zeitalter mediatisierten Heranwachsens*. In: Stapf, I. / Prinzing, M. / Köberer, N. (Hg.): Aufwachsen mit Medien. Zur Ethik mediatisierter Kindheit und Jugend. Nomos, 2019, S. 69-84.

Stapf, Ingrid (2019b): „*Ich sehe was, was Du auch siehst.*" *Wie wir die Privatsphäre von Kindern im Netz neu denken sollten und was Kinder möglicherweise dabei stärkt – ein kinderrechtlicher Impuls.* In: frühe Kindheit 2-19, S. 12-25.

Stapf, Ingrid (2018): *Kindliche Selbstbestimmung in der digital vernetzten Welt: Kinderrechte zwischen Schutz, Befähigung und Partizipation mit Blick auf „evolving capacities"*. In: merzWissenschaft Kinder|Medien|Rechte – Komplexe Anforderungen an Zugang, Schutz und Teilhabe im Medienalltag Heranwachsender. München: kopaed, S. 7-18.

Steinberg, Stacey (2017): *Sharenting: Children's Privacy in the Age of Social Media* (March 8, 2016). 66 Emory Law Journal 839. University of Florida Levin College of Law Research Paper No. 16-41.

Stoilova, Mariya / Livingstone, Sonia / Nandagiri, Rishita (2019): *Children's data and privacy online: Growing up in a digital age. Research findings.* London: London School of Economics and Political Science.

Third, Amanda / Livingstone, Sonia / Lansdown, Gerison (2019): *Recognizing children's rights in relation to digital technologies: Challenges of voice and evidence, principle and practice*. In: Wagner, B. / Kettermann, M. C. / Vieth, K. (Hg.): Research Handbook of Human Rights and Digital Technology. Cheltenham, UK & Northhampton MA, USA: Edward Elgar, S. 376-410.

Tillmann, Angela / Hugger, Kai-Uwe (2014*): Mediatisierte Kindheit – Aufwachsen in mediatisierten Lebenswelten*. In: Friedrichs, H. / Junge, T. / Sander, U. (Hg.): Jugendmedienschutz in Deutschland. Wiesbaden: VS Verlag-Verlag, S. 31-45.

Westin, Alan F. (1967): *Privacy and Freedom.* New York: Atheneum.

Teil II –
Aufwachsen in überwachten Umgebungen: Privatheit in Kita, Schule und Familie

Das ist Privatsache! Zwischen Schutzbedarf und Freiheitswunsch: Aufwachsen im digitalen Umfeld

Jutta Croll und Elena Frense

Abstract

Kinder wachsen heute in einer von (digitalen) Medien geprägten Lebenswelt auf. Die von Erwachsenen vorgenommene Differenzierung von analoger und digitaler Welt ist für sie keine relevante Trennlinie mehr. Insbesondere die Gewährleistung von Datenschutz und Privatsphäre wird im Spannungsfeld von Schutz- und Freiheitsrechten vor Herausforderungen gestellt. Unter Bezugnahme auf die UN-Kinderrechtskonvention analysiert der Beitrag die Regelungen der europäischen Datenschutz-Grundverordnung und deren Umsetzung im Hinblick auf den Vorrang des Kindeswohls gem. Art. 3 UN-KRK; er zeigt wie das Kinderrecht auf Beteiligung an Maßnahmen des Jugend- und Datenschutzes in der Praxis umgesetzt werden kann und welche Perspektive Kinder selbst auf Privatsphäre im digitalen Umfeld haben. Überlegungen, wie die Politik den Rahmen für eine ausgewogene Balance von Schutz und Freiheit und eine an der Lebenswelt Heranwachsender orientierte Erziehung setzen sollte, bilden den Abschluss der Ausführungen.

1. Einleitung: Aufwachsen im digitalen Umfeld

Kinder wachsen heute in einer von (digitalen) Medien geprägten Lebenswelt auf. Internet (97%) und Smartphone (96%) nutzen, Musik hören (93%) und Online-Videos anschauen (84 %) führen laut JIM-Studie 2019 die Hitliste der regelmäßigen Medienbeschäftigungen Heranwachsender in ihrer Freizeit an (Medienpädagogischer Forschungsverbund Südwest 2020: 12–13). Freizeitaktivitäten wie Treffen mit Freund*innen und Bekannten oder Sport machen werden von drei Viertel bis zwei Drittel aller Jugendlichen mindestens mehrmals die Woche ausgeübt (Medienpädagogischer Forschungsverbund Südwest 2020: 10–11).

Die von Erwachsenen, d. h. von Eltern, pädagogischen Fachkräften, aber auch von Wissenschaftler*innen vorgenommene Differenzierung von

analoger und digitaler Welt ist für Kinder[1] heute keine relevante Trennlinie mehr. Kommunikation ist für sie gleich über welchen Kanal in allen Lebenssituationen unverzichtbar, Emotion ist nicht an körperliche Begegnung gebunden und soziale Nähe entfaltet sich (auch) im digitalen Raum. Dies stellt Erziehungsverantwortliche, aber auch Politik und Gesellschaft vor neue Herausforderungen.

Im Folgenden soll das Spannungsfeld von Schutz- und Freiheitsrechten mit einem Fokus auf Datenschutz und Privatsphäre näher beleuchtet werden. Den Rahmen setzen dabei die UN-Kinderrechtskonvention (UN-KRK) und die Umsetzung der darin verbrieften Rechte einerseits und die Entwicklung und Etablierung von Nutzungsformen digital gestützter medialer Kommunikation und Interaktion sowie Produktion und Rezeption medialer Inhalte durch Kinder und Jugendliche andererseits. Dabei kann eine mit der Verabschiedung der UN-KRK und der Entstehung des *World-WideWeb* im Jahr 1989 seit dreißig Jahren parallel verlaufende Entwicklung in den beiden Bereichen beobachtet werden, bei der bisher kaum erforscht ist, inwieweit mögliche Korrelationen und Wechselwirkungen bestehen.

Das Hans-Bredow-Institut hat 2006/2007 das deutsche Jugendschutzsystem, bestehend aus Jugendschutzgesetz (JuSchG) und Jugendmedienschutzstaatsvertrag (JMStV) der Länder evaluiert und in seinem Bericht formuliert: „Insgesamt wird man in diesem Bereich absolute Sicherheit weder versprechen noch erwarten können; es handelt sich um Risikomanagement." Diesen Begriff hat 2015 das Zentrum für Kinderschutz im Internet (I-KiZ) für die Ausrichtung seiner Arbeit aufgegriffen und sich mit der Frage befasst, wie den Risiken und Gefährdungen, denen Kinder und Jugendliche im Internet ausgesetzt sein können, durch eine intelligente, auf unterschiedliche Elemente gestützte Strategie, begegnet werden kann. Darauf soll im Folgenden näher eingegangen und die Anwendbarkeit eines solchen Konzepts im Bereich des Datenschutzes analysiert werden.

1 Der Begriff Kinder wird in diesem Artikel im Sinne der UN-KRK zur Bezeichnung von jungen Menschen, die das 18. Lebensjahr noch nicht vollendet haben, verwendet.

2. Europäische Einordnung von DSGVO und UN-Kinderrechtskonvention: Bezüge, Widersprüche, Erwartungen und Potenziale

Das Konzept der Privatsphäre ist auch in der UN-Kinderrechtskonvention verankert. Art. 16 zum Schutz der Privatsphäre und Ehre lautet wie folgt:

> *(1) Kein Kind darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.*
> *(2) Das Kind hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.*

Diesem Ansatz ist die Ambivalenz von Freiheits- und Schutzrecht inhärent. Der Anspruch auf Privatsphäre – im öffentlichen Raum ebenso wie im familiären Umfeld – ist ein Freiheitsrecht, das angesichts der Risiken und Bedrohungen eben jener Privatsphäre – insbesondere in digitalen Räumen – einen besonderen Schutz erfordert.

2.1 Kinderrechtlich relevante Regelungen der DSGVO

Mit der Europäischen Datenschutz-Grundverordnung wird erstmals im Bereich des Datenschutzes ein altersdifferenzierender Ansatz verfolgt. Dabei stützt sich die DSGVO auf die UN-Kinderrechtskonvention und versteht Kinder als Personen, die das 18. Lebensjahr noch nicht vollendet haben. Sowohl in den Erwägungsgründen als auch im Normtext werden Kinder als eine Gruppe von Betroffenen mehrfach erwähnt, eine im Rahmen des Projektes Kinderschutz und Kinderrechte in der digitalen Welt durchgeführte Synopse ergab 35 unterschiedliche Fundstellen. Zudem werden besondere Anforderungen an die Verarbeitung der Daten von Kindern gestellt.

Die einleitende Formulierung des Erwägungsgrundes 38 „Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz" ist unter Organisationen und Individuen, die sich für das Kindeswohl einsetzen, auf eine breite positive Resonanz gestoßen, hat aber zugleich auch Fragen aufgeworfen, nach der Ausgewogenheit zwischen dem Schutzbedürfnis einerseits und dem Selbstbestimmungsrecht der betroffenen Kinder und Jugendlichen andererseits. Auch Erwägungsgrund 58 hebt die besondere Schutzwürdigkeit von Kindern hervor und fordert, dass „Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann", wenn sich die Datenverarbeitung an

Kinder richtet. Daraus folgt, dass für die Datenverarbeitung in Kontexten, die sich nicht explizit an Kinder richten, aber oft von diesen genutzt werden, die Verständlichkeit für Kinder nicht ausdrücklich gefordert wird. Kindern wird in Art. 13 der UN-KRK das Recht auf freien Zugang zu Informationen verbrieft:

> *(1) Das Kind hat das Recht auf freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, ungeachtet der Staatsgrenzen Informationen und Gedankengut jeder Art in Wort, Schrift oder Druck, durch Kunstwerke oder andere vom Kind gewählte Mittel sich zu beschaffen, zu empfangen und weiterzugeben.*

Dieses Recht kann durch die in Erwägungsgrund 58 formulierte Beschränkung der Verständlichkeitsanforderung auf Kontexte, die sich direkt an Kinder richten, berührt sein.

In Erwägungsgrund 65 erfolgt unter dem Stichwort „Recht auf Vergessenwerden" eine Abwägung zwischen dem Recht des Kindes auf Löschung von Daten, zu deren Verarbeitung es die Einwilligung im Kindesalter gegeben hat, und dem Recht anderer Personen auf freie Meinungsäußerung und Information. Letzterem Recht wird dabei der Vorrang gegeben und die Speicherung der personenbezogenen Daten, zu der das minderjährige Kind seine Zustimmung gegeben hatte, wird im Interesse der Informationsfreiheit Anderer für zulässig erklärt.

Erwägungsgrund 71 nimmt Bezug auf Entscheidungen und Maßnahmen, die ausschließlich auf automatisierter Verarbeitung personenbezogener Daten Betroffener beruhen, d. h. auf der Grundlage des sogenannten *Profilings*, und formuliert, dass derartige Maßnahmen „kein Kind betreffen [sollten]".

Erwägungsgrund 75 adressiert Risiken „für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — die aus einer Verarbeitung personenbezogener Daten hervorgehen können, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere […] wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern", verarbeitet werden. Mit Bezug auf die in den Erwägungsgründen 71 und 75 angeführten Maßnahmen wäre im Sinne von Art. 32 UN-KRK (Schutz vor wirtschaftlicher Ausbeutung) eine Konkretisierung hinsichtlich des *Profiling* zu kommerziellen Zwecken zur Wahrung des Vorrangs des Kindeswohls wünschenswert.

Auch in den Formulierungen der Erwägungsgründe zeigt sich die Ambivalenz des Rechts auf Datenschutz und Privatsphäre, die schon in Art. 16 der UN-KRK festgestellt werden konnte. Dieses gleichermaßen als Frei-

heits- und Schutzrecht angelegte Privileg kann zu konfligierenden Regelungen führen. Im Folgenden soll anhand einiger Bestimmungen der DSGVO, welche Kinder ausdrücklich erwähnen, näher auf Beispiele eingegangen werden.

Das Grundprinzip der DSGVO beruht darauf, Datenverarbeitung für unzulässig zu erklären und nur unter Ausnahmevorbehalt zuzulassen. In der Folge ist zunächst Art. 6[2] vorrangig von Bedeutung. Art. 6 (1) b) erlaubt die Datenverarbeitung „für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist". BGB Art. 108 (1) besagt: „Schließt der Minderjährige einen Vertrag ohne die erforderliche Einwilligung des gesetzlichen Vertreters, so hängt die Wirksamkeit des Vertrags von der Genehmigung des Vertreters ab." Demzufolge wäre der durch eine minderjährige, d. h. unter 18 Jahre alte, Person mit einem Diensteanbieter durch die Registrierung auf dessen Plattform geschlossene Vertrag schwebend unwirksam, so lange diese Genehmigung nicht vorliegt. Daraus ergibt sich die Frage, welche Auswirkungen auf den Vorrang des Kindeswohls zu erwarten sind, wenn sich Diensteanbieter bei der Datenverarbeitung auf Art. 6 (1) b) stützen. Zugleich muss unter dem Primat des Kindeswohls untersucht werden, welche Unterschiede aus der Einwilligung gemäß Art. 6 (1) a) und in der Folge gemäß Art. 8 bei Personen unter 16 Jahren durch den Träger der elterlichen Verantwortung für das Kind einerseits und der Genehmigung des Vertrags gemäß Art. 6 (1) b) durch den gesetzli-

---

2 Art. 6: Rechtmäßigkeit der Verarbeitung (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

chen Vertreter der minderjährigen Person (unter 18 Jahren) andererseits in Bezug auf das Kindeswohl resultieren können.

Art. 6 (1) f) gibt den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, wenn es sich um ein Kind handelt, den Vorrang vor der Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten. Daraus resultiert die Frage, unter welchen Voraussetzungen der Vorrang des Kindeswohls als Interesse, Grundrecht oder Grundfreiheit im Sinne von Art. 6 (1) f) interpretiert werden darf.

In besonderem Maße manifestiert sich ein Konflikt von Schutz- und Freiheitsinteressen des Kindes in den Regelungen des Art. 8[3] der DSGVO. Art. 8 legt als Altersgrenze für die erforderliche Einwilligung der Eltern in die Nutzung des Angebotes eines Dienstes der Informationsgesellschaft, das einem Kind direkt gemacht wird, die Vollendung des 16. Lebensjahres fest. Ab 16 Jahren können Kinder somit selbständig einwilligen, gelten aber bis 18 Jahre als Kind im Sinne der DSGVO. Die Datenschutz-Grundverordnung lässt in diesem Punkt den Mitgliedstaaten der EU einen Gestaltungsspielraum, die Altersgrenze in einem Korridor zwischen 13 und 16 Jahren festzulegen, um den Datenschutz an nationale Gegebenheiten anzupassen (sogenannte Öffnungsklausel). Hier ist unter Bezugnahme auf die Freiheitsrechte des Kindes in erster Linie zu klären, ob die Altersgrenze unter Berücksichtigung des Art. 5 der UN-KRK (Respektierung des Elternrechts) angemessen gesetzt ist. Im europäischen Vergleich sind die verschiedenen Länder hier zu unterschiedlichen Einschätzungen gekom-

3 Art 8: Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft
(1) Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird. Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.
(2) Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.
(3) Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.

men und es ist ein „Flickenteppich" von geltenden Altersgrenzen entstanden: In Deutschland gilt die Altersgrenze von 16 Jahren, in einigen europäischen Ländern hat man sich auf 13 Jahre geeinigt, in anderen gilt eine Altersgrenze von 14 oder 15 Jahren (Milkaite/Lievens 2019). Inwieweit bei der Entscheidung neben bestehenden Altersgrenzen in anderen Rechtsbereichen auch kinderrechtliche Erwägungen einbezogen wurden, kann nicht abschließend beantwortet werden. Ebenso bleibt offen, inwieweit Art. 2 der UN-KRK (Achtung der Kindesrechte; Diskriminierungsverbot) durch diese unterschiedlichen Regeln berührt ist. Dies gilt umso mehr, da bislang Uneinigkeit darüber besteht, ob für die Anwendung der Altersgrenze das Herkunftslandprinzip gilt, d. h. es wäre die Altersgrenze des Landes, in dem das Unternehmen angesiedelt ist, geltend, oder ob hier das Marktortprinzip greift und damit jeweils die Altersgrenze des Landes, in dem das Unternehmen seine Leistungen am Markt erbringt, was für Kinder in Europa zu Ungleichbehandlung führt.

Unter Berücksichtigung von Art. 5 der UN-KRK zur Respektierung des Elternrechts[4] stellt sich die Frage, in welchen Fällen die Einwilligungserfordernis nach Art. 8 DSGVO im Widerspruch zum Vorrang des Kindeswohls steht. Hier ist beispielsweise an die Nutzung von Online-Beratungsdiensten von Kindern in familiären Konfliktsituationen zu denken und an den gemäß SGB VIII Art. 8 (3)[5] Kindern zustehenden Anspruch auf Beratung ohne Kenntnis der Personensorgeberechtigten. Im Sinne der Lebensweltorientierung sozialer Arbeit muss dieser Anspruch heute auch für die Nutzung von Diensten der Informationsgesellschaft für Beratungszwecke gelten.

Grundsätzlich kommt aber die Einwilligungserfordernis nach Art. 8 nur zum Tragen, wenn die datenverarbeitende Stelle die Rechtmäßigkeit der Verarbeitung auf Art. 6, (1) a) „Einwilligung" beruft. Bei Datenverarbeitung gestützt auf Art. 6 (1) b) – f) ist die elterliche Einwilligung nicht erforderlich. Welche positiven oder negativen Auswirkungen die Entscheidung eines Diensteanbieters, sich auf Art. 6 (1) b) – f) zu berufen, auf den Vorrang des Kindeswohls hat, bedarf ebenso der näheren Betrachtung wie die

4 Art. 5: Die Vertragsstaaten achten die Aufgaben, Rechte und Pflichten der Eltern oder gegebenenfalls, soweit nach Ortsbrauch vorgesehen, der Mitglieder der weiteren Familie oder der Gemeinschaft, des Vormunds oder anderer für das Kind gesetzlich verantwortlicher Personen, das Kind bei der Ausübung der in diesem Übereinkommen anerkannten Rechte in einer seiner Entwicklung entsprechenden Weise angemessen zu leiten und zu führen.

5 SGB VIII Art. 8 (3): Kinder und Jugendliche haben Anspruch auf Beratung ohne Kenntnis des Personensorgeberechtigten.

Frage, welche Auswirkungen auf den Vorrang des Kindeswohls sich daraus ergeben können, dass der Diensteanbieter als die datenverarbeitende Stelle die Daten differenziert und sich auf unterschiedliche Abschnitte von Art. 6 (1) beruft, z. B. Verarbeitung allgemeiner Nutzerdaten gestützt auf Art 6 (1) b) oder f), sensible Daten nach Art. 9 gestützt auf Art. 6 (1) a).

Aus den vorstehenden Ausführungen wird deutlich, dass eine abschließende Beurteilung, inwieweit die Regelungen der DSGVO in Einklang zu bringen sind mit dem Vorrang des Kindeswohls gemäß Art. 3 der UN-KRK weiterer Untersuchungen bedarf. Die ausdrücklich auf Kinder Bezug nehmenden Regelungen der DSGVO stellen – wie zuvor dargelegt – die Schutzbedürftigkeit von Kindern in den Vordergrund und bewirken so eine Nachrangigkeit des legitimen Freiheitsanspruchs von Kindern.

2.2 Konvention 108 und die Leitlinien des Europarats zur Achtung, zum Schutz und zur Verwirklichung der Rechte des Kindes im digitalen Umfeld

Der Europarat hat mit dem „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten", der so genannten Konvention 108 bereits 1985 den ersten – und noch immer einzigen – internationalen Vertrag über das Recht des Einzelnen auf den Schutz seiner persönlichen Daten zur Ratifizierung freigegeben und damit frühzeitig auf die zunehmende Bedeutung automatisierter Prozesse für den Schutz personenbezogener Daten hingewiesen. Wenngleich die Regelungen der Konvention 108 deutlich weniger detailliert sind als die der Datenschutzgrundverordnung, ist die Bedeutung des Vertrags durch die Unterzeichnung der Mitgliedstaaten des Europarats und den Beitritt von weiteren neun Nicht-Mitgliedstaaten durchaus weitreichend und auf internationaler Ebene von Relevanz. Mit dem am 18. Mai 2018 vom Ministerkomitee des Europarats verabschiedeten Änderungsprotokoll Konvention 108+ wird angestrebt, den Herausforderungen, welche die Verwendung neuer Informations- und Kommunikationstechnologien für den Schutz der Privatsphäre darstellen, zu begegnen sowie die Umsetzung der Konvention wirksam zu stärken. Zu den vorgenommenen Modernisierungen zählen u. a. die Definition möglicher Rechtsgrundlagen der Datenverarbeitung und die Einführung des Prinzips der Datenminimierung sowie die Berücksichtigung von genetischen und biometrischen Daten als sensible Daten gemäß Art. 6. Darüber hinaus wurde Art. 7 im Hinblick auf die Datensicherheit um Meldepflichten im Fall von Verstößen ergänzt, und die Betroffenenrechte auf Auskunft, Änderung und Löschung wurden gestärkt. Datenverarbeitenden Stellen wird eine Rechenschaftspflicht auferlegt und sie

werden zur Implementierung des Prinzips *Safety by Design* verpflichtet. Schließlich wird dem grenzüberschreitenden Datenverkehr mehr Beachtung geschenkt, und es werden Regelungen eingeführt, um den Schutz personenbezogener Daten auch in diesem Fall zu gewährleisten; die Rolle der Datenschutzaufsichtsbehörden ist um Informations- und Aufklärungsaufgaben erweitert.

Art. 1 der Konvention 108 hebt bereits in der ersten Fassung die Abhängigkeit der Wahrnehmung der Grundrechte und Freiheiten des Menschen von der Gewährleistung des Schutzes seiner Privatsphäre hervor. Dieser menschenrechtliche Ansatz prägt auch die Leitlinien des Europarats zur Achtung, zum Schutz und zur Verwirklichung der Rechte des Kindes im digitalen Umfeld, die parallel zum Änderungsprotokoll der Konvention 108+ von einer Arbeitsgruppe des Europarats entwickelt und am 4. Juli 2018 vom Ministerkomitee verabschiedet wurden. Ausgangspunkt dieser Entwicklung ist die Sofia-Strategie des Europarats, mit der im Jahr 2016 erstmals eine Strategie zur Umsetzung der UN-KRK vom Europarat beschlossen wurde, die neben den Säulen Chancengleichheit, Teilhabe und Partizipation, gewaltfreies Leben und kindgerechte Justiz auch das digitale Umfeld berücksichtigt. Dem *Ad hoc Committee for the Rights of the Child* – CAHENF wurde die Arbeitsgruppe CAHENF-IT zur Seite gestellt, mit dem Auftrag, entsprechende Leitlinien für das digitale Umfeld zu erarbeiten. Die Leitlinien befassen sich im Abschnitt 3.4 zu Datenschutz und Privatsphäre in den Art. 26 bis 39 mit kinderrechtlichen Aspekten dieses Grundrechts. Sie adressieren den Schutz der Privatsphäre des Kindes im öffentlichen wie im privaten Bereich, stellen Anforderungen an die kindgerechte Information und Aufklärung sowie die Einbeziehung von Kindern, formulieren einen Auftrag zur Berücksichtigung des Kindeswohls bei Technikgestaltung und Voreinstellungen sowie einen Anspruch des Kindes auf anonyme und pseudonyme Nutzungsmöglichkeiten. Mit der in Art. 37 formulierten Forderung, „das Profiling von Kindern, d.h. jede Form der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, ein ‚Profil' eines Kindes anzulegen, insbesondere um Entscheidungen über das Kind zu treffen oder seine persönlichen Vorlieben, Verhaltensweisen und Einstellungen zu analysieren oder vorherzusagen," gesetzlich zu verbieten, gehen die Leitlinien des Europarats über die gesetzlichen Anforderungen der DSGVO hinaus.

Für die Abwägung der Balance von Schutz- und Freiheitsrechten ist die in Art. 31[6] formulierte Anforderung, bei jeglicher Datenverarbeitung eine Bewertung der möglichen Auswirkungen und der Risiken in Bezug auf die Beeinträchtigung der Rechte des Kindes vorzunehmen, besonders relevant; denn damit wird der zuvor bereits dargelegten Ambivalenz des Schutz- und Freiheitsrechts auf Privatsphäre in den Leitlinien ausdrücklich Rechnung getragen (Europarat 2018/2019: 16–18).

Im Folgenden soll näher darauf eingegangen werden, wie der auf politischer Ebene formulierte Anspruch durch die Beteiligung von Kindern und Jugendlichen verwirklicht und so die Perspektive der Betroffenen selbst in politisches Handeln einbezogen werden kann.

3. Beteiligung von Kindern an sie betreffenden Angelegenheiten

Wie zuvor ausgeführt ist die Beteiligung von Kindern in den einschlägigen Normen zum Datenschutz praktisch nicht vorgesehen. Lediglich die Leitlinien des Europarats bieten – gestützt auf die UN-KRK – einen Anknüpfungspunkt. Im folgenden Abschnitt werden Grundlagen und Möglichkeiten der Beteiligung von Kindern an sie betreffenden Angelegenheiten und Maßnahmen am Beispiel des Jugendmedienschutzes aufgezeigt.

3.1 Warum: Grundlagen in der UN-KRK

In der UN-KRK von 1989 sind die Beteiligungsrechte von Kindern fest verankert. Art. 12 und 13 sehen vor, dass Kinder in allen sie betreffenden Angelegenheiten anzuhören sind und ihre Meinung angemessen und entsprechend ihrem Alter und ihrer Reife zu berücksichtigen ist. Allerdings werden die Kindern zustehenden Beteiligungsrechte in der Gesetzgebungspraxis bislang nur selten berücksichtigt. Erstmals soll im Rahmen der aktuellen Novellierung des Jugendschutzgesetzes im Jahr 2020 auch gesetzlich verankert werden, dass Kinder an der Entwicklung sie betreffender Schutzmaßnahmen zu beteiligen sind. Dabei stützt sich der Entwurf des JuSchG auf die UN-KRK und sieht Jugendschutz als Resultat von Maßnahmen in

6 Art. 31: Die Staaten sollten sicherstellen, dass potenzielle Auswirkungen der beabsichtigten Datenverarbeitung auf die Rechte des Kindes bewertet werden und dass die Datenverarbeitung so konzipiert ist, dass das Risiko einer Beeinträchtigung dieser Rechte vermieden oder minimiert wird.

einem Dreieck aus Schutz, Befähigung und Teilhabe, bei dem das Kindeswohl im Mittelpunkt steht. Auf die Wechselwirkung zwischen den Elementen des Dreiecks wird abschließend noch näher eingegangen.

3.2 Wie: Methoden der Kinderbeteiligung

Dass und wie Kinder an der Erarbeitung von Fragen des Jugendmedienschutzes beteiligt werden können, zeigt eine aktuelle Studie von Frense (2020). In ihrer empirischen Untersuchung hat sie mit Sechst- und Zehntklässler*innen Handlungsempfehlungen für einen zeitgemäßen Jugendmedienschutz erarbeitet. Das zugrundeliegende Paradigma Kinderschutz durch Partizipation und Befähigung, angelehnt u.a. an Liebel (2009: 33), Lansdown (2005: 39ff.), Feinstein und O'Kane (2009: 5), illustriert, dass es gelingen kann, Kinder an der Entwicklung effektiver Schutzstrategien zu beteiligen. Zentral ist es dabei, Räume zu schaffen, in denen Kinder als Expert*innen ihrer Lebenswelt ernst genommen werden, ihnen Gehör verschafft und ihnen auf Augenhöhe begegnet wird. Dabei sind stets die sich entwickelnden Fähigkeiten (*evolving capacities*) der Kinder zu berücksichtigen. Dies kann beispielsweise im Rahmen von Workshops geschehen, die inhaltlich nah an der medialen Lebenswelt der Heranwachsenden orientiert sind. Basis für diese Art der Beteiligung stellt die Befähigung dar, um die Kinder in die Lage zu versetzen, informierte Entscheidungen zu treffen.

> „Aber was braucht es, um Kinder zu befähigen? […] Information ist die Voraussetzung für tatsächliche Beteiligung, denn nur wer informiert ist, kann substanziell mitreden." (Radlicki 2011: 18)

Neben der Information ist auch die Befähigung zur Reflexion des eigenen (Medien-)Handelns und der daraus resultierenden Konsequenzen und Implikationen zentral. Dafür bieten sich Ansätze an, die klassischerweise in den Bereich der Medienpädagogik fallen. Was es braucht sind also seitens der Diensteanbieter Bezüge und Schnittstellen zur Medienpädagogik und seitens erwachsener Entscheidungsträger en Willen, Kinder aktiv in die Ausgestaltung von Schutzmaßnahmen einzubeziehen, was auch Ausdruck einer demokratischen Gesellschaft ist:

> „Es ist an den Erwachsenen zu prüfen, ob sie die Anliegen von Kindern ernsthaft hören wollen und, ob ihnen tatsächlich Instrumente und Selbstvertrauen gegeben werden, sich für ihre Dinge zu engagieren. / Demokratie bemisst sich auch daran, wie gut sie die Stimme der

> Schwächsten hört. Für mich gehören starke und befähigte Kinder und ihre Stimme essenziell zu einer demokratischen Gesellschaft." (Radlicki 2011: 17)

Anhand empirischer Daten wird im nächsten Abschnitt die Perspektive von Kindern selbst auf Privatsphäre und Datenschutz als ein ihnen zustehendes Freiheits- und Schutzrecht dargelegt.

4. Die Perspektive der Kinder

Heranwachsende haben heute – in Abhängigkeit von ihren sich entwickelnden Fähigkeiten (*evolving capacities*) – schon früh ein Bewusstsein für den eigenen Anspruch auf Privatsphäre und die aus der Onlinenutzung und dem eigenen Handeln potenziell resultierenden Gefährdungen. Das Thema Privatheit wird für sie insbesondere dann bedeutend, wenn diese nicht respektiert wird. Laut DIVSI U25-Studie (2014 und 2018) vermeiden Kinder im Alter von neun bis 13 Jahren, um ihre Privatsphäre zu schützen vor allem die Angabe von Klarnamen und Adressen sowie die Veröffentlichung von Fotos, auf denen sie selbst abgebildet sind. Möglicher Datenmissbrauch im Internet oder die kommerzielle Verwertung persönlicher Informationen werden erst im späteren Altersverlauf als Risiken wahrgenommen. Die Altersgruppe der 14- bis 17-Jährigen definiert als privat vorrangig alles, was in den Bereich des Intimen und Peinlichen fällt, so zum Beispiel Informationen rund um Gefühle, Sorgen oder Ängste. Allgemeine personenbezogene Daten wie Geburtsdatum, Wohnort oder Schule hingegen werden von dieser Altersgruppe als weniger problematisch eingestuft und somit auch häufiger preisgegeben. Ein Verständnis für den Wert dieser Daten, insbesondere im Zusammenhang mit der Analyse des individuellen Nutzungsverhaltes zu kommerziellen Zwecken, ist kaum vorhanden. Als Instrument des Selbstschutzes werden entsprechende Privatsphäre-Einstellungen in Online-Communitys für ausreichend erachtet. 79 % der 16- bis 18-Jährigen, aber nur ein Viertel der 10- bis 11-Jährigen haben laut einer Studie des BITKOM (2014) individuelle Privatsphäre-Einstellungen in den von ihnen genutzten sozialen Netzwerken vorgenommen. Damit die Kinder neben dem Bewusstsein für Privatheit und die eigene Privatsphäre im Netz auch aktiv Maßnahmen zum Selbstschutz ergreifen, bedarf es offensichtlich sowohl eines gewissen Reifegrades und Alters als auch der umfassenden Vermittlung von Kenntnissen im Bereich des Datenschutzes und der Medienkompetenz (Croll/Pohle 2018).

Im Rahmen des Projektes *Kinderschutz und Kinderrechte in der digitalen Welt* wurden 2018 Kinder mittels einer nicht repräsentativen Online-Befragung[7] um ihre Meinung zu Aspekten des Datenschutzes gebeten. Die große Mehrheit der Kinder betont in dieser auf die Beziehung und Abgrenzung zu ihren Eltern fokussierenden Erhebung den Anspruch auf Schutz der Privatsphäre im familiären Umfeld hinsichtlich ihrer Online-Kommunikationsaktivitäten. In Bezug auf das eigene Handeln stellt sie der verantwortungsbewusste Umgang mit persönlichen Daten vor das Dilemma, unter Umständen nur einen eingeschränkten oder gar keinen Zugang zu für sie wichtigen Online-Angeboten und Diensten zu haben. In diesem Fall tendieren sie entweder zu einer pragmatischen Entscheidung für die Preisgabe der geforderten Daten und nehmen den damit einhergehenden Verlust an Privatsphäre in Kauf oder entwickeln Lösungsstrategien wie die Verwendung von Fake-Namen oder eigens für solche Zwecke angelegten sogenannten „Spam-E-Mail-Adressen".

Ein zentrales Anliegen der von Frense (2020) befragten jungen Menschen ist die auch in Erwägungsgrund 58 der DSGVO geforderte kindgerechte Verständlichkeit von Datenschutzinformationen, wie die folgenden Zitate zeigen:

> „*Sowas wie AGBs oder so. Wenn da jetzt irgendwie stehen würde ‚Ihre geographische Lage wird jetzt in selektiertem Blablabla irgendwas'. Sowas wird da bestimmt gemacht, weil die es ja rechtlich korrekt machen müssen, aber für den User ist es besser, wenn dann so gesagt wird: 'Ihr Standort wird jetzt gezeigt. Sie können ihn an- und ausmachen und für diese an und für diese nicht.'*" (männlich, 16 Jahre)

> „*[A]uch so jugendgerechte Kommunikation zwischen Hersteller und Nutzer […] also, dass Jugendliche jetzt nicht in den Appstore gehen müssen und dann wirklich so die ganzen AGBs durchlesen müssen oder irgendwelche Informationen durchlesen müssen. Dass man das dann wirklich auf der App erscheint, dass das für die Kinder einfacher ist.*" (männlich, 16 Jahre)

Hintergrund ist dabei oft die persönliche Erfahrung mit mangelhaften Privatsphäre-Einstellungen, da Datenschutzbedingungen und Allgemeine Ge-

---

7 Insgesamt haben sich im Zeitraum vom 17. April bis 7. Mai 2018 221 Kinder unter https://kinderrechte.digital sowie www.kindersache.de beteiligt. Weitere 24 Schülerinnen und Schüler einer sechsten Klasse aus Berlin haben im Rahmen einer Unterrichtsstunde teilgenommen und den Kurz-Fragebogen, der geschlossene Fragen und jeweils drei Antwortmöglichkeiten zur Auswahl anbot, ausgefüllt sowie teilweise ergänzend eigene Kommentare zu den Fragen abgegeben.

schäftsbedingungen (AGB) vielfach als nutzer*innenunfreundlich wahrgenommen werden und beklagt wird, dass seitens der Diensteanbieter Updates nicht transparent kommuniziert werden.

> *„[S]chon am Anfang, als es die Funktion neu gab, da habe ich gar nicht gecheckt, dass ich meinen Standort an hatte und dann […] hatte ich den irgendwie am Anfang an und ich wollte den eigentlich gar nicht an haben. Und dann habe ich das irgendwie erst eine Woche später oder so mitbekommen, dass ich den überhaupt an hab. Keine Ahnung, das hätten die irgendwie am Anfang vielleicht deutlicher sagen können, fand ich jetzt so.“* (weiblich, 15 Jahre)

Daneben wurde in den Befragungen ein Spannungsverhältnis zwischen Forderungen nach Autonomie und individueller Verantwortung bezüglich des Umgangs mit Risiken deutlich. Die individuelle Verantwortung wurde sogar derart weit interpretiert, dass in Situationen von Privatsphäre- und/oder anderen Rechtsverletzungen dem Individuum und nicht den Anbietern der Plattform die Verantwortung zugesprochen wird. (Frense 2020: 61)

> *„Letztendlich ist es ja die eigene Entscheidung, wenn man die Videos veröffentlicht oder seinen Account öffentlich stellt. Das ist ja bei jedem selbst. Also man kann ja auch bei TikTok einfach nur so TikToks machen, die dann privat sind und die man sich nur selbst angucken kann. Also von daher ist es dann ja sozusagen die eigene Schuld, wenn man es dann hochlädt auf seinem Account und irgendwie veröffentlicht.“* (weiblich, 16 Jahre)

Weitere Forderungen von Kindern und Jugendlichen wie ein Recht auf Löschen im Internet und die Kontrolle von dessen Einhaltung sowie eine Zustimmungspflicht bei der Veröffentlichung von Bildern der Kinder im Netz wurden im Rahmen des Netzfestes der *re:publica* 2019 mit Kindern erarbeitet (Croll 2019).

Diese mit unterschiedlichen Methoden erhobenen Perspektiven von Kindern auf ihre Rechte gemäß Art. 16 der UN-KRK zeigen ein breites Spektrum von Haltungen gegenüber Risiken und Verletzungen der Privatsphäre im digitalen Umfeld und sie zeugen von einem hohen Bewusstsein für die Notwendigkeit von Maßnahmen des Schutzes und der Eigenverantwortlichkeit.

5. Fazit und Ausblick: Das Recht auf Privatsphäre unter Druck im Digitalen

Wenn Kinder im digitalen Umfeld aufwachsen, geschieht das in einem Spannungsfeld zwischen Schutzbedarf und Freiheitswunsch. Dies sollte eine an der Lebenswelt orientierte Erziehung (Thiersch 2014) berücksichtigen und die Politik dafür den geeigneten Rahmen setzen.

Die im Modell des Intelligenten Risikomanagements für verschiedene Altersgruppen definierten strategischen Schutzziele Risikoausschluss, Risikovermeidung und Risikoreduzierung spiegeln die Entwicklung entlang der Kindheits- und Jugendphasen wider. Je jünger die Kinder sind, umso mehr sollen Instrumente des Jugendmedienschutzes Risiken ausschließen oder vermeiden. Mit zunehmendem Alter der Kinder und Jugendlichen kann sich der Jugendmedienschutz auf die Reduzierung (gravierender) Risiken beschränken und den Fokus auf die Befähigung zum Umgang mit Risiken richten. Dieses Modell ist auf den Bereich des Datenschutzes übertragbar. Dazu bedarf es allerdings sowohl der Einhaltung der Vorgaben der DSGVO in Bezug auf Transparenz und Verständlichkeit, als auch der Förderung der Kompetenzen in Bezug auf den Datenschutz bei Kindern ebenso wie bei den für sie Verantwortung tragenden Erwachsenen.

Wird für Befähigungsmaßnahmen ein partizipativer Ansatz gewählt, d. h. die Kinder werden selbst an der Entscheidung über zu adressierende Risiken und der Entwicklung von geeigneten Schutzkonzepten beteiligt, darf erwartet werden, dass sie diese in höherem Maße akzeptieren. Die bisher eingesetzten Instrumente des Jugendschutzes und des Datenschutzes werden insbesondere von jungen Menschen im Teenageralter eher als Herausforderung gesehen, die es zu umgehen gilt. Gerade deshalb ist die Einbeziehung von Jugendlichen in die Entwicklung von Schutzmaßnahmen wichtig. Aus der Partizipation heraus wächst das Interesse und das Verständnis für die Notwendigkeit des Schutzes, Maßnahmen, an deren Entwicklung junge Menschen mitwirken, haben das Potenzial, in der Zielgruppe größere Akzeptanz zu finden. So kann mittels partizipativer Methoden ein effektiver Jugendmedienschutz gestaltet werden, der an der Lebenswelt und den Bedarfen von Heranwachsenden ansetzt.

Wie zuvor ausgeführt orientiert sich der aktuelle Prozess der Novellierung des JuSchG an der UN-KRK und sieht einen Jugendmedienschutz vor, der sich auf Art. 3 der UN-KRK stützt und das Kindeswohl in den Mittelpunkt eines Dreiecks aus Schutz, Befähigung und Teilhabe stellt (Croll 2018: 45). Schutz und Befähigung sind dabei die Grundlagen für gesellschaftliche Teilhabe, wobei sich Teilhabe wiederum positiv auf die Bereitschaft zur Akzeptanz von Schutz- und Befähigungsmaßnahmen auswirkt. In den Regelungen der DSGVO hingegen scheint teilweise eine diesen

pro-partizipativen Entwicklungen zuwiderlaufende und paternalistisch vor allem auf Schutzmaßnahmen setzende Haltung auf. Diese steht insbesondere im Widerspruch zu dem in Art. 12 der UN-KRK verbrieften Recht des Kindes gehört zu werden. Ein potenziell aus der Berücksichtigung des Kindeswillens einerseits und dem Vorrang des Kindeswohls andererseits resultierendes Dilemma muss zukünftig auch im Bereich des Datenschutzes noch aufgelöst werden.

Literatur

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Hg.) (2014): *Jung und vernetzt—Kinder und Jugendliche in der digitalen Gesellschaft*. Berlin. Online verfügbar unter: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2014/Studien/Jung-und-vernetzt-Kinder-und-Jugendliche-in-der-digitalen-Gesellschaft/BITKOM-Studie-Jung-und-vernetzt-2014.pdf (Abfrage am: 25.05.2020).

Croll, Jutta (2019): *Wo sind die Stimmen der Kinder in der Netzpolitik. Kinderschutz und Kinderrechte in der digitalen Welt*. Online verfügbar unter: http://kinderrechte.digital/fokus/index.cfm/key.3443 (Abfrage am: 13.04.2020).

Croll, Jutta (2019): *Das Recht des Kindes auf Privatsphäre in einer digitalisierten Lebenswelt*. In: Frühe Kindheit (2), S. 24-31.

Croll, Jutta (2018): *Im Mittelpunkt das Kind. Eine kinderrechtliche Perspektive auf den Kinder- und Jugendschutz im Internet*. In: Aus Politik und Zeitgeschichte 68 (40/41), S. 40-46.

Croll, Jutta / Pohle, Sophie (2018): *Stopp! Geheim – Das Kinderrecht auf Datenschutz und Privatsphäre in der digitalen Welt*. In: Merz Wissenschaft Kinder|Medien|Rechte 62 (6), S. 29-40.

Deutsches Institut für Vertrauen und Sicherheit im Internet (2018): *DIVSI U25-Studie – Euphorie war gestern*. Online verfügbar unter: https://www.divsi.de/wp-content/uploads/2018/11/DIVSI-U25-Studie-euphorie.pdf (Abfrage am: 25.05.2020).

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (2014): *DIVSI-U25-Studie–Kinder, Jugendliche und junge Erwachsene in der digitalen Welt*. Online verfügbar unter: https://www.divsi.de/wp-content/uploads/2014/02/DIVSI-U25-Studie.pdf (Abfrage am: 25.05.2020).

Europarat (2018/2019): *Leitlinien zur Achtung, zum Schutz und zur Verwirklichung der Rechte des Kindes im digitalen Umfeld*. Online verfügbar unter: https://rm.coe.int/168092dd25 (Abfrage am: 03.06.2019).

Feinstein, Clare / O'Kane, Claire (2009): *Children's and Adolescents' Participation and Protection from Sexual Abuse and Exploitation*. No. 2009/09. New York: UNICEF Innocenti Research Centre. https://doi.org/10.18356/443a21a8-en.

Frense, Elena (2020): *Partizipativer Jugendmedienschutz: Anforderungen an einen zeitgemäßen Jugendmedienschutz aus Perspektive von Kindern und Jugendlichen*. Frankfurt am Main: Debus Pädagogik.

Lansdown, Gerison (2005): *The Evolving Capacities of the Child*. Florence: Unicef Innocenti Research Centre.

Liebel, Manfred (2009): *Kinderrechte – Aus Kindersicht: Wie Kinder weltweit zu ihrem Recht kommen*. Berlin: Lit.

Medienpädagogischer Forschungsverbund Südwest (Hg.) (2020): *JIM-Studie 2019—Jugend, Information, Medien—Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger*. Online verfügbar unter: https://www.mpfs.de/fileadmin/files/Studien/JIM/2019/JIM_2019.pdf (Abfrage am: 24.05.2020).

Milkaite, Ingrida / Lievens, Eva (2019): *Better Internet for Kids—Status Quo regarding the Child's Article 8 GDPR Age of Consent for Data Processing across the EU*. Better Internet for Kids. Online verfügbar unter: https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751 (Abfrage am: 25.05.2020).

Radlicki, Eva (2011): *Wie ernst ist es uns mit dem „Kinder ernst nehmen"?* In: Schächter, Markus / Apel, Peter (Hg.): Ich kann. Ich darf. Ich will: Chancen und Grenzen sinnvoller Kinderbeteiligung. Baden-Baden: Nomos, S. 17-20.

Thiersch, Hans (2014): *Lebensweltorientierte Soziale Arbeit: Aufgaben der Praxis im sozialen Wandel* (Edition Soziale Arbeit) (9. Auflage). Weinheim Basel: Beltz Juventa.

„Gebe ich jetzt meine Daten preis oder nicht?“ Privatheit und Datenschutz in der Frühen Kindheit

Senta Pfaff-Rüdiger, Andreas Oberlinner, Susanne Eggert und Andrea Drexl

Abstract

Datenschutz und der verantwortungsbewusste Umgang mit eigenen und fremden Daten bei der Mediennutzung ist ein komplexes Thema, das besondere Herausforderungen mit sich bringt: Für viele Eltern ist es nicht einfach, an konkreten Beispielen zu erläutern, wie Daten verarbeitet und zu welchen Zwecken sie von Anbietern genutzt werden. Datenmissbrauch und die Bedeutung von Datenschutz und Privatheit sind darüber hinaus keine Phänomene, denen die Kinder in ihrer alltäglichen Mediennutzung häufig begegnen. Vor diesem Hintergrund ein Bewusstsein für die eher abstrakten Themen Privatheit und Datenschutz in der frühen Kindheit zu entwickeln und im medienerzieherischen Alltag umzusetzen, ist umso schwieriger. In einer qualitativen Langzeitstudie mit Familien mit Kindern im Alter von null bis sechs Jahren wurden die Haltungen und (Medienerziehungs-)Praktiken der Eltern im Umgang mit den Daten ihrer Kinder erhoben. Dabei konnten anhand der Kriterien Relevanz des Themas und Umsetzung im medienerzieherischen Handeln drei unterschiedliche Typen herausgearbeitet werden. Es wurde deutlich, dass die Auseinandersetzung und der Umgang mit dem Bereich Datenschutz und Privatheit von Kindern im Kleinkindalter insbesondere mit der medienerzieherischen Haltung der Eltern zusammenhängen.

1. Einleitung

Die Mediatisierung von Gesellschaft und Familie führt dazu, dass sämtliche Lebensbereiche mit digitalen Informations- und Kommunikationstechnologien durchdrungen werden. Kinder kommen dadurch immer früher mit digitalen Medien in Berührung und Eltern sehen sich mit der Aufgabe konfrontiert, ihre Kinder vom ersten Lebenstag an bei der Entwicklung eines kompetenten Medienumgangs zu begleiten und zu unterstüt-

zen. Aufgrund der kognitiven kindlichen Entwicklung bedeutet dies zunächst, dass Eltern ihren Kindern eine souveräne Gestaltung des Alltags mit digitalen Medien vorleben und ihnen damit als Vorbild dienen, an dem die Kinder sich in ihrem eigenen Handeln orientieren können. Dies erfordert auf Seiten der Eltern die Reflexion und Bewusstheit des eigenen Medienhandelns und damit verknüpft eine Sensibilität für die medienbezogenen Bedürfnisse ihrer Kinder (vgl. Eggert/Wagner 2016). Da Kinder im frühkindlichen Stadium sich dieser Bedürfnisse zum Teil nur unzureichend oder (noch) gar nicht bewusst sind und diese (noch) nicht äußern können, sind die Eltern in der Verantwortung, an ihrer Stelle zu entscheiden. Mit Blick auf den Umgang mit Daten der Kinder heißt das auch, Entscheidungen zu treffen, deren mögliche Konsequenzen vielleicht erst in der Zukunft liegen. Dies gelingt den Eltern in unterschiedlichem Maße.

Hier setzt der Beitrag an. Im Zentrum stehen die Haltungen und das medienerzieherische Handeln von Eltern zum Thema Privatheit und Datenschutz in der frühen Kindheit, und damit bei Eltern von Kindern, die selbst noch kein Bewusstsein von Privatheit und Datenschutz haben. Welche Haltung haben Eltern zu Datenschutz, Privatheit und Sharenting und wie setzen sie dies in ihrem medienerzieherischen Handeln um? Im Rahmen der Langzeitstudie Familien-Medien-Monitoring wurden 2019 hierzu 17 Familien qualitativ befragt. Der Beitrag geht im Folgenden zunächst auf Privatheit und Datenschutz in der frühen Kindheit ein (Kapitel 2), bevor das methodische Vorgehen vorgestellt (Kapitel 3) und die zentralen Ergebnisse (Kapitel 4) diskutiert werden. Eine Typologie der unterschiedlichen medienerzieherischen Herangehensweisen an das Thema Privatheit macht abschließend (Kapitel 4.5) Einflussfaktoren erkennbar und gibt Hinweise darauf, wie Eltern in ihrer medienerzieherischen Kompetenz unterstützt werden können.

2. *Privatheit und Datenschutz in der frühen Kindheit*

Das Aufwachsen in einer sich kontinuierlich wandelnden Medienumwelt bringt Themen wie Datenschutz und Privatheit mit sich. Im Rahmen der Medienerziehung beschäftigen sich Eltern damit häufig erst, wenn es die eigenständige Nutzung der Kinder von Smartphone und Internet betrifft (vgl. Kutscher/Bouillon 2018). Im Fokus der wissenschaftlichen Auseinandersetzung standen dabei lange das Medienhandeln der Kinder und die Gefahren, denen Kinder durch Dritte online ausgesetzt sind. Ausgeblendet wurde dabei, welche Folgen das Medienhandeln der Eltern selbst für die Kinder haben kann (Kutscher 2019: 9f.). Im Folgenden geht es um den

Umgang der Eltern mit Privatheit und Datenschutz in Familien mit Kindern im Alter von 0 bis 6 Jahren (frühe Kindheit) und damit um einen Bereich, der sehr stark vom Handeln der Eltern geprägt ist.

2.1 Privatheit in der frühen Kindheit

In der Annahme, dass Eltern ihre Kinder am besten kennen und einschätzen können, agieren Eltern von Kindern im Alter zwischen null und sechs Jahren als deren Treuhänder*innen und vertreten ihre Rechte (vgl. § 104 BGB). Kinder verfügen in diesem Alter noch nicht über die kognitiven Fähigkeiten, um einen Wunsch nach Privatheit auszubilden und zu artikulieren (vgl. Stapf 2019: 18) oder über das Gefühl von Scham, ihr Bedürfnis nach Privatheit zum Ausdruck zu bringen (Walper/Maywald 2019: 3). Ebenso wird davon ausgegangen, dass Erwachsene aufgrund eines gewissen Erfahrungsvorsprunges und Informiertheit abwägen können, welche Folgen medienbezogenes Handeln mit sich bringen kann (vgl. Kutscher 2019: 9). Eltern sind sich jedoch oft der frühkindlichen Privatsphäre nicht bewusst (Stapf 2019: 18f.). Dadurch wird die Privatheit der Kinder, die Grundlage eines selbstbestimmten Lebens in der digitalen Welt ist, gefährdet, obwohl Kinder gleichzeitig ein Recht auf Privatheit (Art. 16 UN Kinderrechtskonvention) sowie ein Recht am eigenen Bild (§ 22 KunstUrhebG) haben.

Für Eltern sind Privatheit und Datenschutz wichtige Themen (DIVSI 2015: 17, Kutscher 2019: 12). Oftmals offenbaren sie aber persönliche Informationen über ihre Kinder im Netz (Naab 2019: 98). Das Privacy Paradox betrifft damit nicht nur die Preisgabe eigener Informationen, sondern auch die Preisgabe von persönlichen Informationen der Kinder. Grundsätzlich wird zwischen der informationellen, der psychologischen und der sozialen Privatheit unterschieden (vgl. Burgoon 1982). *Informationelle* Privatheit, d. h. Daten, die angegeben werden, um sich auf sozialen Netzwerken anzumelden, wird vor allem im Kontext einer aufkommenden datafizierten Kindheit thematisiert, bei der immer mehr Daten bereits von Kleinkindern online zu Verfügung stehen (Siibak/Traks 2019: 116), sei es durch Sharenting, die Nutzung von Kinderapps oder digitalem Spielzeug (Barassi 2018: 169f.). Die *psychologische* Privatheit bezieht sich auf meist intime Informationen, die geteilt werden, um die eigene Identität oder Beziehungen zu gestalten (Naab 2019: 98), während es bei der *sozialen* Privatheit darum geht, selbst bestimmen zu können, sich dem Kontakt zu anderen zu entziehen (Braun/Trepte 2017: 7). Eltern ist es dabei ein „wichtiges Anliegen, dass ihre Kinder verstehen, dass Inhalte – Fotos, Texte, persönli-

che Daten etc. – die im Internet stehen, öffentlich sind" (Wagner et al. 2016: 23). Maßnahmen können dabei auf drei Privatheitsebenen umgesetzt werden: der kommerziellen, der institutionellen und der interpersonellen Privatheit (Livingstone et al. 2019). Die gewerbliche Datenverwendung durch Unternehmen kann als *kommerzielle* Privatheit beschrieben werden. Hier zeigt sich ein Unbehagen insbesondere bei personalisierter Werbung (Barassi 2018: 170). Die *institutionelle* Privatheit umfasst Daten, die im Kontext von Kindertageseinrichtungen, der Regierung oder von Gesundheitseinrichtungen gesammelt und ausgewertet werden. Beim Sharenting ist die *interpersonelle Privatheit* besonders wichtig. Im Sharenting „verbindet sich die seit langer Zeit zum Doing Family gehörende Praxis des Fotografierens von Familienmitgliedern (…) durch die Eltern mit der digitalen sozialen Netzwerkpraktik des Postens und Teilens" (Kutscher 2019: 8); es geht vorzugsweise um das Beziehungsmanagement, familialen Zusammenhalt und die Vermittlung von Kontinuität (Brosch 2018: 76, Schier 2013: 51). Hier liegt der Fokus auf der relationalen Ebene und der Frage, wie durch Privatheit Grenzen in Beziehungen ausgehandelt werden, beispielsweise welche Informationen wann mit wem geteilt werden (Livingstone et al. 2019: 11). Die Bedürfnisbefriedigung der Eltern steht dabei im Kontrast zur Datensparsamkeit und den Rechten der Kinder. Die Eltern müssen folglich abwägen, welche Daten sie wo preisgeben.

2.2 Sharenting als Familienpraxis

Durch die zunehmende Mediatisierung der Gesellschaft wird Familie immer häufiger über digitale Medien (re-)produziert und Sharenting hat sich als eine familiale Alltagspraxis etabliert (Autenrieth 2017: 147, Schlör 2019: 8). Das Phänomen Sharenting lässt sich nach vier Kategorien unterscheiden (Brosch 2018: 79). Zum einen nach (1) dem *Kanal*, über den Kinderbilder geteilt werden. Hiermit sind nicht nur unterschiedliche Social-Media-Anwendungen oder Messenger gemeint, sondern auch, ob die Bilder als Profil- bzw. Statusbild genutzt oder im privaten Chat verschickt werden. Die *Häufigkeit* der Nutzung (2) und die *Abwägung, mit welchem Adressat*innenkreis* (3) die Bilder geteilt werden, stellen weitere Kategorien dar. Dabei geht es vor allem um das unsichtbare Publikum und die Tatsache, dass Bildmotive, die zu einem nicht zu vernachlässigenden Teil peinlich für die Kinder sind, unbeabsichtigt in eine breitere Öffentlichkeit gelangen können (Brosch 2016: 230f., Kutscher/Bouillon 2018: 7). Es ist nahezu unmöglich, das Teilen und Verschicken von Bildern auf den gewünschten Adressat*innenkreis zu begrenzen und eine weitere Verbrei-

tung zu kontrollieren bzw. zu verhindern (vgl. z.B. UNICEF 2017: 92). Geteilt werden in Social Media häufig glückliche Momente des Familienlebens. Im Fokus stehen dabei *inhaltlich* (4) besondere Ereignisse oder Alltagsimpressionen. Oft sind Kinder bereits durch Ultraschallaufnahmen oder Bilder kurz nach der Geburt im Netz präsent (Autenrieth 2014: 102). Hier wird die Ambivalenz des Themas deutlich, da beim Sharenting eine Vielzahl von Kinderrechten verletzt werden können. Eine in den Medien häufig thematisierte Gefahr ist die Verbreitung von Kinderbildern in Pädophilen-Foren. Fotos, auf denen Kinder nackt oder nur teilweise bekleidet sind, werden durch Dritte von privaten Profilen heruntergeladen und zweckentfremdet. Problematisch sind auch Bilder, welche die Kinder in anderen Kontexten identifizierbar machen. Personenbezogene Daten wie der volle Name, die Adresse oder der aktuelle Aufenthaltsort können missbraucht werden.

2.3 Privatheit und Datenschutz als Teil der elterlichen Medienerziehung

Sharenting und der Umgang mit Datenschutz und der Privatheit der Kinder ist eingebettet in das medienerzieherische Handeln der Eltern. Studien zeigen, dass Eltern im Zuge der Medienerziehung ihren Kindern die Kompetenzen vermitteln wollen, ihre Privatsphäre zu schützen und die Konsequenzen des eigenen Handelns abzuschätzen (DIVSI 2015: 108, Wagner et al. 2016: 23). Für die kindliche Mediennutzung ist die Balance zwischen klaren Regeln, Vertrauen zwischen Eltern und Kindern und der Grad der Kontrolle durch die Eltern von Bedeutung. Gelingt dies, können Eltern ihrem Kind dabei helfen, ein Bewusstsein für seine Privatheit zu entwickeln und Medien und ihre Inhalte den eigenen Zielen und Bedürfnissen entsprechend kompetent zu nutzen (Walper/Maywald 2019: 3).

Die Studie „Kinder.Bilder.Rechte“ (2018) zeigt, dass Eltern Datenschutz und die Privatheit der Kinder zwar als wichtige Themen wahrnehmen, aber nicht über das nötige Wissen und die Fähigkeiten verfügen, um diese in der Praxis ausreichend zu schützen. Die Grundlage der elterlichen Datenschutzstrategien ist laut Kutscher „[e]ine Melange von Halbinformiertheit, Unsicherheit, Hilf- und Machtlosigkeit aber auch Gewöhnung an die Nutzungslogiken der digitalen Dienste“ (Kutscher 2019: 12). Vielfach werden dabei (un-)bewusst Kinderrechte verletzt, da der Wunsch nach eigener Bedürfnisbefriedigung stärker wirkt als der die Rechte der Kinder zu schützen (Naab 2019: 108f., Kutscher/Bouillon 2018: 8). Eingesetzte Strategien, um Privatheit und informationelle Selbstbestimmung zu gewährleisten, können dabei nicht getrennt werden von der Motivation, soziale Netzwer-

ke oder andere Dienste zu nutzen (Brüggen/Wagner 2017: 138). Darüber hinaus haben die Eltern keine konsistente Vorstellung davon, wie sie Medienkompetenz und Medienwissen ihrer Kinder im Bereich Privatheit fördern können (Naab 2019: 98). Ihrer Verantwortungs- und Vorbildfunktion sind sich die Eltern kaum bewusst. Auch die Folgen ihrer Social-Media-Aktivitäten können sie nur begrenzt abschätzen (Kutscher/Bouillon 2018: 14). Je geringer die Kompetenz der Eltern im Umgang mit digitalen Medien, desto weniger Sicherheitsmaßnahmen ergreifen sie zum Schutz ihrer Kinder (DIVSI 2015: 133). Da die Eltern in der frühen Kindheit eine Treuhänder*innen-Rolle für ihre Kinder übernehmen, hat ihr Medien- und medienerzieherisches Handeln einen großen Einfluss darauf, welche Kompetenzen Kinder später in diesem Bereich erwerben können. Lange wurde bei der Frage nach Privatheit von Kindern ausgeblendet, welche Folgen das Medienhandeln der Eltern selbst für die Kinder haben kann. Die Studie fokussiert deshalb auf das medienerzieherische Handeln und die Haltung der Eltern zu Privatheit und Datenschutz in der frühen Kindheit und fragt auch danach, wie es gelingen kann, dass Eltern bereits in der frühen Kindheit, Privatheit und Datenschutz als wichtige medienerzieherische Themen erkennen und in ihr medienerzieherisches Handeln integrieren.

3. Methodisches Vorgehen und Stichprobe

Die Teilstudie „Familien-Medien-Monitoring“ (FaMeMo) fragt nach der Bedeutung digitaler und mobiler Medien in Familien mit Kindern im Alter von 0 bis 8 Jahren, wie sich Kinder diese Medien im Gesamtkontext der sie umgebenden Medienwelt aneignen und wie Eltern sie dabei begleiten. In einer Längsschnittstudie wurden 20 Familien bayernweit von 2017 bis 2020 in sechs Erhebungen mit qualitativen Leitfadeninterviews befragt. Neben der kontinuierlichen Erfassung der sich verändernden Mediennutzung und Begleitung durch die Eltern, wurden zusätzlich unterschiedliche Schwerpunktthemen gesetzt, um vertiefende Einblicke in bestimmte Bereiche zu erlangen. In der fünften Erhebung wurde mit gezielten Fragen auf die Praxis des Sharenting und auf Regeln bezüglich des Datenschutzes in der Familie eingegangen.

Die Auswahl der Familien erfolgte nach einer Quotenstichprobe (Akremi 2014: 273). Die Kriterien waren dabei das Geschlecht und Alter der Fokuskinder zu Beginn der Erhebung, die infrastrukturellen Rahmenbedingungen der Haushalte (städtische Kontexte, ländliche Räume) sowie die Bildung der Eltern, erhoben über die Ausbildungshintergründe der Eltern (niedriger/höher, vgl. Abb. 1). Eine Voraussetzung zur Teilnahme war,

dass digitale Medien in der Familie vorhanden sind und auch genutzt werden. Die Medienaffinität der Eltern war kein Auswahlwahlkriterium, im Verlauf der Studie stellte sich aber heraus, dass die Familien digitale Medien unterschiedlich stark nutzen. Von den 20 Familien zu Beginn waren 2019 noch 17 Familien in der Befragung dabei, diese Panelmortalität wurde in der Zusammenstellung des Sample einkalkuliert (vgl. Stein 2014: 144).

Abbildung 1: Zusammensetzung des Samples nach Kriterien, Stand: 2019

Kriterium	Alter 2017[1]				Start 2017	Stand 2019
	1 Jahr	2 Jahre	3 Jahre	4-5 Jahre		
Anzahl der Fokuskinder	6	3	6	5	20	17
Geschlecht Fokuskind (m/w)	2/4	2/1	3/3	2/3	9/11	9/8
Infrastruktureller Bezugsraum (Stadt/Land)[2]	4/2	0/3	3/3	3/2	10/10	8/9
Bildungshintergrund Eltern (höher/niedriger)	3/3	2/1	2/4	3/2	10/10	9/8

Die Leitfadeninterviews fanden meist bei den Familien zu Hause statt und dauerten 60 bis 90 Minuten. Die Interviews wurden vollständig transkribiert, anonymisiert und anschließend mit MAXQDA codiert. Die Auswertung fand dabei deduktiv theoriegeleitet und induktiv aus dem Material heraus statt (vgl. Meyen et al. 2019). Abschließend wurde eine Typologie entwickelt, die sich an der empirisch fundierten Typologiebildung nach Kluge (2000) orientiert. Nach der ersten Auswertung wurde deutlich, dass sich die Eltern vor allem darin unterscheiden,

1. welche persönliche *Relevanz* sie dem Thema Datenschutz und Privatheit zuschreiben,
2. ob sie Datenschutz und Privatheit auch *in ihre medienerzieherische Praxis integrieren*.

Anhand dieser zwei Kriterien wurden Gemeinsamkeiten und Unterschiede zwischen den Eltern deutlich, die zu einer Typenbildung sowie einer Charakterisierung und Namengebung führten. Um Einflussfaktoren ableiten zu können, wurden Kontextfaktoren in die Typologie einbezogen (vgl. Schorb/Theunert 2000).

1 Zum Zeitpunkt der fünften Erhebung, in deren Kontext Sharenting abgefragt wurde, waren die Kinder zwei Jahre älter.
2 Unter den Bezugsraum Land werden ländliche Räume und Kleinstädte gefasst, der Bezugsraum Stadt meint mittlere und große Städte.

4. Privatheit und Datenschutz im Familien-Medien-Monitoring

4.1 Zwischen smarten Geräten und eigenständiger Nutzung: Mediennutzung und Medienerziehung in den Familien

Seit Beginn der Erhebungen sind in den Familien umfangreich digitale Mediengeräte vorhanden. So besitzen alle Eltern Smartphones. Laptops, Computer oder Tablets sind als zusätzliche Geräte neben den meist exklusiv persönlich genutzten Smartphones ebenfalls zu finden. Nur in den wenigsten Haushalten gibt es keine Fernsehgeräte, häufig verfügen die Familien über Smart-TVs oder sind mit einem Streaming-Stick ausgestattet. Die Familien ohne Fernsehgerät streamen Videos über Laptops oder Tablets. Daneben gibt es vereinzelt auch andere Geräte wie Smartwatches, 3D-Drucker, Konsolen sowie in drei Familien Sprachassistenzsysteme.

Mediennutzung in den Familien: Zwischen Streaming und Sprachassistenzsystemen

Die Mediennutzung der Eltern ist neben dem Fernsehen und der vereinzelten Nutzung des Laptops zum Arbeiten sehr stark auf das Smartphone konzentriert. Besonders *WhatsApp*, aber auch *Facebook* und vereinzelt *Instagram* werden intensiv für den Austausch mit Bekannten, Freund*innen und Verwandten genutzt. Daneben wird das Handy als Allrounder für Online Shopping, als Wecker, für Fotos oder zum Telefonieren verwendet. Ähnlich breit ist auch das Nutzungsverhalten der Kinder: Sie haben auf unterschiedliche Art und Weise Zugang zu digitalen Medien, die rezeptive Zuwendung dominiert dabei. So gibt es nur wenige Kinder, die nicht eine Fernsehsendung oder gestreamte Videos ansehen dürfen. *YouTube* spielt dabei in vielen Familien eine große Rolle und variiert von der gemeinsamen Nutzung auf dem Fernsehgerät bis zur alleinigen Nutzung des Kindes auf dem Smartphone der Eltern. Neben der rezeptiven Nutzung audiovisueller Medien nutzen die Kinder auch andere Anwendungen auf mobilen Geräten, zum Beispiel fotografieren sie mit dem Smartphone oder nutzen Sprachassistenzsysteme wie *Alexa*. So wird beispielsweise *Alexa* bei Familie Huber[3] zum Musikhören genutzt, während das Kind spielt. Adrian (3) versteht es dabei, *Alexa* selbst per Sprachsteuerung zu bedienen. Vereinzelt werden auch Medienangebote wie *Skype* oder *WhatsApp* genutzt, damit das Kind mit den Großeltern Kontakt halten kann. Auch sprachgesteuerte

3 Die Namen der Familien sind anonymisiert.

Streaming-Sticks wie der *Fire-TV-Stick* von *Amazon* werden von einigen Kindern bereits selbst bedient. Mit zunehmendem Alter stehen den Kindern andere Medienangebote zu Verfügung. So durfte der Sohn von Familie Huber bereits mit zwei Jahren den Sprachassistenten bedienen, Zugang zu Fernsehinhalten bekam er aber erst nach und nach. Mit vier Jahren darf er nun auch selbstständig altersgerechte Spiele auf dem Tablet spielen. Auch bei vielen anderen Kindern hat sich im Untersuchungszeitraum die eigenständige Nutzung erhöht, die Kinder machen zum Teil Fotos mit den Smartphones ihrer Eltern oder nutzen bereits *YouTube Kids* alleine.

Medienerziehung in den Familien: Regeln und Vorbildfunktion

Die Mediennutzung läuft in vielen Familien sehr strukturiert ab. Oft gibt es klare Regeln, die die Nutzung von Geräten zeitlich und inhaltlich festlegen und in die Alltagsstruktur integrieren (vgl. Oberlinner et al. 2018). Ausnahmen gibt es dann, wenn Außergewöhnliches im Leben der Familien passiert, beispielsweise wenn ein Kind krank ist. Die Regeln werden aber nur selten den Kindern gegenüber begründet, sondern meist lediglich gesetzt. Die Eltern achten insgesamt auf altersgerechte Angebote und schließen bestimmte Inhalte aus, die sie als ungeeignet erachten. Viele Eltern möchten beim eigenen Umgang mit ihren Mediengeräten gute Vorbilder für ihre Kinder sein. Dies gelingt manchen nach eigener Einschätzung gut, andere sehen sich selbst als schlechte Vorbilder. Sie sorgen sich, dass die Kinder ihr Verhalten kopieren oder sie ihren Kindern zu wenig Beachtung schenken. Nur wenige Eltern benennen klare Regeln für sich selbst, wie zum Beispiel den Verzicht auf das Handy beim Essen.

4.2 Zwischen Datensparsamkeit und personalisierter Werbung: Haltungen zu Privatheit und Datenschutz

Privatheit und Datenschutz sind für alle befragten Eltern relevante Themen. Je nachdem, wie Eltern das Thema wahrnehmen, richten sie ihr medienerzieherisches Handeln danach aus (vgl. Eggert 2019). Die Haltungen sind dabei sehr unterschiedlich und reichen von einer „digital konservativen“, auf Datensparsamkeit bedachten Einstellung bei Familie Schäfer (EH2, Sohn 3,5 Jahre)[4] bis zu einer „ein stückweit vielleicht gutgläubig

4 Die Altersangaben zu denselben Kindern können im Text variieren, da die Belege sich immer auf die jeweilige Erhebungswelle (EH1 bis EH5) beziehen und jeweils angegeben wird, wie alt die Kinder zum Zeitpunkt dieser Erhebung waren.

oder naiv[en]“ Haltung bei Frau Walter, die sich nicht vorstellen kann, wer sich derart für ihren „private[n] Kram“ interessieren könnte, „um das jetzt zu missbrauchen“ (EH5, Tochter, 5,5 Jahre). Herr Schäfer führt seine Haltung auf sein Informatikstudium „zu Beginn des Internets“ zurück, in dessen Kontext das Thema Datenschutz selbstverständlich gewesen sei (EH4, Sohn 4,5 Jahre).

Die Haltung der Familien lässt sich nach der je betroffenen Privatheitsperspektive differenzieren. Die *psychologische Privatheit* wird – auch über Sharenting hinaus – deutlich häufiger angesprochen als die informationelle Privatheit, die eher im Kontext von kommerzieller und institutioneller Privatheit thematisiert wird.[5] Betrachtet man die *informationelle Privatheit*, dann lässt sich festhalten, dass die meisten Eltern über wenig Wissen verfügen, was mit den eigenen Daten passiert. Ausnahmen sind Familien Ziegler, Unger und Witt. Sie thematisieren beispielsweise die Möglichkeit, sich über die Kamera des Tablets zuzuschalten und so Daten sammeln zu können, um über Bilder auf den Aufenthaltsort der Kinder schließen zu können, aber auch, dass „Perverse“ Zugang zu Kinderbildern bekommen könnten (Frau Witt, EH3, Sohn, 3,5 Jahre). Über weiterführendes Wissen über Datengenerierungs- und -verarbeitungsprozesse verfügt – abgesehen von Herrn Schäfer – von den befragten Eltern niemand.

Sehr wohl gibt es aber bei vielen ein Bewusstsein darüber, dass für *kommerzielle* Interessen Daten gesammelt werden. Es geht um personalisierte Werbung oder die Tatsache, dass Daten preisgegeben werden müssen, um online einkaufen zu können. Frau Ritter ist sich dessen bewusst, aber auch skeptisch, ob sie „es hinkriegen kann, das so zu verschleiern, dass die [Firmen] nichts davon mitkriegen“ (EH5, Sohn, 3 Jahre). Die Alltagsbelastungen führen eher dazu, dass die Datenfreigabe bewusst in Kauf genommen wird. Eine Familie ist darüber hinaus bereit, die eigenen Kinder zu Werbezwecken auf die Webseite der eigenen Arbeitsstätte zu stellen (Frau Baumer, EH5, Sohn, 5,5 Jahre). Dass über *WhatsApp* Metadaten an den *Facebook*-Konzern weitergegeben werden, wird von den Eltern kaum thematisiert. Lediglich Familie Schäfer (*Signal*) und Herr Ritter (*Threema*) haben sich für einen alternativen Messenger entschieden.

Auch die *institutionelle Privatheit* spielt für das Familienleben eine Rolle, wenn es um Krippen, Kindergärten oder bei älteren Geschwistern um die

5 Auf Selbstoffenbarung (self-disclosure) und psychologische Privatheit wird im Kapitel über Sharenting noch ausführlich eingegangen werden. An dieser Stelle soll nur festgehalten werden, dass hier eine große Anzahl an Eltern zumindest ein Unbehagen darüber ausdrückt, dass Bilder von den Kindern online kursieren.

Schule geht. Während Frau Brandt sich über die *Facebook*-Seite der Krippe ihres Sohnes freut und lobend erwähnt, dass die Gesichter der Kinder dort nicht zu sehen seien, fühlen sich andere Familien eher in die Einverständniserklärung für die Verwendung der Daten gezwungen. So führt Herr Walter beispielsweise an, dass „jetzt auch immer alles unterschrieben werden“ müsste (EH5, Tochter, 5,5 Jahre) und Frau Lindmüller möchte ihrer älteren Tochter keine Nachteile durch das Verweigern der Unterschrift bescheren (EH5, Tochter, 4,5 Jahre).

4.3 Zwischen Beziehungsarbeit und Shaming: Sharenting

Im Bereich der *interpersonellen Privatheit* spielt vor allem das Sharenting eine Rolle, das für viele Familien bereits zum „Gewohnheitsding“ (Frau Flacher, EH5, Sohn, 4 Jahre) geworden ist, das nicht mehr hinterfragt wird. Was den *Adressat*innenkreis* und den *Kanal* angeht, unterscheiden die Eltern, ähnlich wie in der Studie „Kinder.Bilder.Rechte“ (2018), zwischen *Facebook* und *WhatsApp*. Fast alle Familien lehnen ein Posten von Bildern auf *Facebook* ab. Sie wollen die Kinder „lieber ins Album bringen“ als sie auf *Facebook* für alle „ausstellen“ (Frau Beckmann, EH5, Sohn, 6,5 Jahre). Auch hier steht die Sorge im Vordergrund, nicht kontrollieren zu können, wer das Bild „mal für was verwendet“ (Herr Ziegler, EH4, Tochter, 5 Jahre) und die Kinder später nicht beschämen zu wollen.

Im Gegensatz dazu werden in fast allen Familien Bilder auf *WhatsApp* geteilt. Die Familien unterscheiden hier zwischen den einzelnen Verbreitungsmöglichkeiten. Nur wenige stellen Bilder der Kinder auch in den Status oder nutzen sie als Profilbild. In Bezug auf den Status nahmen zwei Familien kulturelle Unterschiede wahr: Frau Grün und Frau Lindmüller mussten den amerikanischen Cousin bzw. die mexikanische Bekannte darauf hinweisen, doch bitte keine Bilder ihrer Kinder in den eigenen Status zu stellen. Die Familien betonen, dass sie auf *WhatsApp* nur Bilder mit „ganz vertrauenswürdigen Personen“ (Herr Bogner, EH5, Tochter, 6,5 Jahre) teilen. Meist handelt es sich bei den *Adressat*innen* um enge Verwandte oder Freund*innen. Die Eltern gehen dabei davon aus, dass die Bilder nicht weitergegeben werden. Viele sind sich allerdings darüber nicht sicher und vermuten eher, dass „die Bilder nach kurzer Zeit wieder gelöscht werden“ (Frau Färber, EH5, Tochter, 3 Jahre) oder die Großeltern nicht über die notwendige Medienkompetenz verfügen, um sie weiterzugeben. Das Bedürfnis, die Großeltern an der eigenen Lebenswelt teilhaben zu lassen, ist jedoch wichtiger als die Kontrolle über Daten. Besonders gilt dies für herausragende Familienereignisse wie eine Geburt oder den Erfolg ei-

nes Enkelkindes beim Sport. Die *Häufigkeit* variiert dabei von „sehr dezentem" Austausch von Bildern (Frau Beckmann, EH5, Sohn, 6,5 Jahre) bis zum täglichen Update bei Familie Ritter oder Walter.

Was den *Inhalt der geteilten Bilder* angeht, sind sich die Familien einig, dass Badebilder, die die Kinder (halb-)nackt zeigen, unangebracht sind. Wegen eines Bilds auf einem Bagger seien die Kinder dagegen „in zehn oder auch 20 Jahren nicht böse" (Frau Baumer, EH5, Sohn, 5,5 Jahre). Die Eltern wägen also ab, welche Bilder sie mit anderen teilen, sie beziehen aber die Kinder nicht in ihre Entscheidung mit ein und verletzen so deren Recht am eigenen Bild. Wie andere Studien zeigen, haben Kinder mit zunehmendem Alter aber ein Gefühl dafür, welche Bildinhalte für sie in Ordnung sind und möchten hier auch gefragt werden (Kutscher/Bouillon 2018, jugendschutz.net 2019). Gerade in der frühen Kindheit ist es wichtig, dass die Eltern ihr Elternprivileg hier nicht leichtfertig auslegen.

4.4 Klare Vorbilder sind gefragt: Medienerzieherisches Handeln zum Thema Datenschutz

Viele der befragten Eltern sehen bei ihren Kindern (noch) keinen Handlungsbedarf (vgl. Kutscher/Bouillon 2018) und thematisieren Datenschutz und Privatheit eher im Kontext der Smartphonenutzung von verwandten oder befreundeten Jugendlichen. Vereinzelt überlegen die Eltern, wie sie später mit der Privatsphäre ihrer Kinder umgehen wollen. Dass ihre Kinder bereits eigenständig Internetangebote nutzen und so Daten weitergeben, wenn sie beispielsweise *YouTube* nutzen, mit der Oma auf *WhatsApp* videotelefonieren oder Sprachassistenzsysteme benutzen, ist kaum einem Elternteil bewusst. In den Familien mit Sprachassistenzsystemen sorgen sich die Mütter eher darum, dass die Kinder hier einen Befehlston lernen (Frau Baumer, EH1, Sohn, 3,5 Jahre) bzw. sprechen in einem Atemzug von Datenschutz, während sie *Alexa* darum bitten, die Musik leiser zu stellen (Frau Huber, EH5, Sohn, 3,5 Jahre).

Regeln werden den Kleinkindern in Bezug auf Datenschutz und Privatheit kommunikativ (noch) nicht vermittelt und beziehen sich stattdessen eher auf das elterliche Medienhandeln, beispielsweise darauf, keine Kinderbilder online zu posten. In einigen Familien gilt die eingeschränkte Regel, nur „unbedenkbare [Bilder] von hinten" (Herr Bogner, EH5, Tochter, 6,5 Jahre) online zu stellen. Einige Eltern handeln aus, welche Inhalte von den Kindern online gestellt werden können. Dass die Eltern mit ihrem Medienhandeln im Bereich Datenschutz und Privatheit den Kindern als Vorbild dienen, ist nur den wenigsten bewusst, ebenso wenig ihre Treu-

händer*innenschaft (vgl. Naab 2019). Dies mag auch daran liegen, dass die Kinder das Handeln der Eltern mit Bezug auf Privatheitsfragen – anders als einen achtsamen Umgang mit den Geräten – schlechter wahrnehmen können und die Vorbildrolle deshalb kommunikativ hergestellt werden müsste.

Privatheit und Datenschutz sind zudem innerhalb der Medienerziehung nur ein Thema unter vielen und im Familien-Medien-Monitoring deutlich weniger präsent als in quantitativen Befragungen zur Medienerziehung (vgl. z.B. DIVSI 2015) oder zu elterlichem Jugendmedienschutz (Brüggen et al. 2017). Für die Mehrheit der Familien haben sie nicht den gleichen Stellenwert wie beispielsweise Fragen nach einer altersgerechten Nutzung oder nach Medienwirkungen. Nur Frau Unger und Frau Schäfer formulieren Privatheit und Datenschutz explizit als Erziehungsziel („da muss man halt aufpassen, was man macht oder was man postet, was man öffentlich macht“, Frau Unger, EH5, Tochter, 4 Jahre). Bei den anderen Familien dominiert der Wunsch, ein „gesundes Mittelmaß“ zu finden (Frau Grün, EH5, Tochter, 3 Jahre), den Umgang mit Technik zu lernen bzw. den Kindern das notwendige Wissen zu vermitteln, um Selbstoptimierungsansprüche bzw. Informationen einordnen und bewerten zu können.

Die Eltern sorgen sich zum Teil um das Wohl ihrer Kinder, wenn sie über Shaming oder die Tatsache reflektieren, dass „das Internet [nichts] vergisst“ (Frau Witt, EH3, Sohn, 3,5 Jahre), haben aber nicht die Rechte der Kinder im Blick. Diese werden nicht thematisiert. Frau Durr erwähnt stattdessen explizit, dass die Kinder in der frühen Kindheit noch nicht über die kognitiven und emotionalen Fähigkeiten verfügen würden, um die Folgen der Weitergabe von Daten verarbeiten zu können (EH3, Tochter, 3,5 Jahre).

4.5 Typologie: Relevanz des Themas Privatheit in der Erziehung

Basierend auf der Relevanz des Themas Privatheit und dem medienerzieherischen Handeln zum Datenschutz wurde eine Typologie gebildet, um herauszuarbeiten, wovon es abhängt, ob die Eltern über Datenschutz nachdenken und dies sogar in ihr medienerzieherisches Handeln integrieren (vgl. zum methodischen Vorgehen Kapitel 3). Typologisierungskriterien waren dabei die Relevanz, die Eltern dem Thema Datenschutz und Privatheit (hoch vs. niedrig) zuschreiben und ob sie die Relevanz des Themas auch in eigene medienerzieherische Maßnahmen umsetzen (ja vs. nein). Aus dem Material ließen sich drei Typen ableiten (vgl. Abb. 2).

Abbildung 2: Typologie Privatheit in der Medienerziehung

Relevanz/Umsetzung	Umsetzung in medienerzieherisches Handeln	keine Umsetzung in medienerzieherisches Handeln
Datenschutz wird als relevantes Thema erkannt	Die Konsequenten	Die Pragmatischen
Datenschutz wird nicht als relevantes Thema erkannt	*Im Sample nicht vertreten*	Die Sorglosen

Typ 1: Die Konsequenten

Neun Familien reflektieren ihr eigenes Medienhandeln und beziehen auch Privatheitsaspekte mit ein. Diese Familien verfügen über Wissen, was informationelle Privatheit angeht. Kinderbilder werden zwar auf Messengern mit der (Groß-)Familie geteilt, dabei wird aber stark nach Kontexten differenziert (wem wird welches Bild geschickt) und darauf geachtet, die Kinder nicht zu kompromittieren. Die Eltern unterscheiden dabei sowohl den Kanal als auch die Inhalte und die Häufigkeiten des Sharentings, teilen Fotos eher selten und nur bei besonderen Anlässen. Darüber hinaus fällt auf, dass das Thema Datenschutz und Privatheit in diesen Familien mit den Großeltern, den älteren Geschwistern oder zwischen den Eltern kommunikativ ausgehandelt wird. So hat Frau Unger bereits mit den älteren Geschwistern über die Folgen von öffentlichen Bildern gesprochen und Frau Ziegler mit ihrem Mann sowie Herr Bogner mit der Großmutter ausgehandelt, dass keine Bilder der Kinder auf *Facebook* gepostet werden. Die Eltern sehen sich zum Teil dabei auch als Vorbilder für die Kinder. Einen Sonderfall stellt Familie Schäfer dar, die über sehr explizites Wissen über Datenschutz verfügt und auch gesellschaftliche Folgen mitdenkt und diskutiert.

Die Mütter dieses Typs arbeiten häufig in sozialen Berufen, die Väter kommen zum Teil aus der Informatik und der Pädagogik. Die Kinder sind tendenziell schon älter und haben häufig ältere Geschwister. Anders als bei den anderen beiden Typen nutzen die Kinder bereits häufiger eigenständig Apps wie *YouTube* auf mobilen Geräten. Smarte Geräte wie Smartwatches oder Smart-TV sind eher selten. Was die Vorbildfunktion betrifft, machen sich die Eltern vor allem Gedanken um den „Aufmerksamkeitsschlucker Smartphone “ (Herr Bogner, EH1, Tochter, 4 Jahre), sehen ihre eigene Mediennutzung kritisch und legen auf alternative Tätigkeiten der Kinder Wert.

Typ 2: Die Pragmatischen

Diese fünf Eltern haben ein Problembewusstsein, was Datenschutz und Privatheit angeht und erkennen, dass sie Daten angeben müssen, wenn sie online aktiv sein wollen. Sie ergreifen aber nicht die entsprechenden Maßnahmen, um ihre Daten zu schützen bzw. verfügen nicht über die technischen Kenntnisse. Andere Bedürfnisse stehen im Vordergrund. Dies betrifft zum einen – auf der interpersonellen Privatheitsebene – das Verbundensein mit anderen Familienmitgliedern. Auf der kommerziellen Ebene geht es darum, sich den Alltag zu vereinfachen, indem Anfragen über *Alexa* gestellt werden oder beim Online-Shopping bewusst in Kauf genommen wird, dass die eigenen Daten dort gespeichert werden. Anders als bei den *Sorglosen* (vgl. Typ 3), findet bei den *Pragmatischen* Kommunikation über das Thema Datenschutz und Privatheit nur reaktiv statt, wenn beispielsweise Großeltern sich zu viele Rechte herausnehmen oder man sich an die Praxis der anderen Familienmitglieder anpasst. Frau Ritter überlegt zwar im Interview immer wieder, ob sie anders handeln könnte. Ihr fehlt aber – ähnlich wie den anderen Mitgliedern dieses Typs – eine Idee für Alternativen und damit ein Handlungswissen, das über reine Privatsphäreeinstellungen hinausgeht. Zu diesem Typ gehören eher Familien mit jüngeren Kindern (zu Beginn des Panels ein Jahr alt), die Eltern sind höher gebildet, die Mütter arbeiten alle, zum Teil auch in Vollzeit, darunter eine Journalistin und eine Lehrerin. Die Medienausstattung ist sehr umfangreich und es gibt einige Haushalte, in denen die Väter sich gerne mit den neuesten Geräten ausstatten. Auffällig ist, dass die Kinder in ihrer Mediennutzung sehr viel Musik hören, häufig Musikvideos auf *YouTube* sehen und mit den Großeltern zum Teil schon videotelefonieren. Anders als bei den *Konsequenten*, erleben die befragten Mütter ihre Vorbildrolle positiv und beziehen diese vor allem auf einen bewussten und reduzierten Umgang mit dem Smartphone.

Typ 3: Die Sorglosen

Drei Familien kennen das Thema Datenschutz und Privatheit, es ist aber für sie nicht handlungsrelevant – weder für das eigene Medienhandeln noch für die Medienerziehung. Darüber hinaus verfügen sie über wenig privatheitsbezogenes Wissen. Frau Walter kann als Reisekauffrau die „deutsche Angst vor Online-Buchungen“ nicht nachvollziehen, sie habe „immer gute Erfahrungen gemacht“ (Frau Walter, EH4). Insbesondere was die kommerzielle Privatheit angeht, gehen diese Eltern bewusst Risiken ein, stellen unter anderem das eigene Kind auf die berufliche Webseite zu Werbezwecken und missachten so die Kinderrechte. Diese Familien stehen

viel mit anderen in Kontakt und teilen regelmäßig Fotos der Kinder online. Die Kinder sind in diesem Typ alle älter (zu Beginn drei Jahre alt) und haben meist ältere Geschwister. Die Mütter arbeiten und haben in ihren Berufen online mit Daten oder Werbung zu tun. Die Medienausstattung unterscheidet sich in den Familien nicht explizit von anderen. Die Kinder dürfen bereits mit älteren Geschwistern oder Nachbarn an der Konsole spielen. In ihrer eigenen Vorbildrolle sind diese Eltern unsicher und können sie weniger als die anderen Typen an einem konkreten (eigenen) Medienverhalten festmachen.

Einflussfaktoren auf das Privatheitsverhalten

Was beeinflusst nun aber, ob die Familien eher konsequent, pragmatisch oder sorglos im Umgang mit den Daten sind?

- **Medienensemble zuhause**: Hier fällt auf, dass die *Pragmatischen* sehr an Technologie interessiert sind und sich gerne mit den neuesten Geräten ausstatten. In diesem Typ finden sich deshalb auch deutlich mehr Smartgeräte als beispielweise bei den *Konsequenten*.
- **Beruf**: Unter den *Konsequenten* finden sich einige Informatiker, ein Pädagoge, der bereits beim Film gearbeitet hat und eine Rechtsanwaltsgehilfin. Sie haben berufsbedingt einen anderen Blick auf Datenschutz als die *Sorglosen*, die ebenso wie *die Pragmatischen* eine Faszination für Technik mitbringen, aber über Datenentstehungs- und -verwertungsprozesse nicht Bescheid wissen.
- **Alter der Kinder**: Unter den *Pragmatischen* sind nur Kinder, die zu Beginn ein oder zwei Jahre alt waren und noch wenig eigenständig digitale Medien nutzen, dafür aber bereits mit den Großeltern über Videotelefonie in Kontakt sind. Hier stellt sich auch die Frage, ob die *Pragmatischen* nicht auch aufgrund der Alltagsbelastung mit sehr kleinen Kindern Datenschutzfragen zurückstellen (müssen). Werden die Kinder älter und weitet sich ihr Nutzungsspektrum aus, reagieren die Eltern entweder mit Vorsicht (die *Konsequenten*) oder machen sich (weiterhin) keine Gedanken über Datenschutz und Privatheit (die *Sorglosen*).
- **Ziele der Medienerziehung:** Die *Konsequenten* sind die einzigen, die zumindest zum Teil Datenschutz und Privatheit als Ziel ihrer Medienerziehung definieren. Sie setzen es dabei neben aktive Gestaltungsmöglichkeiten mit den Medien. Da sie hier das selbstständige Handeln der Kinder in den Vordergrund rücken, werden Aspekte, die sie dabei schützen, wichtiger. Anders dagegen die *Pragmatischen*: Sie kritisieren vor allem den Konsum- und Selbstoptimierungsaspekt der Medien und wollen die Kinder darauf vorbereiten. Interessanterweise nehmen sie

aber in Kauf, dass beim Konsum eigene Daten weitergeben werden. Die *Sorglosen* haben dagegen noch keine Ziele, wenn es um die Medienerziehung geht und verschieben das Thema auf das Schulalter. Hier lässt sich deutlich sehen, wie wichtig es ist, das eigene medienerzieherische Handeln auf Basis der damit verbundenen Ziele zu reflektieren. Wer Ziele benennen kann, kann diese auch ins eigene Handeln integrieren.

5. Fazit

Datenschutz und Privatheit sind Themen, die Eltern von Kindern im Alter von null bis sechs Jahren nicht fremd sind. Sie wünschen sich, dass die Daten, die sie im Rahmen ihrer Mediennutzung von sich selbst oder von ihren Kindern preisgeben, sicher sind und nicht missbraucht werden. Wie sie selber dazu beitragen können, welche technischen Sicherheitsvorkehrungen sie vornehmen können und welche Maßnahmen in ihrem alltäglichen Medienhandeln wie auch im Rahmen ihrer Medienerziehung zielführend sind, ist vielen Eltern nicht bewusst. Den Schutz ihrer eigenen und der Daten ihrer Kinder überlassen viele Eltern anderen und zeigen dabei zum Teil eine fatalistische und resignative Haltung. Zum Ziel ihrer Medienerziehung machen Eltern den sicheren und verantwortungsbewussten Umgang mit Daten – eigenen und fremden – dann, wenn sie das Thema selbst als Herausforderung sehen und es sogar Einzug in ihre normativen Vorstellungen von Medienerziehung gefunden hat (*die Konsequenten*). Voraussetzung dafür ist, dass sie über ein ausführliches Medienstrukturwissen verfügen bzw. sich – beispielsweise ausgelöst durch Medienberichterstattung oder andere Personen – bereits mit dem Thema auseinandergesetzt haben. Dabei geht es weniger um die Mediennutzung der Kinder, sondern stärker um die elterliche Wahrnehmung von Medienerziehung und die eigenen Ansprüche (vgl. Eggert 2019: 111). Mit Blick auf eine Stärkung der elterlichen Medienerziehungskompetenz gilt es vor diesem Hintergrund, Eltern die Bedeutung, die sie für ihre Kinder als Vorbilder sowie als wichtigste Ansprechpersonen haben, ins Bewusstsein zu rufen.

Literatur

Akremi, Leila (2014): *Stichprobenziehung in der qualitativen Sozialforschung*. In: Baur, Nina / Blasius, Jörg (Hg.): Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: VS Verlag, S. 265–282.

Autenrieth, Ulla (2014): *Die ‚Digital Natives' präsentieren ihre Kinder – Eine Analyse der zunehmenden (Selbst-) Visualisierung von Familie und Kindheit in Onlineumgebungen.* In: Studies in Communication Sciences 10 (35), S. 99-107.

Barassi, Veronica (2018): *The child as datafied citizen. Critical questions on data justice in family life*. In: Mascheroni, Gianna / Ponte, Cristina / Jorge, Ana (Hg.): Digital parenting. The challenges for families in the digital ages. Göteborg: Nordicom, S. 93-102.

Braun, Max / Trepte, Sabine (2017): *Privatheit und informationelle Selbstbestimmung: Trendmonitor zu den Einstellungen, Meinungen und Perspektiven der Deutschen*. Stuttgart: Universität Hohenheim.

Brosch, Anna (2016): *When the child is born into the Internet: Sharenting as a growing trend among parents on Facebook.* In: The New Educational Review 43 (1), S. 225-234.

Brosch, Anna (2018): *Sharenting – why do parents violate their children's privacy?* In: The New Educational Review 54 (4), S. 75-85.

Brüggen, Niels / Dreyer, Stephan / Drosselmeier, Marius / Gebel, Christa / Hasebrink, Uwe / Rechlitz, Marcel (2017): *Jugendmedienschutzindex: Der Umgang mit onlinebezogenen Risiken – Ergebnisse der Befragung für Eltern und Heranwachsenden. Herausgegeben von FSM – Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.* Online verfügbar unter: www.fsm.de/jugendmedienschutzindex (Abfrage am: 16.04.2020).

Brüggen, Niels / Wagner, Ulrike (2017): *Recht oder Verhandlungssache? Herausforderungen für die informationelle Selbstbestimmung aus Perspektive der Jugendlichen*. In: Friedewald, Michael / Lamla, Jörn / Roßnagel, Alexander (Hg.): Informationelle Selbstbestimmung im digitalen Wandel (DuD-Fachbeiträge), Wiesbaden: VS Verlag, S. 131-146.

Burgoon, Judee K. (1982): *Privacy and Communication*. In: Communication Yearbook 6 (1), S. 206–249.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (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)*. Online verfügbar unter: https://www.divsi.de/wp-content/uploads/2015/06/U9-Studie-DIVSI-web.pdf (Abfrage am: 24.3.2019).

Eggert, Susanne / Wagner, Ulrike (2016): *Grundlagen zur Medienerziehung in der Familie. Expertise im Rahmen der Studie MoFam – Mobile Medien in der Familie.* Online verfügbar unter: www.jff.de/studie_mofam (Abfrage am: 7.05.2020).

Eggert, Susanne (2019): *Familiäre Medienerziehung in der Welt digitaler Medien: Ansprüche, Handlungsmuster und Unterstützungsbedarf von Eltern*. In: Fleischer, Sandra / Hajok, Daniel (Hg.): Medienerziehung in der digitalen Welt. Grundlagen und Konzepte für Familie, Kita, Schule und Soziale Arbeit. Stuttgart: Kohlhammer, S. 105-118.

jugendschutz.net (2019): *Report. Kinderbilder auf Instagram. Wann werden Persönlichkeitsrechte von Kindern verletzt?* Online verfügbar unter: https://www.servicestelle-jugendschutz.de/wp-content/uploads/sites/17/2019/10/Report_Kinderbilder_auf_Instagram.pdf (Abfrage am: 16.4.2020).

Kluge, Susanne (2000): *Empirically Grounded Construction of Types and Typologies in Qualitative Social Research.* Forum Qualitative Research 1 (1). Online verfügbar unter: http://www.qualitative-research.net/index.php/fqs/article/view/1124/2500 (Abfrage am: 16.04.2020).

Kutscher, Nadia (2019): *Kinder. Bilder. Rechte. Wie Kinderrechte in der digitalen Welt durch die Eltern alltäglich und ungewollt beeinträchtigt werden*. In: Frühe Kindheit 22 (2), S. 6-13.

Kutscher, Nadia / Bouillon, Ramona (2018): *Kinder. Bilder. Rechte. Persönlichkeitsrechte von Kindern im Kontext der digitalen Mediennutzung in der Familie*. Berlin: Schriftenreihe des Deutschen Kinderhilfswerks Heft 4.

Livingstone, Sonia / Stoilova, Mariya / Nandagiri, Rishita (Hg.) (2019): *Children's data and privacy online. Growing up in a digital age. An evidence review.* Online verfügbar unter: http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf (Abfrage am: 09.11.2019).

Meyen, Michael / Löblich, Maria / Pfaff-Rüdiger, Senta / Riesmeyer, Claudia (2019): *Qualitative Forschung in der Kommunikationswissenschaft. Eine praxisorientierte Einführung (2).* Wiesbaden: Springer VS.

Naab, Thorsten (2019): *Parents' online self-disclosure and parental social media trusteeship. How parents manage the digital identity of their children.* In: Medien Pädagogik Zeitschrift für Theorie und Praxis der Medienbildung (35), S. 97–115. Online verfügbar unter: https://www.medienpaed.com/article/view/656 (Abfrage am: 24.03.2020).

Oberlinner, Andreas / Eggert, Susanne / Schubert, Gisela / Jochim, Valerie / Brüggen, Niels (2018): *Medienrituale und ihre Bedeutung für Kinder und Eltern. Erster Bericht der Teilstudie „Mobile Medien und Internet im Kindesalter – Fokus Familie“*. München: JFF – Institut für Medienpädagogik in Forschung und Praxis. Online verfügbar unter: www.jff.de/mofam (Abfrage am: 16.04.2020).

Schier, Michaela (2013): *Räumliche Entgrenzungen – Multilokales Familienleben*. In: Wagner, Ulrike (Hg.): Familienleben: Entgrenzt und vernetzt?! München: Kopaed Verlag, S. 39-55.

Schlör, Katrin (2019): *Doing Family mit Medien. Impulse für eine lebenslange medienpädagogische Familienbildung*. In: Akademie der Diözese Rottenburg- Stuttgart (Hg.). Im Dialog. Beiträge aus der Akademie der Diözese Rottenburg-Stuttgart. Aufwachsen mit Medien – Mediensozialisation und -kritik heute (41. Stuttgarter Tage der Medienpädagogik) o.Jg. (1), S. 7-22.

Schorb, Bernd / Theunert, Helga (2000): *Kontextuelles Verstehen der Medienaneignung*. In: Paus-Hasebrink, Ingrid / Schorb, Bernd (Hg.): Qualitative Kinder- und Jugendforschung. Theorien und Methoden: Ein Arbeitsbuch. München: Kopead. Verlag, S. 33-57.

Siibak, Andra / Traks, Keily (2019): *The dark sides of sharenting*. In: Catalan Journal of Communication & Cultural Studies 11 (1), S. 115-121.

Stapf, Ingrid (2019): *„Ich sehe was, was du auch siehst". Wie wir die Privatsphäre der Kinder im Netz neu denken sollten und was Kinder möglicherweise dabei stärkt – ein kinderrechtlicher Impuls.* In: Frühe Kindheit 22 (2), S. 14-23.

Stein, Petra (2014): *Forschungsdesigns für die quantitative Sozialforschung*. In: Baur, Nina / Blasius, Jörg (Hg.): Handbuch Methoden der empirischen Sozialforschung. Wiesbaden: Springer VS, S. 135-151.

UNICEF (2017): *The State of The World's Children: Children in a Digital World 2017.* Online verfügbar unter: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf (Abfrage am: 10.04.2020).

Wagner, Ulrike / Eggert, Susanne / Schubert, Gisela (2016): *MoFam – Mobile Medien in der Familie. Langfassung der Studie*. Online verfügbar unter: https://www.jff.de/fileadmin/user_upload/jff/projekte/mofam/JFF_MoFam1_gesamtStudie.pdf (Abfrage am: 10.04.2020).

Walper, Sabine / Maywald, Jörg (2019): *Editorial.* In: Frühe Kindheit 22 (2), S. 3.

Wachsame Maschinen. Freiräume und Notwendigkeit der Verantwortungsübernahme bei der Entwicklung sozialer Roboter und deren Integration in Bildungsinstitutionen.

Ricarda T.D. Reimer und Silvan Flückiger

Abstract

Dieser Beitrag führt in das Thema „Soziale Robotik in der Bildung" ein und beleuchtet dabei insbesondere medienpädagogisch relevante Dimensionen eines sinnvollen wie kritischen Umgangs mit sozialen humanoiden Robotern. Im Mittelpunkt stehen dabei soziale Roboter als komplexe Phänomene: Sie als Interaktionspartner, Lernbegleiter in Lehrveranstaltungen, aber auch als Projektionsflächen menschlicher Sehnsüchte, Ängste und Zukunftsvorstellungen zu reflektieren, ist Auftrag einer kritisch-reflexiven Medienbildung auf allen Bildungsstufen. Was aber ist ein dem heutigen Erkenntnisstand angemessener und ethisch vertretbarer Einsatz von Robotern in Bildungsinstitutionen? Grundlage dieses Beitrags sind aktuelle Forschungstätigkeiten der Fachstelle Digitales Lehren und Lernen in der Hochschule im Rahmen verschiedener Projekte im Feld „Roboter und Bildung" an der Fachhochschule Nordwestschweiz.[1]

1. Einleitung

„Social robots have, in the broadest sense, the potential to become part of the educational infrastructure, just as paper, white boards, and computer tablets have" (Belpaeme et al. 2018: 7). Folgt man Belpaemes Annahme, sehen sich Bildungsverantwortliche möglicherweise bald schon vor der Herausforderung, eine technische Innovation in die Lehre zu integrieren, welche in Bezug auf ihr Bildungspotential, die Effizienz der von ihr initi-

1 Einbezogen werden auch damit verbundene Reflexionen in der Fachstelle sowie Ergebnisse der Podiumsdiskussion am Forum Privatheit vom 20.–22. November 2019 in Berlin mit den Beteiligten Isabel Zorn, Ricarda T.D. Reimer und Silvan Flückiger.

ierten Lernprozesse, den mediendidaktisch sinnvollen Einsatz und den Persönlichkeitsschutz von Lehrenden und Lernenden viele Fragen offenlässt.

Als soziale und humanoide Roboter[2] interagieren Roboter in direktem Kontakt mit Menschen und nach menschlichem Vorbild. Eine wachsende Zahl an Labor- und Feldstudien weisen den Robotern in Vermittlungsprozessen im weitesten Sinne „pädagogische" Rollen zu (Belpaeme et al. 2018). Auch wenn ihre technischen Limitationen (noch) offensichtlich sind[3], zeigen sich bereits das Lernen unterstützende affektive wie kognitive Effekte (Belpaeme et al. 2018). So sind Roboter als Lernbegleiter beispielsweise in der Lage, die Aufmerksamkeit von Lernenden länger aufrecht zu erhalten.[4] Um von solchen Effekten profitieren zu können, erfordert der Einsatz eine sorgfältige didaktische Planung und stellt damit Anforderungen an die (medien-)pädagogischen Kompetenzen von Lehrenden. Dies schließt eine Beschäftigung mit ethischen Problemfeldern, welche dem Einsatz sozialer Roboter in Bildungsinstitutionen stets vorgelagert sein sollte, dringend mit ein. In diesem Kontext wird nach den Gestaltungsmöglichkeiten wie auch nach der Verantwortung der Pädagogik bei der Integration sozialer Roboter in Bildungsinstitutionen gefragt. Eine offene und zugleich kritische Auseinandersetzung mit diesen Maschinen erfordert eine vertiefte Beschäftigung – nicht nur mit der technologischen Seite des Phänomens Roboter, sondern auch mit seiner kulturellen, historischen, ökonomischen, gesellschaftlichen oder philosophischen Dimension.

1.1 (Forschungs-)Gegenstand soziale Roboter

Soziale Roboter zeichnen sich durch wachsende Autonomie im Bereich Spracherkennung, -verarbeitung und -ausgabe, Bewegung und Entscheidungsfähigkeit aus. Ein humanoides Aussehen und Formen künstlicher In-

2 „Sozial" heißt in diesem Kontext, dass die Roboter in der Mensch-Roboter-Interaktion Verhalten zeigen, das sich am menschlichen Sozialverhalten orientiert. Im Folgenden werden wir uns auf die Bezeichnung «sozialer Roboter» oder nur «Roboter» beschränken, meinen damit aber stets Roboter, welche in sozialen Interaktionen eingesetzt und humanoid (auch: anthropomorph) gestaltet werden.

3 Yang et al. (2018) liefern eine Übersicht über aktuelle technische Herausforderungen in der Entwicklung sozialer Roboter.

4 Inwiefern diese Effekte auch auf Dauer messbar sind, müssen Längsschnittstudien aufzeigen, welche allerdings noch nicht realisiert sind.

telligenz verleihen ihnen den Anschein von Kognition und Emotion. Dies ist letztlich der Grund, warum sie für den Einsatz in der realen Lebenswelt der Anwender*innen in Frage kommen. Warum aber werden Roboter für den Einsatz im Klassenzimmer oder an den Hochschulen entwickelt? Welchen pädagogischen Aufgaben, Rollen und Herausforderungen sollen sich diese Maschinen zuwenden?

Auf einer übergeordneten Ebene sieht Michael Decker in den Entwicklungen im Bereich der Sozialrobotik einen Versuch der Verwirklichung eines alten „Menschheitstraums" (Decker 2010: 46), der darin besteht, den Menschen mit Hilfe der Technik nachzubauen oder ihn gar zu überwinden. Auch Käte Meyer-Drawe deutet die Roboterentwicklungen in ähnlicher Weise: „Die Auseinandersetzung mit der eigenen Vergänglichkeit ist eines der vorherrschenden Motive in der Selbstverfolgung des Menschen mit Hilfe seiner Maschinen" (Meyer-Drawe 2007: 31). Daneben bietet die Entwicklung humanoider Roboter aber auch Möglichkeiten eines Lernens vom Menschen für den Menschen: Die technische Rekonstruktion menschlicher Organe oder Verhalten ermöglicht sowohl Erkenntnisse zum Beispiel im Bereich der künstlichen Intelligenz als auch ein besseres Verstehen menschlichen Denkens und Handelns (Decker 2010: 47). Die humanoide Gestaltung der Roboter ist weiter als eine Mittel-Zweck-Relation zu deuten: Humanoides Aussehen und Verhalten erleichtern die Interaktion für beide, Mensch und Roboter (z.B. beim Antizipieren von Bewegungen). Roboter sammeln in der Interaktion mit Menschen nützliche Informationen, um sich in deren Verhalten „einzuüben" (Breazeal 2003). Was ein Vorteil für den Roboter ist, muss nicht zwangsläufig ein Vorteil für den Menschen sein. Wo entstehen Mehrwerte für das lernende Subjekt bei der Entwicklung humanoider Maschinen?

Aktuelle Studien im Bereich der Pädagogik gehen davon aus, dass Roboter zukünftig Lehrkräfte entlasten und neue Lernerlebnisse ermöglichen können (u.a. Belpaeme et al. 2018). Forschung und Entwicklung konzentrieren sich dazu auf den Vor- und Primarschulbereich (Belpaeme et al. 2018). Dabei sind die am häufigsten ausgeführten Aufgaben der Roboter das Vermitteln von Lerninhalten an Gruppen und in 1:1-Settings sowie das Fördern der Aufmerksamkeit und der Motivation. Dementsprechend nehmen Roboter in Lehr-/Lernszenarien unterschiedliche Funktionen ein, die sich aber alle an pädagogischen Rollen orientieren. In der Rolle des Lehrenden, Assistenten oder des Tutors vermitteln Roboter Wissen. Dies können konkrete curriculare Inhalte (Causo et al. 2017) oder Inhalte mit stärkerem Unterhaltungscharakter sein (Kory Westlund et al. 2017). Im Hoch-

schulprojekt H.E.A.R.T[5] wird ein Blended-Learning-Format (Flipped Classroom) von einem Roboter in der *Rolle des Lehrenden* unterstützt (Weber/Zeaiter 2018). In der *Rolle des Student-Peers[6] oder Lernbegleiters* steht die Vermittlung von Lerninhalten, das Führen und Motivieren von Lernenden in einem 1:1-Setting im Vordergrund. In der *Rolle des Neulings* bietet der Roboter den Lernenden die Chance auf einen Rollenwechsel (Lernen durch Lehren), beispielsweise beim Erlernen der Handschrift (Hood et al. 2015). Als „Neuling" kann der Roboter auch von Grund auf, oder für ein bestimmtes Einsatzszenario, programmiert werden.

1.2 Lehren und Lernen mit Robotern

Die humanoide Gestaltung von Aussehen und Verhalten wirken sich auch auf das Lernen selbst aus: Belpaeme et al. (2018) fragen in ihrer Untersuchung von 309 empirischen Einzelstudien nach den Effekten sozialer Roboter auf das Lernen, nach dem Einfluss der Gestaltung und nach den Rollen in pädagogische Kontexten. Dabei stellen sie fest, dass Roboter das Lernen und insbesondere das Erleben der Lernsituation positiv beeinflussen können. Geweckte Neugier oder erhöhte Motivation, sich mit einem Problem zu befassen, kann Verstehen begünstigen, muss es aber nicht: „Furthermore, positive affective outcomes did not imply positive cognitive outcomes, or vice versa." (Belpaeme et al. 2018: 4) In der Metastudie widmen sich die Autor*innen auch dem vielerorts aufgeführten Vergleich zwischen einem physisch anwesenden Roboter und virtuellen Lernhilfen (auch Bots). Hier zeigt sich, dass die Präsenz des Roboters das Gegenüber zu lernförderlichen sozialen Handlungen motiviert (antworten, Fragen stellen etc.). Die Studie zeigt auf, dass mit anwesenden Robotern auch die besseren Lernergebnisse im Vergleich zu virtuellen Lernhilfen erzielt werden können (Belpaeme et al. 2018).

Beim Einsatz als Student-Peer wurde festgestellt, dass die Aufmerksamkeit von Lernenden über längere Zeit aufrechterhalten werden konnte (Belpaeme et al. 2018). Ebenfalls scheint hier ein personalisiertes Verhalten positive Effekte auf das Lernen zu haben (Baxter et al. 2017). Die Effekte in der jeweiligen pädagogischen Interaktion und deren Auswirkungen auf

5 **H**umanoid **E**motional **A**ssistant **R**obots in **T**eaching (H.E.A.R.T). Ein Projekt der Universität Marburg unter der Leitung von Prof. Dr. Jürgen Handke.

6 Die Bezeichnung Student-Peer bezieht sich sowohl auf Schüler*innen wie auch auf Studierende.

die Qualität des Lernens werden durch Faktoren wie das simulierte Geschlecht des Roboters (Reich-Stiebert/Eyssel 2015) oder die Emotionalität der Sprache und Gestik beeinflusst (Kory Westlund et al. 2017). Kennedy, Baxter und Belpaeme (2015) zeigen zudem, dass ein simuliertes, gesteigertes soziales Verhalten des Roboters (z.B. Gestik) für das menschliche Gegenüber auch überfordernd und dadurch nicht mehr lernförderlich sein kann (z.B. weil es die Lernenden ablenkt).

Wie wichtig die Erforschung von (Lern-)Effekten ist, wird vor dem Hintergrund der in der Literatur formulierten Erwartungen an Roboter deutlich (beispielhaft Belpaeme et al. in Bezug auf eine individuelle Betreuung von Lernenden):

> „A social robot has the potential to deliver a learning experience tailored to the learner, supporting and challenging students in ways unavailable in current resource-limited educational environments. Robots can free up precious time for human teachers, allowing the teacher to focus on what people still do best: providing a comprehensive, empathic, and rewarding educational experience" (Belpaeme et al. 2018: 7).

Doch können Roboter solchen Zukunftsbildern überhaupt gerecht werden? Welche Herausforderungen und offenen Fragen stehen zwischen aktuellen Robotermodellen und der Vorstellung einer robotergestützten Pädagogik?

1.3 Offene Fragen und ethische Bedenken

Die Integration von Robotern in Bildungskontexten wirft angesichts der benannten Einsatzgebiete, vorgesehenen Aufgaben und Rollen eine Reihe ethischer Fragen auf. Humanoid gestaltete und in soziale Interaktionen eingebettete Roboter sind in der Lage, menschliches Verhalten nicht nur zu interpretieren, sondern dieses auch gezielt oder unbeabsichtigt durch ihr Design und ihre technischen Möglichkeiten zu verändern: Siebert et al. (2019) diskutieren in diesem Zusammenhang Roboter, deren Potentiale und Risiken als «persuasive technology». Vollmer et al. (2018) weisen beispielsweise darauf hin, dass mehrere Roboter zusammen Gruppenmeinungen entwickeln, und Kinder so unter Druck setzen könnten. Amanda J. C. Sharkey (2016) entfaltet die folgenden Problemfelder mit Blick auf Roboter im schulischen Unterricht: Bindung (attachment), Täuschung (deception), Verlust menschlicher Kontakte (loss of human contact), Datenschutz (privacy), Kontrolle (control) und Verantwortung (accountability). Die

Problemfelder, die in Lehr-/Lern-Szenarien besonders zu beachten sind, werden im Folgenden kurz vorgestellt und ergänzt.

Menschen gehen *Bindungen* mit Mitmenschen ein, können sich aber auch an Objekte wie Maschinen emotional binden. Doch wie wirken sich solche Bindungen auf den Menschen und insbesondere auf Heranwachsende aus?

> „[T]his would open the possibility of the children adopting the robot's apparent values, and as in the case of the robot companion, basing their social skills and world outlook on the behaviour and apparent attitudes of a machine rather than on a living, breathing, empathising human" (Sharkey 2016: 291).

Zentrales und aus ethischer Sicht problematisches Element ist dabei die *Täuschung*. Als Lebendigkeit simulierende Maschinen bedienen sich die programmierten Roboter dem Mittel der Täuschung, um vorgegebene Ziele zu erreichen (z.B. eine vertraute Lernatmosphäre zu gestalten). Sharkey macht im Zusammenhang mit Täuschung zudem darauf aufmerksam, dass von Robotern eine Gefahr ausgehen kann, wenn diese die Illusion wecken, über ein Sein oder Fähigkeiten zu verfügen, die sie in Wirklichkeit nicht haben. Das könnte Menschen dazu verleiten, Roboter für Aufgaben einzusetzen, für die sie nicht geeignet sind. Maschinen, die emotionale Betroffenheit zeigen oder Freundschaften anbieten, vermischen die Kategorien lebendig und maschinenhaft zwar nur scheinbar, sie machen es Menschen jedoch leicht, sich auf das „Spiel" mit dem scheinbar Lebendigen einzulassen – und sich in diesem Spiel zu verlieren, insbesondere dann, wenn sich der Roboter dem Kind als verständnisvoller Freund inszeniert. Das Kind könnte meinen, der Roboter sei lebendig und es selbst sei dem Roboter tatsächlich wichtig (im Sinne von wertvoll). Irgendwann aber realisiert das Kind, dass die vermeintliche emotionale Nähe bloss ein Algorithmus, das erlebte Verständnis nur eine Illusion war. Welche Auswirkungen hat diese Erfahrung auf künftige Beziehungen? Verständnis, Freundschaft oder Mitgefühl sind nur vorgespielt, nur geschickt programmierte Täuschungen, welchen zumindest potentiell die Gefahr der Ent-Täuschung innewohnt (z.B. durch technische Defekte, fehlende Empathie oder Verfügbarkeit des Geräts), was wiederum das Wohlergehen des Kindes angeht oder sich gar auf andere menschliche Beziehungen auswirkt.[7] Sharkey spricht von einer „relationship with a psychopath" (Sharkey 2016: 290) und meint die Tatsa-

7 Der Einwand, Kinder beseelten auch andere Objekte wie Puppen oder Tiere greift deshalb zu kurz, weil Roboter aktiv diese Täuschung unterstützen und die Bezie-

che, dass wir zwar Empathie und Freundschaft gegenüber einem Roboter empfinden können, dieser aber lediglich so programmiert ist, als würde er diese erwidern, selbst aber keinerlei solcher Gefühle hat. Roboter sind immer nur pseudo-soziale Maschinen (Krotz 2007), welche zwar interagieren können, zu echter Sorge – wie sie in einer pädagogischen Beziehung notwendig wäre – aber nicht in der Lage sind.

Als problematisch beurteilt Sharkey vor allem Roboterrollen wie die des Student-Peer und des Lernbegleiters. Folgerichtig fordert sie eine kritische Folgenabschätzung beim Einsatz sozialer Roboter im Unterricht, vor allem hinsichtlich eines möglichen Verlustes oder der Schädigung menschlicher Kontakte. So könnte das Kind die Gesellschaft eines Roboters der anderer Kinder vorziehen, insbesondere dann, wenn ihm der Roboter stets freundlich gesinnt ist und seine Wertschätzung ihm gegenüber ausdrückt. Die Beziehung zu einem Roboter kann aber nur sehr bedingt als Ersatz für echte menschliche Kontakte dienen.

Brščić et al. (2015) stellen fest, dass bösartiges Verhalten von Kindern gegenüber Robotern meist unbemerkt (wenn das Kind alleine mit dem Roboter ist) und ohne Konsequenzen bleibt. Die Roboterethik diskutiert deshalb darüber, den Roboter als Träger moralischer Werte und Rechte zu definieren (u.a. Loh 2018), nicht nur, um ihn vor Schaden zu bewahren, sondern auch, um den Menschen vor den negativen Auswirkungen seines gewalttätigen Verhaltens gegenüber Robotern zu bewahren (z.B. Empathieverlust in realen menschlichen Beziehungen).

Überdies berühren Roboter noch ein weiteres Problemfeld, nämlich den *Schutz von Privatheit* bzw. *Datenschutz*, wobei mindestens fünf Faktoren zentral erscheinen. Erstens ist der Roboter mit Sensoren ausgestattet, die potentiell persönliche und sensible Daten erfassen, verarbeiten und speichern. Die Möglichkeit der Speicherung so erhobener Daten verschärft zweitens die Gefahr von Datenmissbrauch. Wolfert et al. (2020) weisen darauf hin, dass ein Roboter und seine sozialen Fähigkeiten das Ziel von Hacking-Angriffen sein können und so Zugang zu Orten und Informationen offenlegen oder gar zu Handlungen motivieren könnten, welche dem Menschen Schaden zuführen können. Drittens werden Roboter immer autonomer, was ihre Fähigkeit betrifft, auf erhobenen Daten basierende Entscheidungen zu fällen. Viertens werden Roboter mobiler (kleiner, tragbar) was ihnen erlaubt, auch im Privaten, z.B. im Kinderzimmer, eingesetzt zu werden (z.B. als Spielzeug, Nanny oder Aufgabenhilfe). Fünftens offeriert

---

hung zum menschlichen Gegenüber mitgestalten können, was bei einem anderen Objekt nicht der Fall ist.

die Gestaltung des Roboters eine neue Art der Nähe zwischen Maschine und Mensch, physisch wie auch emotional. Humanoide Roboter könnten dadurch dem Menschen viel leichter persönliche Informationen entlocken als andere Maschinen, auch, weil die Datenerfassung meist unbemerkt bleibt (z.B. weil man sich unbeobachtet fühlt).

Für den Unterrichtsalltag bedeutet dies, dass ein Roboter fähig sein könnte, einzelne Kinder oder Gruppen von Kindern zu überwachen und deren Verhalten zu analysieren und zu bewerten. Bereits die Verwendung von Technologie zur Ermittlung von Emotionen kann als Verletzung der Privatheit verstanden werden (Sharkey 2016). Außerdem besteht noch keine Einigkeit darüber, wofür die bereits heute verfügbaren Daten verwendet werden könnten und sollten: Wer erhält Zugang zu den Lerndaten der Lernenden? Welche wirtschaftlichen Interessen fließen mit der Datenerhebung in die Unterrichtspraxis mit ein? Welche ethischen Grundsätze sollen berücksichtigt werden? Unklar bleibt ebenfalls, ob und aufgrund welcher Datensätze der Roboter selbständige Entscheidungen in der Interaktion mit Menschen treffen darf.[8]

Wird der Roboter in der Rolle des Lehrenden in einem Klassenverband eingesetzt, stellt sich im Weiteren die Frage nach der Autorität. Roboter in einer entsprechenden Position müssen mit der nötigen Autorität ausgestattet werden, um nicht nur auf geltende Regeln hinzuweisen, sondern diese gegebenenfalls durchzusetzen. Voraussetzung dafür ist, dass der Roboter positives und lernförderliches von negativem und die pädagogische Interaktion störendem Verhalten unterscheiden kann. Ebenso muss er die Vermittlung laufend an die aktuellen Bedürfnisse im Lernraum anpassen können. Zu beidem sind bisher eingesetzte Robotermodelle (noch) nicht fähig. Es scheint aus heutiger Sicht fraglich, ob Roboter jemals der Komplexität einer pädagogischen Interaktion gerecht werden können. Als Ersatz einer menschlichen Lehrkraft scheidet er deshalb aus: „[R]obots do not have the necessary moral and situational understanding to be able to adequately, or acceptably, fulfil this role." (Sharkey 2016: 293)

Entscheidungsmöglichkeiten sozialer Roboter in Lehre oder Erziehung können nicht unabhängig von moralischen Werten diskutiert werden. Die weiterführende Frage lautet dann, wie sich Moral überhaupt in eine Maschine implementieren lässt und ist Teil maschinenethischer Diskurse.

8 Zwar wird die Möglichkeit diskutiert, dass Roboter fairere und unparteiischere Entscheidungen als Menschen treffen könnten, weil sie sich nicht von Emotionen leiten ließen (Sharkey 2016). Allerdings kann der Roboter immer nur so „gut" sein, wie der Mensch, der ihn programmiert, und nur so objektiv, wie die Daten, auf die er zugreift (Friedman/Nissenbaum 1996).

Grundsätzlich scheinen drei Ansätze denkbar (Loh 2018: 9f). Moralische (Grund-)Werte könnten in geeignete Programmiersprachen übersetzt und dem Roboter implementiert werden (Top-Down). Abgesehen von der damit verbundenen Übersetzungsherausforderung könnte eine vorab programmierte „Moral" der Komplexität alltäglicher Entscheidungen nicht gerecht werden (es fehlt an Kontextsensibilität). Die umgekehrte Herangehensweise, diejenige, dass der Roboter nach seinem menschlichen Vorbild Schritt für Schritt lernt, moralische Urteile zu fällen, scheint hier adäquater (Bottom-Up). Da sich ein solches Lernen auf der Basis künstlicher Intelligenz vollziehen würde, scheint die Befürchtung gerechtfertigt, dass der Roboter auch von vermeintlich objektiven Datensätzen und unerwünschten Vorbildern lernen (also bspw. rassistische Urteile fällen oder ganz neue, eigene Maßstäbe entwickeln) könnte. Als Zwischenweg bietet sich darum ein hybrider Ansatz an, bei dem der Roboter gewisse (moralische) Grundsätze implementiert erhält, gleichzeitig aber in begrenztem Ausmaß Autonomie und moralische Sensibilität entwickeln kann (Loh 2018: 10).

Von gesellschaftlicher Seite bedürfte der Einsatz sozialer Roboter in Bildungskontexten der Legitimation, Kontrolle über Menschen auszuüben. Ein Roboter müsste adäquat einschreiten können, wenn Lernende sich selbst oder andere gefährden. Diese Autorität ist aber bisher Erziehungsberechtigten vorbehalten. Daraus ergibt sich der wenig praktische Umstand, dass ein Roboter im Unterricht nie alleine mit Lernenden gelassen werden darf.

Die bisherigen Überlegungen führen zu grundsätzlichen Fragen im Hinblick auf den Einsatz sozialer Roboter im Bildungsbereich. Zentral ist ein Nachdenken über die möglichen pädagogischen Rollen, die Roboter zugewiesen bekommen, sowie ihre Entscheidungsspielräume und -befugnisse hinsichtlich der Lernformen und -inhalte aber auch in der Bewertung der Leistung oder des Verhaltens von Lernenden. „To what extent should robots be trusted to make the right decisions about what humans should do?" (Sharkey 2016: 288) wirft folgerichtig die Frage auf, welchen Platz wir der Robotertechnologie im Bildungswesen zuweisen möchten, oder wie es Belpaeme et al. formulieren: „How far do we want the education of our children to be delegated to machines, and social robots in particular?" (Belpaeme et al. 2018: 7).

2. Integration in die Lehre und medienpädagogische Implikationen

Bei der Integration sozialer Roboter in die Lehre sind curriculare Vorgaben und didaktische Ziele, aber auch Aspekte wie Kostenaufwand sowie

die Medienkompetenzen von Lehrenden und Lernenden zu berücksichtigen. Roboter sinnstiftend in Lehr-/Lernprozesse zu integrieren, erfordert auf Seiten der Lehrpersonen oder einer Assistenz Programmierkenntnisse, welche es erlauben, den Robotereinsatz inhaltlich passend und niveaugerecht zu gestalten sowie auf das jeweilige (medien-)pädagogische Konzept auszurichten, welches den Ansatz der kritisch-reflexiven Medienbildung berücksichtigt. Beobachtungen aus der Praxis zeigen, dass beim derzeitigen technischen Entwicklungsstand ein gewisses „Tüftlertum" unumgänglich ist. Der Zeitaufwand für die Planung und Umsetzung von robotergestützten Lehr-/Lernszenarien ist dabei, unabhängig des Fachbereichs, beachtlich. Überdies muss der Support der Geräte sichergestellt werden, was wiederum hohe Ansprüche an die Institutionen stellt (IT-Support, Gerätewartung, Transport, Lagerung etc.).

Im Zentrum eines sinnvollen Robotereinsatzes in der Lehre steht aber nicht die Technologie, sondern die (medien-)pädagogischen Implikationen. Grundlage dafür ist die Unterscheidung von Robotern als *Lehr-/Lernmittel* und *Lerngegenstand* sowie der Ansatz der kritisch-reflexiven Medienbildung (Reimer 2003, 2019).

2.1 Bildungspotential sozialer Roboter

Bisherige Praxiseinsätze konzentrieren sich darauf, den Roboter als Lehr- und Lernmittel einzusetzen, vom Spracherwerb bis hin zum Lernen in MINT-Fächern (z.B. Programmieren). Ebenfalls wird explizit sein Unterhaltungswert („Edutainment") erwähnt. Ein Roboter verfügt allerdings gerade in seiner humanoider Gestalt über ein Bildungspotential, welches über das eines Werkzeuges hinausgeht, nämlich dann, wenn er als Gegenstand reflektiert wird. Den Roboter als Gegenstand zu thematisieren heißt, ihn in seinen aktuellen und künftigen Rollen ernst zu nehmen und ihn als solchen in die Lehre zu integrieren. Dies beinhaltet unter anderem auch seine kulturelle, historische oder ökonomische Dimension, seine Inszenierung als lebendige*r Interaktionspartner*in z.B. in Lehr-/Lernprozessen, wie auch gesellschaftliche oder ethische Fragestellungen.

Im Bereich der Arbeit übernehmen Roboter schon seit Jahrzehnten umfangreiche Aufgaben und drängen nun als soziale Roboter immer stärker auch in nicht-industrielle und soziale Bereiche vor. Hier entlasten sie den Menschen, stellen aber wiederum sein Selbstverständnis im jeweiligen Tätigkeitsbereich in Frage. Diese Veränderungen in den unterschiedlichen Arbeitswelten durch die Robotik müssen im Bereich der betrieblichen Bildung, letztlich aber bereits während der Schul- und Studienzeit reflektiert

werden. Neben Fragen des Persönlichkeitsschutzes (v.a. von Kindern und Jugendlichen) gilt es auch ökonomische Interessen und damit verbundene Machtstrukturen, die hinter den Entwicklungen der Sozialrobotik stehen, zu thematisieren.

Die Entwicklungen im Bereich der künstlichen Intelligenz und der Ausdruckskraft der Roboter (Gestik, Mimik, Intonation der Stimme etc.) verringern von außen erkennbare Unterschiede zwischen Maschinen und lebendigen Wesen. Als Lebendigkeit simulierendes Artefakt fordert der Lerngegenstand sozialer Roboter die Lernenden in ihrem Grundverständnis als Mensch, seiner Kognition und Emotionalität heraus. Der Roboter stellt die Frage nach dem Leben selbst, sowie nach dem spezifisch Menschlichen (Brenner 2009).

Erich Fromm (1968: 43f.) machte schon 1968 auf gesellschaftliche Problematiken in Bezug auf die Entwicklung humanoider Roboter aufmerksam:

> „The possibility that we can build robots who are like men belongs, if anywhere, to the future. But the present already shows us men who act like robots. When the majority of men are like robots, then indeed there will be no problem in building robots who are like men."

Das Bestreben, Maschinen zu bauen, die „wie wir" sind, sich aber eben doch vom Menschen – durch Unsterblichkeit oder Unfehlbarkeit bspw. – unterscheiden, zeugt von einem bestimmten Menschenbild, einer Vision dessen, was der Mensch sein oder werden soll. Fromm beschreibt eine Bewegung beider, Maschine und Mensch, aufeinander zu, ein Ineinandergleiten vermeintlich klar getrennter Entitäten. Humanoide Maschinen als Projektionsflächen menschlicher Sehnsüchte, Ängste und Zukunftsvorstellungen zu reflektieren, ist Auftrag einer kritisch-reflexiven Medienbildung. Eine Konfrontation mit sozialen Robotern in ihrer Mehrdimensionalität birgt immer auch, so die These dieses Beitrags, ein Potential der Irritation und damit der Reflexion eigener Selbst- und Weltverhältnisse. Beispielsweise kann der reichhaltige Korpus dramatischer, prosaischer, zeichnerischer oder filmischer Quellen rund um das Thema Roboter in Lehrveranstaltungen einbezogen werden. Das erlaubt den Lernenden, ihre eigenen (inneren) Bilder von Robotern zu aktivieren und diese zu reflektieren, was ihnen nicht zuletzt ermöglicht, sich in einer dringend nötigen Diskussion um die Entwicklung und Verbreitung dieser Technologie zu positionieren.

2.2 Roboter in Bildungsinstitutionen: Mitgestalten, Mitverantworten

Der Roboter als Kulturerzeugnis, seine Rolle in einer vom Digitalen geprägten Welt, seine technologische, historische und symbolische Dimension – all dies sind Facetten des Phänomens Roboter. Die Integration von Robotern in die Lehre bedingt, diese Perspektiven stets mitzudenken, sie curricular und fächerübergreifend im Schul- und Hochschulalltag zu verankern. Medienbildung heißt, die Frage nach der gesellschaftlichen, kulturellen und ethischen Dimension technischer Innovationen und ihren Folgen ins Zentrum zu rücken: „Sowohl in der Schule als auch an den Universitäten darf der vermehrte Einsatz der neuen Medien[9] – als Unterrichtsmittel und Forschungsinstrument – nicht das Reden über sie verdrängen" (Simanowski 2018: 23). Für einen kritischen Umgang und eine reflektierte Anwendung digitaler Technologien erweist sich die kritisch-reflexive Medienbildung als ein Ansatz für die Lehre, der basierend auf einem klassischen Bildungsbegriff, Urteilsvermögen, Kreativität und Kritikfähigkeit betont und Bildung nicht auf Arbeitsmarktbefähigung reduziert. Ziel ist ein mündiger Umgang mit Technologie und mit den eigenen Vorstellungen und (Zukunfts-)Phantasien davon.

Auf der Ebene der Institution bedeutet dies, sich der Herausforderung sozialer Roboter zu stellen und die eigene Verantwortung wahrzunehmen. Dass Roboter sich in der Lehre etablieren werden, wird in der Forschung kaum in Frage gestellt. Es scheint allein eine Frage der technischen Innovation und damit der Zeit, bis Roboter routinemäßig in Bildungsinstitutionen zum Einsatz kommen. Eine solche Formulierung negiert allerdings den Gestaltungsfreiraum und die daraus abzuleitende Verantwortung der Institutionen bei der Integration von Robotern. Eine kritisch-reflexive Medienbildung weist auf diesen Freiraum sowie die Rolle und Verantwortung der Pädagogik in dieser Entwicklung hin. Letztendlich müssen es Pädagog*innen selbst sein, die über Form und Umfang von Robotereinsätzen in Bildungsinstitutionen entscheiden, begründet auf theoretischen und empirischen Grundlagen sowie medienpädagogischen, insbesondere mediendidaktischen Überlegungen.

Diese Mitgestaltung sollte bereits im Stadium der Forschung und der Entwicklung von Robotertechnologien für den Bildungsbereich erfolgen, indem pädagogische Expertise in Forschungsprojekten zwingend eingefor-

9 Wenngleich Simanowski hier Roboter nicht explizit als neue Medien nennt, kann seine Aussage in diesem Sinne interpretiert werden und in die Argumentation miteinfliessen.

dert wird. Hier gilt es, pädagogische Fragen im Zusammenhang mit Robotern über interdisziplinär breit abgestützte Forschungsprojekte zu bearbeiten und weiterzuentwickeln. Dabei sind Forscher*innen auch auf entsprechende Mittel angewiesen, was Bildungspolitik und Hochschulleitungen in die Verantwortung miteinbezieht. Die Entwicklung soll nicht allein privatwirtschaftlichen Interessen überlassen werden. Die im Rahmen des Forschungsprojekts FHNW Robo-Lab durchgeführten Workshops sind nur eine Möglichkeit, Teilbereiche der kritisch-reflexiven Medienbildung mit Studierenden und weiteren Bildungsverantwortlichen in Bezug auf soziale Roboter zu stärken (Flückiger/Reimer 2021). Konkret können Lernende bspw. die Aufgabe erhalten, einen idealen Roboter zu entwerfen, und zwar im Hinblick auf dessen Funktionen, Rollen, Aufgaben und moralische Handlungsautonomie. Erfahrungen im Projekt zeigen, dass Studierende den Robotereinsatz als außergewöhnliches Erlebnis im Studierendenalltag schätzen. Gleichzeitig fällt auf, dass die ethische und gesellschaftliche Relevanz sozialer Roboter unterschätzt wird. Eine Diskussion der unterschiedlichen Dimensionen eines Roboters muss aktiv angeregt werden, sonst findet sie nicht statt.

3. Diskussion

Was folgt aus den voranstehenden Überlegungen hinsichtlich der Integration sozialer Roboter in die Lehre für die einzelnen Bildungsinstitutionen? Roboter können einerseits bestehende pädagogische Praktiken übernehmen oder ergänzen, indem sie zum Beispiel Wissen personalisiert vermitteln. Andererseits sollen sie neue Unterrichtspraxen ermöglichen, die es den Lehrkräften erlauben, sich noch stärker ihren Kernkompetenzen im direkten Umgang mit Lernenden zuzuwenden. Die Erwartungen an soziale Roboter sind aber hoch und auch dann, wenn man dem verbreiteten Optimismus im Kern zustimmt, bleibt zweifelhaft, ob diese Erwartungen realistisch sind. Dies liegt einerseits an technischen Herausforderungen, welche die pädagogische Praxis an die Roboter stellt. Andererseits bleiben eine Reihe ethischer Fragen offen, welche sich unter anderem aus der humanoiden Gestaltung der Geräte in Verbindung mit einer vulnerablen Zielgruppe (z.B. Kinder, Menschen mit Beeinträchtigungen) ergeben. Die humanoide Gestaltung von Mensch-Maschinen-Interaktionen sollte daher besondere Aufmerksamkeit erhalten. Einer gezielt simulierten Vermischung von Maschinen mit genuin menschlichen Fähigkeiten wie Emotionalität, Empathie, Bindungsfähigkeit, Vertrauen oder Freundschaft – und damit einer Beförderung einer Täuschung – ist kritisch zu begegnen. Gera-

de die Pädagogik muss dem würdevollen und achtsamen Umgang mit dem Menschen und seiner Privatheit in der Interaktion stets von Neuem einen zentralen Platz einräumen. Grundsätzlich ist es angezeigt, der Einführung sozialer Roboter in unterschiedliche Bereiche der Bildung die Fragen vorwegzustellen, welche konkreten Probleme soziale Roboter im Bildungssystem lösen können, welche sie verschärfen und welche neuen Probleme sie schaffen könnten. Der Einsatz sozialer Roboter in Vor- und Primarschuleinrichtungen ist nach dem heutigen Kenntnisstand nur unter Begleitung medienpädagogisch geschulter Pädagogen und Pädagoginnen und mit klaren didaktischen Zielsetzungen gerechtfertigt. Ebenfalls muss auf allen Bildungsstufen über eine adäquate, d.h., kritisch-reflexive Form der Medienbildung nachgedacht werden, welche den Roboter in seiner Ganzheit erfasst und ihn als Gegenstand zu thematisieren versteht.

Literatur

Baxter, Paul / Ashurst, Emily / Read, Robin / Kennedy, James / Belpaeme, Tony (2017): *Robot Education Peers in a Situated Primary School Study: Personalisation Promotes Child Learning*. In: PloS One 12(5):e0178126.

Belpaeme, Tony / Kennedy, James / Ramachandran, Aditi / Scassellati, Brian / Tanaka, Fumihide (2018): *Social Robots for Education: A Review*. In: Science Robotics 3 (21).

Breazeal, Cynthia (2003): *Toward Sociable Robots.* In: Robotics and Autonomous Systems 42 (3-4), S. 167-175.

Brenner, Andreas (2009): *Leben*. Stuttgart: Philipp Reclam jun.

Brščić, Drazen / Kidokoro, Hiroyuki / Suehiro, Yoshitaka / Kanda, Takayuki (2015): *Escaping from Children's Abuse of Social Robots*. In: Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction - HRI *'15*. Portland, Oregon, USA: ACM Press, S. 59–66.

Causo, Albert / Zin Win, Phyo / Peng Guo, Sheng / Chen, I-Ming (2017*): Deploying social robots as teaching aid in pre-school K2 classes: A proof-of-concept study.* In: 2017 IEEE International Conference on Robotics and Automation (ICRA), S. 4264–4269.

Decker, Michael (2010): *Ein Abbild des Menschen: Humanoide Roboter.* In: Information und Menschenbild 37 (1). Berlin, Heidelberg: Springer, S. 41–62.

Flückiger, Silvan / Reimer, Ricarda T.D. (2021) (im Erscheinen): *Projektbericht FHNW Robo-Lab – Schwerpunkt „Bildung und Roboter".*

Friedman, Batya / Nissenbaum, Helen (1996): *Bias in computer systems*. In: ACM Transactions on Information Systems 14(3), S. 330–347.

Fromm, Erich (1968): *The revolution of hope: toward a humanized technology.* New York*:* HarperCollins.

Hood, Deanna / Lemaignan, Séverin / Dillenbourg, Pierre (2015): *When Children Teach a Robot to Write: An Autonomous Teachable Humanoid Which Uses Simulated Handwriting*. In: 10th ACM/IEEE International Conference on Human-Robot Interaction (HRI), S. 83–90.

Yang, Guang-Zhong / Bellingham, Jim / Dupont, Pierre E. / Fischer, Peer / Florid, Luciano / Full, Robert / Jacobstein, Neil / Kumar, Vijay / McNutt, Marcia / Merrifield, Robert / Nelson, Bradley J. / Scassellati, Brian / Taddeo, Mariarosaria / Taylor, Russell / Veloso, Manuela / Lin Wang, Zhong / Wood, Robert (2018): *The Grand Challenges of Science Robotics*. In: Science Robotics 3(14), S. 1–14.

Kennedy, James / Baxter, Paul / Belpaeme, Tony (2015): *The Robot Who Tried Too Hard: Social Behaviour of a Robot Tutor Can Negatively Affect Child Learning*. In: 10th ACM/IEEE International Conference on Human-Robot Interaction (HRI), S. 67–74.

Kory Westlund, Jacqueline M. / Jeong, Sooyeon / Park, Hae W. / Ronfard, Samuel / Aradhana, Adhikari / Harris, Paul L. / DeSteno, David / Breazeal, Cynthia L. (2017): *Flat vs. Expressive Storytelling: Young Children's Learning and Retention of a Social Robot's Narrative*. In: Frontiers in Human Neuroscience 11(295), S. 1-20.

Loh, Janina (2018): *Maschinenethik und Roboterethik*. In: Oliver Bendel (Hg.): Handbuch Maschinenethik. Wiesbaden: Springer Fachmedien, S. 1–19.

Meyer-Drawe, Käte (2007): *Menschen im Spiegel ihrer Maschinen*. München: Wilhelm Fink Verlag.

Reich-Stiebert, Natalia / Eyssel, Friederike (2015): *Learning with Educational Companion Robots? Toward Attitudes on Education Robots, Predictors of Attitudes, and Application Potentials for Education Robots*. In: International Journal of Social Robotics 7(5), S. 875–888.

Reimer, Ricarda T.D. (2003): *Medienpädagogische Gestaltungsideen zur Integration von E- Learning in der Hochschullehre*. In: Online-Zeitschrift MedienPädagogik. Online verfügbar unter: http://www.medienpaed.com/03-1/reimer03-1.pdf (Abfrage am: 22.04.2020).

Reimer, Ricarda T.D. (2019): *Bildungsverantwortung der Hochschulen im Zeitalter der Digitalisierung*. In: Marlene Miglbauer / Lene Kieberl / Stefan Schmid (Hg.): Hochschule digital.innovativ I #digiPH. Tagungsband zur 1. Online-Tagung. Norderstedt: Books on Demand GmbH, S. 23–34.

Siebert, Scarlet / Tolksdorf, Nils / Rohlfing, Katharina / Zorn, Isabel (2019): *Raising Robotic Natives?: Persuasive Potentials of Social Robots in Early Education.* In: The Journal of Communication and Media Studies 4(4), S. 21–35.

Sharkey, Amanda J. C. (2016): *Should We Welcome Robot Teachers?* In: Ethics and Information Technology 18(4), S. 283–297.

Simanowski, Roberto (2018): *Stumme Medien. Vom Verschwinden der Computer in Bildung und Gesellschaft.* Berlin: Matthes & Seitz.

Vollmer, Anna-Lisa / Mühlig, Manuel / Steil, Jochen J. / Pitsch, Karola / Fritsch, Jannik / Rohlfing, Katharina J. / Wrede, Britta (2014): *Robots Show Us How to Teach Them: Feedback from Robots Shapes Tutoring Behavior during Action Learning*. In: PLoS ONE 9(3): e91349. https://doi.org/10.1371/journal.pone.0091349.

Weber, Katharina / Zeaiter, Sabrina (2018): *Project H.E.A.R.T. (Humanoid Emotional Assistant Robots in Teaching).* In: J. Buchner / Chr. Freisleben-Teutscher / J. Haag & E. Rauscher (Hg.): Inverted Classroom. Vielfältiges Lernen. Begleitband zur 7. Konferenz Inverted Classroom and Beyond 2018; FH St. Pölten, 20. & 21. Februar 2018, Brunn am Gebirge: ikon Verlag, S. 237–244.

Wolfert, Pieter / Deschuyteneer, Jorre / Oetringer, Djamari / Robinson, Nicole / Belpaeme, Tony (2020): *Security Risks of Social Robots Used to Persuade and Manipulate: A Proof of Concept Study*. In: Companion of the 2020 ACM/IEEE International Conference on Human-Robot Interaction. Cambridge United Kingdom: ACM, S. 523–525.

Teil III –
Datenschutz und Privatheit als Thema der Gesetzgebung und Medienregulierung

Recht auf mein Selbst – Schutzräume kindlicher Entwicklungsphasen in der digitalen Gesellschaft

Stephan Dreyer

Abstract

Die digitale Gesellschaft datafiziert unweigerlich auch die Kindheit. Doch was bedeutet das für die gesetzliche Einhegung dieser besonderen Entwicklungsphase? Der Beitrag zeigt, dass das grundgesetzliche Recht auf freie Persönlichkeitsentwicklung kindbezogene Schutzräume (auch) im Digitalen umfasst. Dabei werden die Schutzgehalte eines spezifischen Kinderrechts auf Privatsphäre aus dem Recht auf freie Persönlichkeitsentwicklung und -entfaltung hergeleitet und dessen Besonderheiten und Ausprägungen in digitalen Medienumgebungen aufgezeigt. Durch den Abgleich verfassungsrechtlich erwünschter digitaler Schutzräume mit empirischen Einblicken in die datenschutzbezogenen Kenntnisse, Sorgen und Wünsche von Kindern und Jugendlichen zeigt der Beitrag bestehende Regelungslücken, aber auch die Herausforderungen bei ihrer gesetzlichen Ausfüllung auf. Denn die mögliche Umsetzung der Pflicht zur Schaffung gesetzlicher Schutzräume für Kinder im Digitalen weist strukturelle Herausforderungen und Spannungsfelder auf, etwa Datenschutz- oder Geheimnisinteressen der Minderjährigen, das Erziehungsrecht der Eltern sowie die begrenzte Steuerungsmacht sanktionsbewehrter Normen.

1. Freie Persönlichkeitsentfaltung: Das Recht, sich selbst zu gehören

Die Freiheit des Einzelnen wurde mit der Schaffung des Art. 2 Abs. 1 GG von einem vorgesetzlichen Naturrecht in eine positivrechtliche Form gegossen, die die Garantie der Menschenwürde aus Art. 1 Abs. 1 GG mit einer programmatischen Gewährleistung ergänzt: der prinzipiellen Freiheitsvermutung. Menschsein und Freiheit haben Vorrang vor staatlich verordnetem Dasein (Di Fabio 2019). Die Freiheit, die Art. 2 Abs. 1 GG garantiert, ist die freie Entfaltung der Persönlichkeit. Sie bezieht sich zum einen auf die Ebene der physischen Handlungsfreiheit, das heißt, jede Person darf prinzipiell tun und lassen, was sie will. Sie enthält aber auch eine psy-

chische Komponente, die auf die innere Freiheit des Einzelnen abzielt: Kern dieser Freiheitsdimension ist das Allgemeine Persönlichkeitsrecht, das die Integrität der Persönlichkeit in geistig-seelischer Hinsicht und die soziale Identität schützt. Damit wird nicht eine bestimme Handlung oder ein bestimmtes Tun geschützt, sondern die Freiheit, nach eigenem Willen darüber zu entscheiden, was man tun oder nicht tun möchte. Dies rückt die jeder Handlung oder jedem Unterlassen vorausgehende innere Entscheidung des Einzelnen in den Fokus dieser Grundrechtsausprägung. Es geht um die Gewährleistung freier Selbstbestimmung in einem Zustand, in dem jede Entscheidungsfindung autonom und ohne fremde Einwirkungen erfolgen kann, in dem das Selbst, das eigene „Ich" alleiniger Entscheidungshersteller und -träger ist. Damit umfasst das Recht auf freie Persönlichkeitsentfaltung zentral das Recht, sich selbst zu gehören. Der autonomiebezogene Schutz einer solchen entscheidungsbezogenen Lesart des Allgemeinen Persönlichkeitsrechts ist Vorbedingung für die Ausübung vieler weiteren Grundrechte, von der Wahrnehmung von Informations- und Kommunikationsgrundrechten über die Religionsfreiheit bis hin zur Versammlungsfreiheit.

Welche spezifischen Gehalte aber weist dieses Recht auf mein Selbst für Kinder und Jugendliche in einer digitalisierten, datafizierten Gesellschaft auf? Der Beitrag arbeitet die Notwendigkeit und Quelle eines spezifischen Persönlichkeitsentwicklungsrechts heraus (2.), zeigt anhand entwicklungspsychologischer Erkenntnisse und besonderer rechtlicher Umhegungen die derzeitigen Herleitungen und Ausgestaltungen besonderer Schutzräume von Kindern auf (3.) und setzt diese in Relation zu Formen informationeller Privatheit und Autonomie bei der digitalen Mediennutzung (4.). Schließlich wird aufgezeigt, dass für Kinder und Jugendliche aufgrund der begrenzten Kenntnisse der komplexen Datenverarbeitungspraktiken und personalisierten Selektionslogiken mit ihren vielfältigen Autonomiebezügen dringend auch die regulatorische Absicherung von Schutzräumen im Digitalen nötig ist, dass die Gesetzgebung sich hier aber teils komplexen Spannungsfelder gegenübersieht, die einfache Ansätze verbieten (5.).

2. *Unbeeinträchtigte Persönlichkeitsentwicklung als Vorbedingung freier Persönlichkeitsentfaltung*

Die Entfaltung des Selbst ist nur möglich, wenn sich zuvor ein Selbst entwickeln und Bahn brechen konnte. Das beschriebene Allgemeine Persönlichkeitsrecht geht implizit davon aus, dass es so etwas wie eine „Persönlichkeit" gibt, die sich durch Denken und Handeln nach innen und außen

manifestiert. Dass jene Persönlichkeit aber nicht auf einmal dem Nichts entspringt, sondern das Ergebnis eines Prozesses ist, lässt sich aus Formulierungen wie einer „gelungenen Identitätsbildung", der Idee einer „Entstehung des Selbst" oder einer „Subjektwerdung" (Becker 2017b) ablesen. Soll das Ergebnis eines solchen Prozesses die autonome Persönlichkeitsentfaltung sein, so muss sich jede Gewährleistung und Garantie der Freiheit der Entfaltung auch auf den vorherigen und andauernden Entwicklungsprozess beziehen: Die Vorbedingung der freien Entfaltung ist das Ergebnis einer freien Entwicklung.

Man wird nicht so weit gehen können, zu sagen, dass aus jeder fremdbestimmten oder manipulierten Entwicklungsphase zwingend eine unfreie Persönlichkeit entsteht – der Einzelne kann hier durchaus resilient sein, Fremdbestimmung bewusst als Eingriff werten und entsprechende Coping-Strategien entwickeln. Aus Sicht eines staatlichen Gewährleistungsauftrags kann aber jedenfalls nicht ausgeschlossen werden, dass eine Beeinträchtigung der freien Entwicklung sich so negativ auf die Ausbildung und Fortbildung von Persönlichkeitsfacetten auswirkt, dass der Prozess der Persönlichkeitsbildung nachhaltig gestört und – im schlimmsten Fall – zu einem Zustand führen kann, in dem eine freie Persönlichkeitsentfaltung gehemmt ist. Der staatliche Auftrag zur Gewährleistung der freien Persönlichkeits*entfaltung* umfasst vor diesem Hintergrund auch den vorausgehenden Prozess der Persönlichkeits*entwicklung*: Verfassungsrechtlich gesehen ist die freie Entwicklung der Persönlichkeit zwingende Voraussetzung für eine freie Persönlichkeitsentfaltung.

3. Kindheit als besondere Phase der Persönlichkeitsentwicklung

Dass sich das Grundgesetz in Art. 2 Abs. 1 GG auf die Persönlichkeitsentfaltung konzentriert, und damit eine irgendwie abgeschlossene Entwicklung impliziert, ist entwicklungspsychologisch längst überholt. Auch im (hohen) Erwachsenenalter formt und prägt sich unsere Persönlichkeit immer weiter aus; die (Weiter-)Entwicklung der eigenen Persönlichkeit ist ein lebenslanger Prozess. Dennoch unterscheidet sich die Kindheit substantiell von den späteren Phasen (Kap. 3.1). Das Recht umhegt diesen Zeitraum entsprechend in besonderer Weise (Kap. 3.2).

3.1 Kindheit als besondere biologische, psychologische und psychosoziale Entwicklungsphase

In der Kindheit erscheinen viele Persönlichkeitsfacetten noch als dynamisch – das „Selbst" ist hier in Teilen instabil, die eigene Persönlichkeit entsteht, wird in der sozialen Interaktion mit anderen ausprobiert und immer wieder angepasst. Teile der Persönlichkeit werden bewusst und unterbewusst verworfen, neue Facetten hinzugefügt. In der Kindheit und Jugend werden (Verhaltens-)Grenzen erkannt, aber auch ausgetestet, sozialadäquates Verhalten gelernt und die eigene Individualität, aber auch die von anderen beobachtet.

Die menschliche Entwicklung durchläuft dabei mehrere Stufen bzw. Konzepte des „Selbst": Nach dem frühen Punkt des Selbst-Bewusstseins, in dem man den eigenen Körper als kontrollierbare biologische Einheit erkennt (Siegler et al. 2016: 410), entsteht nach und nach ein Selbst-Konzept. Das Selbst-Konzept erweitert die Eigenwahrnehmung um die kognitive Identitätskomponente, die über Generalisierungsprozesse aus situativen Selbstbewertungen entsteht und auf sprachliche Entwicklungen und Auseinandersetzungen angewiesen ist. Es entwickelt sich eine erste Gesamtheit der Einstellungen zur eigenen Person, deren Organisation sich durch immer wieder erfolgende Selbstbeurteilungen zunehmend ordnet. Später tritt dann ein Selbst-Wert(gefühl) dazu, bestehend aus der Generalisierung der affektierten Selbstbewertung und aus Kontrollüberzeugungen in Form einer handlungsbezogenen personalen Kontrolle. Diese Kontrolle ist Kern einer Identitätsentwicklung, bei der sich mit zunehmendem Alter und je nach konkreten Kontexten Verhaltensweisen ausdifferenzieren (Siegler et al. 2016: 412 ff.).

Die Phase des Heranwachsens zeichnet sich dabei durch die Instabilität des Selbst-Konzepts aus: Selbstbezogene Kognitionen und Evaluationen schwanken und verändern sich unter dem Einfluss einer Vielzahl sozialer und sozialpsychologischer Bedingungsgrößen. Bei älteren Jugendlichen stabilisieren sich diese Konzepte zunehmend (Greve/Thomsen 2019: 163), spätestens im Erwachsenenalter spricht die Entwicklungspsychologie von relativer Selbst-Konsistenz oder einer gefestigten Identität. Selbst-Konzepte weisen in unterschiedlichen sozialen Kontexten im frühen Kindheitsalter weniger, im Jugendalter umso mehr Varianzen in ihren generellen und spezifischen Aspekten auf: So sind Selbst-Konzepte bis weit in die Kindheit hinein stark positiv verzerrt (Siegler et al. 2016: 411). Erst später nimmt die Genauigkeit der Selbsteinschätzungen durch die allmähliche Integration auch negativer Informationen über eigene Fähigkeiten und Eigenschaften in das Selbstbild zu. Mit dieser Entwicklung einher geht die zunehmende

Ausdifferenzierung des eigenen Rollenbildes; am Ende der Jugendzeit reflektiert das Selbstkonzept dann relativ stabile Überzeugungen und Werte.

Drei Dinge werden bereits anhand dieses sehr kurzen Überblicks deutlich: Selbst-Konzepte von Kindern und Jugendlichen sind hochgradig fluide, sie stabilisieren sich aber mit zunehmendem Alter. Dieser großen Veränderungen unterliegende Raum der Selbst-Entwicklung bildet sich bei Kindern und Jugendlichen aufgrund der Interaktion mit anderen weiter aus. Diese Interaktion ist Wirkfaktor im Sinne einer Sozialisations- und Entwicklungsinstanz: Persönlichkeitsentwicklung ist damit ein „permeabler Schutzraum auch des Sozialen". Mit zunehmendem Kindesalter kann dabei das soziale Verhalten in unterschiedlichen sozialen und kommunikativen Kontexten unterschiedliche Ausprägungen aufweisen.

3.2 Kindheit als rechtlich besonders umhegtes Lebensalter

Die beschriebenen, fluiden Selbst-Konzepte bei Kindern und Heranwachsenden werden für einen besonderen gesetzlichen Schutz im Recht nicht ausdrücklich herangezogen. Sie zeigen sich aber in Form von Gesetzesbegründungen, die einem kindheitstheoretischen Konzept von Vulnerabilität anhängen (Andresen 2018). Als Gründe für den besonderen Schutz von Kindern und Jugendlichen finden sich regelmäßig deren geistige bzw. seelische Verwundbarkeit, ihre im Vergleich einfachere Beeinflussbarkeit, ihre Naivität oder Unwissenheit hinsichtlich komplexer wirtschaftlicher oder sozialer Prozesse, ihre begrenzte Fähigkeit zur Abschätzung von Handlungsfolgen oder ihre Impulsivität. Damit stellt die Gesetzgebung vordergründig vor allem auf begrenzte Erfahrungen und leichte Manipulierbarkeit durch äußere Reize oder Interaktionen statt. Auf den zweiten Blick aber geht es dem Recht darum, mögliche Enttäuschungen, Rückschläge, Verunsicherungen, Schäden und schlicht (rechtlichen oder elterlichen) Ärger, etwa beim Tappen in eine Abofalle, zu minimieren. Es geht um den Schutz vor Entscheidungen des Kindes, die sich negativ auf die Persönlichkeitsentwicklung auswirken können. Die oben dargestellte Herausbildung von Selbst-Konzepten steht so strukturell auch im Fokus des rechtlichen Kinderschutzes.

Mit Blick auf das Schutzgut einer freien, d.h. möglichst unbeeinträchtigten Selbst-Entwicklungsmöglichkeit und Selbst-Entfaltungsmöglichkeit nutzt das Recht dabei in unterschiedlichen Rechtsbereichen Altersgrenzen in Form rechtsfiktiver Entwicklungsstadien. Fiktionen sind im Recht ein oft genutztes Mittel, um einen ungewissen Sachverhalt rechtssicher zu regeln, indem gesetzlich eine bestimmte Tatsachenfolge verbindlich festge-

schrieben wird. In Bezug auf Kinder und Jugendliche knüpfen rechtliche Fiktionen an bestimmte Altersgruppen und die dabei erreichten Entwicklungsstufen an, und sehen regelmäßig entsprechend abgestufte Rechtsfolgen vor. Im Folgenden einige Beispiele:

- **Arbeitsschutz**: Das Arbeitsrecht sieht kinderspezifische Normen vor, um die körperliche wie geistig-seelische Entwicklung von Kindern und Jugendlichen nicht durch schwere körperliche Arbeit oder Überforderung zu gefährden. Das Jugendarbeitsschutzgesetz (JArbSchG) geht vom Grundsatz eines Beschäftigungsverbots für Kinder und Jugendliche unter 15 Jahren aus (im Fall leichter Arbeit und mit Einwilligung der Erziehungsberechtigten: unter 14 Jahren). Ausnahmen für bestimmte Beschäftigungen von noch Jüngeren sind nur nach behördlicher Genehmigung möglich und unterliegen weitreichenden Anforderungen, darunter etwa ein aktuelles ärztliches Attest und Nachweise über Vorkehrungen zur Vermeidung einer Beeinträchtigung der körperlichen oder seelisch-geistigen Entwicklung. Auch in diesem genehmigungsbedürftigen Bereich sieht das Gesetz altersdifferenzierte Abstufungen vor. So dürfen Kinder zwischen drei und sechs Jahren maximal bis zu zwei Stunden täglich und nur in der Zeit von 8 bis 17 Uhr, Kinder über sechs Jahre bis zu drei Stunden täglich und in der Zeit von 8 bis 22 Uhr beschäftigt werden.
- **Jugendmedienschutz**: Klassisches Ziel des Jugendmedienschutzes ist es, dass Minderjährige nicht mit belastenden Medieninhalten in Kontakt kommen. Solche medieninduzierten Entwicklungsrisiken ergeben sich für unterschiedliche Altersstufen aus unterschiedlich drastischen, belastenden oder desorientierenden Darstellungen. Sowohl das Jugendschutzgesetz (JuSchG) im Bereich der Trägermedien als auch der Jugendmedienschutz-Staatsvertrag für Rundfunk und Telemedien (JMStV) sehen Altersbewertungen und entsprechende Alterskennzeichen vor und knüpfen altersabhängige Abgabe- bzw. Zugangsbeschränkungen an diese. Die gesetzlich vorgegebenen Altersgrenzen sind 6, 12, 16 und 18 Jahre. Mit Blick auf die fortschreitende Entwicklung werden Kindern und Jugendlichen bei der Alterseinstufung mit steigendem Alter zunehmende Kompetenzen beim Umgang mit und der Verarbeitung von auch fordernden jugendschutzrelevanten Darstellungen zugemutet.
- **Zivilrechtliche Geschäftsfähigkeit**: Ein weiteres Beispiel für gesetzgeberische Altersabstufungen bei Kindern und Jugendlichen ist die Regelung der Geschäftsfähigkeit Minderjähriger im Bürgerlichen Gesetzbuch (BGB). Schutzgedanke ist hier, dass Rechtsgeschäfte nachteilige

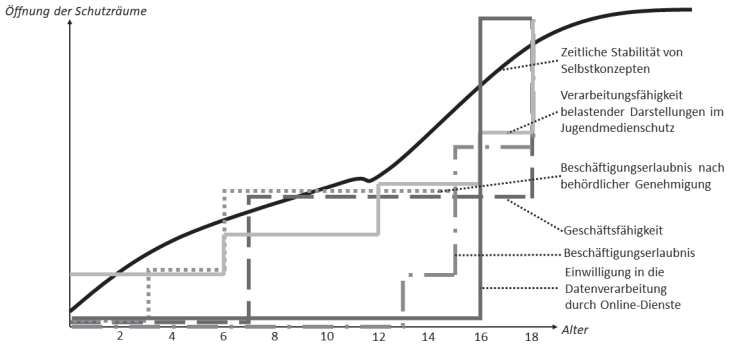
Folgen für die Rechtsposition und das Eigentum von Minderjährigen haben können. Zentral unterstellt der Gesetzgeber hier Defizite in der Möglichkeit der eigenverantwortlichen Willensbildung (Spickhoff 2018); es geht um einen „Schutz vor sich selbst". Nach den §§ 104 ff. BGB sind Kinder unter sieben Jahren geschäftsunfähig, d.h. sie können keine wirksamen Willenserklärungen abgeben und keine Rechtsgeschäfte abschließen. Kinder zwischen sieben und 17 sind beschränkt geschäftsfähig, d.h. sie können Willenserklärungen abgeben und (ausschließlich vorteilhafte) Rechtsgeschäfte vornehmen. Bis zu der elterlichen Genehmigung sind geschlossene Verträge schwebend unwirksam. Nach dem sog. „Taschengeldparagraphen" (§ 107 BGB) können Minderjährige zwischen sieben und 17 Jahren ausnahmsweise auch ohne elterliche Zustimmung verbindliche Verträge schließen, wenn sie zur Bewirkung der Leistung Mittel nutzen, die dem Minderjährigen zu diesem Zweck oder zur freien Verfügung überlassen wurden.

- **Datenschutzrechtliche Einwilligung:** Das EU-Datenschutzrecht geht davon aus, dass Kinder bei der Verarbeitung ihrer Daten eines besonderen Schutzes bedürfen, vor allem mit Blick auf die spezifischen Gefahren der Datenverarbeitung für den Datenschutz, aber auch für die Ausübung von anderen Grundrechten und Freiheiten (sog. Vorfeldschutz). Art. 8 DSGVO sieht vor, dass eine Einwilligung gegenüber Online-Diensten in die Verarbeitung der eigenen personenbezogenen Daten durch Kinder und Jugendliche unter 16 Jahren stets durch die Eltern erfolgen muss. Außerhalb dieser im Vergleich starren Regelung der Einwilligung gegenüber Diensten der Informationsgesellschaft gilt weiterhin der Grundsatz, dass die individuelle Einsichtsfähigkeit Voraussetzung einer wirksamen datenschutzrechtlichen Einwilligung ist. Auch mit Blick auf die angenommene Einsichtsfähigkeit in die teils komplexen Datenverarbeitungsvorgänge geht die Rechtswissenschaft davon aus, dass diese mit dem fortschreitendem Alter Heranwachsender zunimmt.

Die ausgewählten Beispiele zeigen, dass das Recht vielfach abgestufte Schutzräume und -vorkehrungen für Kinder und Jugendliche vorsieht bzw. einzieht. Die gesetzgeberischen Annahmen entsprechen dabei den oben beschriebenen Erkenntnissen der Entwicklungspsychologie: Mit zunehmendem Alter traut das Recht Minderjährigen mehr Einsichtsfähigkeit und Verantwortung zu. (s. die vereinfachte Abb. 1). Der besondere Schutz Minderjähriger im Recht bezieht sich dabei auf zeitliche, physische, psychische, aber auch soziale Schutzräume, in denen Kinder und Jugendliche

aufwachsen und ihre Persönlichkeit möglichst unbeeinträchtigt entwickeln (sollen).

Abb. 1: Biologische Entwicklung und Abstufungen rechtlicher Schutzräume (vereinfacht)



4. *Privatheits- und autonomiebezogene Zielaspekte bei der Gewährleistung unbeeinträchtigten Aufwachsens*

Die Anschlussfrage mit Blick auf das Schutzziel einer möglichst unbeeinträchtigten Persönlichkeitsentwicklung ist, inwieweit dieses Ziel auch autonomie- und privatheitsbezogene Aspekte beinhaltet. Das Recht auf unbeeinträchtigte Persönlichkeitsentwicklung betrifft angesichts ihrer besonderen Entwicklungsphase und der daraus folgenden besonderen Ausgestaltung rechtlicher Schutzräume vor allem heranwachsende Kinder und Jugendliche. Nicht umsonst erscheint die Freiheit der Persönlichkeitsentwicklung als Kern des verfassungsrechtlichen Kinder- und Jugendschutzes. Deswegen lohnt ein zweiter Blick auf dessen Schutzziele:

Kernelemente des Ziels einer freien Persönlichkeitsentwicklung und -entfaltung von Minderjährigen sind nach Ansicht des BVerfG die Gemeinschaftsfähigkeit und die Eigenverantwortlichkeit.[1] Hier konkretisiert sich die Entwicklungs*freiheit* als ein nicht zum Selbstzweck gewährtes Recht, sondern als Aufrechterhaltung eines normativen Nexus an Entwicklungsmöglichkeiten, dessen Zielerreichung der Staat sich wünschen, aber selbst nicht positiv garantieren kann. Der Schutzauftrag soll dann wenigstens die auf diese Erreichung negativ wirkenden Einflüsse fernhalten – die

1 BVerfGE 79, 51 (63 f.); 83, 130 (139).

Gewährleistung von Entwicklungsfreiheit erfolgt um die *Möglichkeit*, mündige Bürger*innen zu werden.

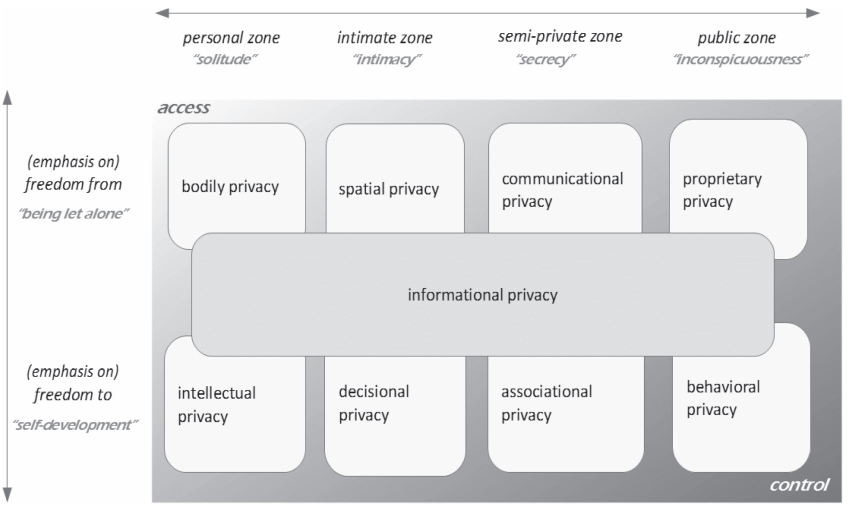
Das grundgesetzlich erwünschte Entwicklungsziel der Eigenverantwortlichkeit verweist auf ein „Verständnis der Persönlichkeitsentwicklung als autonomer Prozess, als Möglichkeit, das eigene Selbstbild nach eigenem Entwurf zu gestalten, ohne dass externe Einflüsse in diese Entwicklung eingreifen" (Dreyer 2018a: 202). In diesem Verständnis von Eigenverantwortlichkeit als Selbstbestimmtheit scheint das oben angesprochene Recht auf sein „Selbst" und die damit verbundene Autonomie deutlich auf. Der Gewährleistungsauftrag für Autonomie im Sinne einer Selbstbestimmtheit zielt ab auf den Schutz gegen Fremdbestimmtheit, etwa in Form von willentlicher Beeinflussung bis hin zu Fremdsteuerung. Der staatliche Jugendschutzauftrag umfasst so neben klassischen Entwicklungsrisiken, die Traumata, Ängste oder psychische Störungen und Zwänge auslösen können und sich als Einschränkung oder Hemmung eigenverantwortlicher Entscheidungen manifestieren, auch „weichere" Beeinträchtigungen der Autonomie: Dort, wo autonome Entscheidungen oder autonomes Handeln durch von außen aufoktroyierte Werte, Sichtweisen oder Rollenverständnisse und ohne Möglichkeit des Erlernens kritischer Reflektion, Hinterfragung und Offenheit für andere, alternative Sicht- und Entscheidungsweisen eingeschränkt werden, muss der Schutzauftrag ebenfalls aktiviert sein (Dreyer 2018a: 157).

4.1 Verschränkung von Autonomie und Privatheit

Für die Nutzung digitaler Medien durch Kinder und Jugendliche muss vom Autonomieschutz ausgehend auch dessen enge Beziehung zu Privatheit und Privatheitskonzepten diskutiert werden. Autonomie, verstanden als das Recht und die Möglichkeit, über sein Selbst zu bestimmen, benötigt Privatheit: Es bedarf individueller Räume, in denen sich die eigene Persönlichkeit entwickeln kann (Rössler 2018: 93). Privatheit als Privatsphäre umschreibt den Raum, in dem sich autonome Selbstentwicklung vollziehen kann und vollzieht – sie ist „das herausgehobene Refugium der Selbstverwirklichung" (Weiß/Groebel 2013: 19). Wie oben gezeigt entwickelt sich Identität aber – und vor allem – auch durch soziale Interaktion. Diese Interaktion kann auch digital vermittelt sein. Es reicht für das Privatheitsverständnis nicht, nur auf eine engere persönliche physische Sphäre abzustellen, sondern auch weiterreichende soziale Räume unter den Privatheitsbegriff zu subsumieren. Rössler und Trepte haben den sozialen Aspekt von (relationaler) Privatheit herausgearbeitet (Rössler 2001:

234–251, Rössler 2018, Trepte 2016). Weitere neue Privatheitskonzepte weisen zudem auf das Verhältnis von Privatheit, Autonomie und Demokratie als supraindividuelle, gesamtgesellschaftliche Wirkungsdimensionen hin (Becker 2017a, Becker/Seubert 2016, Gusy 2015). Koops et al. haben 2017 die vielschichten Privatheitsdimensionen entlang ihrer jeweils relevanten Sphäre und ihrer freiheitsbezogenen Schutzrichtungen in einer relativ umfassenden Matrix aufgespannt (s. Abb. 2), die nachvollziehbar aufzeigt, wieso Privatheit und Autonomie auch bei digitaler Mediennutzung umfassend berührt sind.

Abb. 2: Typologisierung von Privatheitskonzepten („A typology of privacy")



Quelle: Koops/Newell/Timan/Škorvánek/Chokrevski/Galič 2017: 566.

In der Zusammenschau des Spektrums unterschiedlicher Persönlichkeitssphären (höchstpersönlich/intim, privat, sozial, öffentlich) und den unterschiedlichen freiheitsbezogenen Schutzrichtungen (Freiheit von etwas, und Freiheit zu etwas – hier in erster Linie die der Persönlichkeitsentwicklung) liegt der Aspekt der informationellen Privatheit quer über alle Sphären und berührt sowohl die negative als auch die positive Ausprägung eines Rechts auf Privatheit. Über medial vermittelte Kommunikation können alle Formen der intimen, persönlichen, sozialen und öffentlichen Formen der Persönlichkeitsentwicklung und -entfaltung berührt sein; informationelle Privatheit erscheint daher als fundamental wichtig „in allen sozialen Bezügen, in denen Subjekte leben" (Rössler 2003: 33).

4.2 Reichweite informationeller Privatheit bei der digitalen Mediennutzung Heranwachsender

Anhand einiger exemplarischer Bereiche sollen die vielfältigen Berührungspunkte informationeller Privatheit bei der Nutzung digitaler Medien und deren Autonomiegesichtspunkte aufgefächert werden. Ausgangspunkt der folgenden Überlegungen ist der Umstand der Rückkanalfähigkeit digitaler Kommunikation, und damit die Möglichkeit der Beobachtbarkeit. Durch die Nutzung digitaler Kommunikationsmedien fallen nicht nur die Kommunikations*inhalte* als Daten an, sondern auch die technischen Verkehrs- oder Nutzungsdaten in Form von *Metadaten*: Wer mit wem kommuniziert, von wo aus, worüber und wie lange; wer wann welche Angebote und Dienste nutzt; die Praxis der Beobachtung, Sammlung und Auswertung (auch) dieser Daten kommunikativer Kontakte ist weit verbreitet und Grundlage datenbasierter Monetarisierungsstrategien und Geschäftsmodelle. Durch die Auswertung von Inhalts- und Nutzungsdaten können Anbieter datenbasierte Gegenbilder in Form von Persönlichkeitsprofilen oder Segmenten generieren, die als Input in algorithmischen Selektionsverfahren wiederum Einfluss auf den Output gegenüber diesen Personen haben. Auf diese Weise entstehen Feedback-Loops auf Basis der mathematischen Normalisierung der Persönlichkeitsfacetten, der „Schubladisierung" von Identitätsaspekten auch bei Heranwachsenden. Die digitalen Abbilder von Einzelnen sind dabei relativ statisch und können dynamische Entwicklungen und Veränderungen sowie Kontextspezifika nur schlecht abbilden. Dadurch entsteht das Risiko, dass die Profilierung von Heranwachsenden eher den „Schnappschuss" eines Stadiums der Persönlichkeitsentwicklung zu einem bestimmten Zeitpunkt und in einem bestimmten Kontext darstellen, der zügig durch neue oder erweiterte Selbstkonzepte oder Kontextveränderungen abgelöst wird und damit nicht mehr valide ist. Durch die Zementierung digitaler Abbildung aber entstehen Formen digitaler Personae – „Datenschatten" –, die nur zum Teil selbst kreiert sind, sondern durch externe Beobachtung ermittelt, berechnet und profiliert wurden (Roosendaal 2010). Die personalisierten Dienstleistungen entsprechen so nicht der tatsächlichen jeweiligen Persönlichkeit, sondern produzieren Ergebnisse auf Grundlage eines früheren, unscharfen Abbilds der Persönlichkeitsfacetten und Interessen der jeweils berechneten Person; sie sind zeitlich und kontextuell desintegriert. Durch Output auf Grundlage invalider Inputs aber werden ggf. Entwicklungsprozesse angestoßen, die sich ohne die Beobachtungspraktiken nicht realisiert hätten (zu den epistemischen Verschränkungen von Datenanalyse und Subjektentscheidung vgl. Albers 2017: 25f.). Der Autonomiebezug wird bereits hier deutlich.

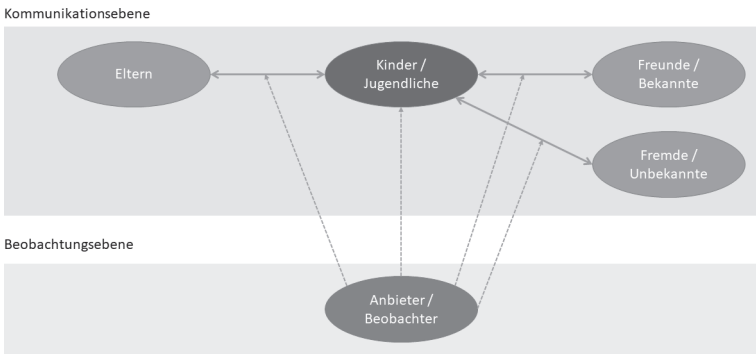
Auch die Frage der Kenntnis der Beobachtbarkeit und Beobachtung hilft bei Kindern und Jugendlichen nicht als moderierender Effekt: Haben minderjährige Nutzer*innen Kenntnis von der Beobachtung und Profilierung, so könnte dies bereits zu einem angepassten, jeweils vermeintlich sozialadäquaten Verhalten führen. Eine wirklich autonome Persönlichkeitsentwicklung wäre so nicht gewährleistet. Bei Nicht-Kenntnis von Profiling-Praktiken dagegen würden sich Minderjährige entsprechend unbeobachtet verhalten und damit ggf. besonders intime bzw. private Verhaltensmuster offenbaren. Diese aber wären Inbegriff der experimentellen Entwicklungsphase von Heranwachsenden, die nur deswegen an den Tag gelegt werden, *weil* man sich unbeobachtet fühlt. Beide Alternativen weisen insoweit deutliche Autonomiebezüge auf.

Mit der umfassenden Beobachtung und algorithmischen Informationsselektion erfolgt zudem eine autonomierelevante Aufmerksamkeitssteuerung (Dreyer/Heldt 2021). Durch predictive analytics werden die Wahrscheinlichkeiten relevanter – oder eher: aufmerksamkeits- und verweildauermaximierender – Informationen berechnet und entsprechende Informationen priorisiert. Dadurch entstehen niedrigschwellige, individualisierte Informationsangebote und „Feeds", die Einfluss auf die Entscheidungsfreiheit nehmen. Die gleichen Algorithmen steuern Teile des sozialen Austauschs und der Selbstdarstellung auf Plattformen und darüber hinaus: Sie entscheiden für den Einzelnen, welche Informationen, Updates und Likes von welchen Freunden und Bekannten zu sehen sind – und welche nicht. Diese Selektion erfolgt auch hinsichtlich der eigenen Informationen, und welche der eigenen Freund*innen und Bekannten diese Informationen von mir bzw. über mich sieht. Damit weisen diese Praktiken auch Berührungspunkte zum eigenen Beziehungs- und Identitätsmanagement (Schmidt 2006, Schmidt 2017) auf: Nicht mehr der Einzelne entscheidet, wer was wann über ihn weiß, sondern die Selektions- und Rankingalgorithmen von Plattformen. Aufmerksamkeitssteuerung durch Algorithmen ist auch Steuerung von sozialen Beziehungen, Kontexten und wahrgenommener Identität (Thimm/Bächle 2019: 80, Einspänner-Pflock 2017: 101). Beides – die aufmerksamkeitsbezogene Steuerung der Inhalte anderer und die Steuerung der Rezeption der eigenen Inhalte bei anderen – hat hohe Relevanz für die Persönlichkeitsentwicklung und -entfaltung (Becker 2017b).

Deutlich wird bei den hier aufgezeigten autonomierelevanten Praktiken der Beobachtung und Aufmerksamkeitssteuerung im Digitalen, dass unterschiedliche Arten und Herkunftssphären von Daten dabei eine Rolle spielen (s. Abb. 3): Teile der Beobachtung und Auswertung fußen auf bewusst selbst preisgegebenen Informationen von Kindern und Jugendlichen, wei-

tere erfolgen auf Grundlage unbewusst preisgegebener bzw. beiläufig erzeugter Informationen im Rahmen der Mediennutzung. Daneben können auch Dritte (Eltern, Freunde, Bekannte, Unbekannte) die Ursache für die Preisgabe von Daten gebildet haben – etwa durch absichtlich offengelegte Informationen oder durch unbewusst entstandene Daten im Rahmen der Kontaktaufnahme oder durch die Auswertung von Kommunikationsinhalten.

Abb. 3: Kommunikations- und Beobachtungsebene



5. *Digitale Mediennutzung von Kindern als Experimentierraum der Persönlichkeitsentwicklung: Regulierungsnotwendigkeit und Steuerungsherausforderungen*

Der kurze Überblick hat gezeigt, dass bei der digitalen Mediennutzung von Kindern und Jugendlichen eine Reihe von Beobachtungs- und Auswertungspraktiken stattfindet, die Berührungspunkte zu Autonomie aufweisen. Dabei scheinen unterschiedliche Schutzdimensionen auf: Erstens nutzen Heranwachsende Kommunikationsmedien als digitale Experimentierräume der Persönlichkeitsentwicklung. Die Beobachtung dieses Aufwachsens in Online-Umgebungen erscheint grundsätzlich als Eingriff in die besonders schützenswerte Privatsphäre von Kindern und Jugendlichen. Zweitens sind die dabei entstehenden digitalen Gegenbilder und Persönlichkeitsprofile angesichts der fluiden Selbstkonzepte bei Heranwachsenden schnell nicht mehr valide. Durch die Speicherung nicht mehr aktueller Persönlichkeitsprofile und der Selektion von darauf basierenden Einzelinhalten wird Einfluss genommen auf das Informations-, Identitäts- und Beziehungsmanagement der minderjährigen Nutzer*innen und so eben-

falls das Recht auf unbeeinträchtigte Persönlichkeitsentwicklung berührt. Und drittens weisen prädiktive Verfahren Potenziale für autonomierelevante self-fulfilling prophecies auf, wenn sie sich zwischen profilbasierten Anzeige- und empfängerseitigen Auswahlentscheidungen zu Selbstverstärkungseffekten hochschaukeln (Dreyer 2018c).

Diese drei Aspekte verweisen auf den staatlichen Schutzauftrag im Jugendschutz, dennoch stellt sich die Frage, ob eine gesetzliche Intervention in der Folge notwendig wird? Das wäre zu bejahen, wenn es einen Schutzbedarf von Kindern und Jugendlichen gibt. Von einem solchen Bedarf ist wie gezeigt dann auszugehen, wenn die Heranwachsenden keine Möglichkeit haben, den autonomierelevanten Praktiken zu entgehen, oder gar keine Kenntnis von diesen Verfahren haben. Ihnen fehlte dann dasjenige Wissen, das für eine kritische Reflexion und ein entsprechend angepasstes, autonomes Handeln in der Nutzungspraxis erforderlich wäre.

5.1 Kenntnis der Datenverarbeitungspraktiken und datenreflektiertes Handeln

Für die Bestimmung eines möglichen Auslösens des gesetzgeberischen Schutzauftrags im Bereich eines spezifischen Kinderdatenschutzes ist es notwendig, den Blick über theoretische Ansätze hinaus (Peter/Valkenburg 2011) auch auf empirische Untersuchungen zu werfen, die Evidenzen hinsichtlich der Kenntnisse von Datenverarbeitungspraktiken von Kindern und Jugendlichen zu Tage gefördert haben und Hinweise auf ein entsprechend geringes oder hohes datenreflektiertes Handeln liefern. Die einschlägigen Erhebungen (Schenk et al. 2012, Trepte/Masur 2015, DIVSI/SINUS 2014, BITKOM 2014, Livingstone et al. 2018) weisen im Kern und entsprechend der oben beschriebenen auch kognitiven Entwicklungen in Kindheit und Jugend eine deutliche Altersabhängigkeit der datenbezogenen Kenntnisse und des Handelns auf.[2] Der Einfachheit halber differenziert der Beitrag hier die Altersgruppen der 0-6-Jährigen, der 7-13-Jährigen und der 14-18-Jährigen:

- Die Untersuchungen zum Privatheitsverständnis von kleineren Kindern (0-6 Jahre) weisen darauf hin, dass diese Altersgruppe in der Regel

2 Die hier gemachten Aussagen beruhen zusätzlich auf den Vorabergebnissen qualitativer Befragungen von Kindern und Jugendlichen zu Privatsphäre und Datenschutz im Herbst 2019 im Rahmen des Projekts „Datafied Childhood“ von Stephan Dreyer, Claudia Lampert und Kira Thiel; die Ergebnisse sind noch nicht veröffentlicht.

nur ein binäres Konzept von Privatheit entwickelt hat. Unterschieden wird von Kindern in dieser Altersgruppe nur zwischen Alleinsein versus Zusammensein (Livingstone et al. 2018, Birkner 2005).

- Die Befragungen von älteren Kindern (7-13 Jahre) zeigen, dass in diesem Alterssegment ein Verständnis von Privatheit grundsätzlich vorhanden ist (Schenk/Niemann/Reinmann/Roßnagel 2012, Livingstone et al. 2018). Hier entwickeln sich Konzepte unterschiedlich privater Räume und Formen verschieden privater und offener Sphären, die stark kontextabhängig sind. Dieses Grundverständnis wird in Ansätzen auf digitale Medienumgebungen übertragen, erfolgt dort aber fokussiert auf Formen relationaler Privatheit, d.h. die Einordnung des Privatheitsgrades von Informationen und Interaktionen erfolgt praktisch ausschließlich auf Grundlage des bekannten oder vermeintlichen Gegenübers, z.B. Verwandte, Freund*innen, Bekannte, Unbekannte (Einspänner-Pflock 2017, Litt 2012). In dieser Altersgruppe erlangen die meisten Kinder erste Kenntnisse von Überwachbarkeit im Netz generell, haben teilweise etwas von Verfolgbarkeit oder Beobachtbarkeit durch „Fremde" gehört, ordnen dies aber noch nicht regelmäßig einzelnen Akteuren zu.
- Bei Jugendlichen ab 14 Jahren wird deutlich, dass die Heranwachsenden bereits eine gute Kenntnis der grundsätzlichen Problematik von Überwachbarkeit und Auswertbarkeit digitaler Mediennutzung haben (DIVSI/SINUS 2014). Sie weisen regelmäßig eine starke Erwartungshaltung in Richtung einer kontextuellen Privatheit auf, d.h. sie bewerten Privatheit vor allem anhand des Geheimnisinteresses einer bestimmten Information oder Konversation gegenüber Personen und Akteur*innen, denen das Wissen darüber nicht zusteht bzw. zustehen sollte (Nissenbaum 2010, Livingstone et al. 2018:19). Dabei nutzen sie meist einfache Risikoheuristiken, die bei einleuchtenden Affordanzen und kommunikativen Netzwerkeffekten aber schnell in den Hintergrund treten können: „Eigentlich gefällt mir nicht, dass jemand beobachten kann, mit wem ich worüber spreche, aber auf bestimmten Plattformen erreiche ich meine besten FreundInnen am einfachsten." Auch die Risikozuschreibung an einzelne Akteure zeigt die Oberflächlichkeit des Wissens um Datenverarbeitungspraktiken: Aus Sicht der Jugendlichen ist es in der Regel der App-Anbieter, der Webseitenanbieter, der Spiele-Publisher, der die Nutzer beobachtet. Die Kenntnis angebotsübergreifender Möglichkeiten der systematischen Beobachtung, Auswertung und Profilierung (WhatsApp/Instagram/Facebook; FitBit/Youtube/Google) ist nur einzeln festzustellen. Das Wissen um komplexere angebots- und geräteübergreifende Tracking-Techniken, die sich einer Viel-

zahl ineinandergreifender Dienste und Anbieter (insbesondere sog. ad services) bedient, fehlt in diesem Alterssegment praktisch völlig.

Der Abgleich von Schutzzielen und den Hinweisen auf die aktuelle Kenntnis schutzzielrelevanter Praktiken und einem entsprechenden Handeln weist durchgängig signifikante Diskrepanzen auf. Insbesondere durch die systematische Beobachtung und Sammlung kommunikationsbezogener (Meta-)Daten bei der Mediennutzung Minderjähriger entstehen Gefährdungen für die Gewährleistung einer freien und unbeeinträchtigten Persönlichkeitsentwicklung. Dieses Risikopotenzial entsteht zum einen durch ein wachsendes Bewusstsein bezüglich des Beobachtet-Seins bei Heranwachsenden, was nicht nur theoretisch zu einem vermeintlich sozial angepassten – und damit unfreiem – Online-Verhalten führen kann. Zum anderen können durch die systematische Beobachtung und eine darauf basierende Persönlichkeitsprofilierung Situationen entstehen, in denen Selektionen, Ausspielungen, Priorisierungen, aber auch De-Priorisierungen zu einer algorithmisierten „De-Autonomisierung" der Persönlichkeitsentwicklung führen können. Die Persönlichkeitsfacetten Minderjähriger entwickeln sich (schlimmstenfalls) in jene Richtungen, die von profilbildenden Algorithmen berechnet und in Selbstverstärkungskaskaden zementiert werden. Gegen derartige Effekte haben Kinder und Jugendliche wenig Handhabe, wenn sie kaum etwas über die Umstände ihrer Herkunft und Entstehung wissen und keine entsprechenden Reflexionsebenen oder Abwehrstrategien entwickeln können. Neben den autonomiebezogenen Beeinträchtigungen scheinen auch hier letzten Endes demokratiebezogene Mündigkeitsproblematiken auf (vgl. Berson/Berson 2006).

5.2 Möglichkeiten und Grenzen rechtlicher Steuerung

Der Auftrag an die Gesetzgebung, eine freie Persönlichkeitsentwicklung auch im Digitalen zu gewährleisten, erscheint angesichts der empirischen Evidenzen gerechtfertigt. Die anschließende Frage, die sich stellt, ist dann, ob und in welcher Form gesetzliche Vorgaben hier helfen können – und mit welchen Steuerungsinstrumenten dies umgesetzt werden könnte. Die rechtliche Bearbeitung von Privatheitsrisiken bietet sich durch Interventionen insbesondere mit Blick auf die oben gezeigten vier Akteurskonstellationen an (Abb. 3): Erstens im Verhältnis von Kind und datenverarbeitenden Anbietern eines Dienstes, zweitens im Verhältnis von Kind und Erziehungsberechtigten, drittens im Verhältnis von Kind und befreundeten oder bekannten Kommunikationspartner*innen und viertens im Verhält-

nis von Kind und fremden oder unbekannten Kommunikationspartner*innen. Doch bei jeder der vier Konstellationen sieht sich rechtliche Steuerung (unterschiedlichen) komplexen Herausforderungen gegenüber:

- Auf den ersten Blick vielversprechend erscheint es, wenn gesetzliche Regelungen an die beobachtenden bzw. datenverarbeitenden Anbieter eines Onlinedienstes, den Kinder und Jugendliche nutzen, anknüpfen. Hier könnten Beschränkungen (z.B. Verarbeitungsverbote), besondere Vorgaben (z.B. kindgerechte Voreinstellungen) oder Transparenzpflichten genau gegenüber jenen Akteur*innen gemacht werden, die den ersten Zugriff auf die genutzte Technologie und Infrastruktur haben. Alternativ könnte der Gesetzgeber das Mindestalter für die Nutzung entsprechender Dienste vorgeben. Dieser Ansatz aber weist Problempotenziale auf, da der Anbieter dafür genau wissen müsste, welche der Nutzenden eine minderjährige Person ist. Folgen müssten also Maßnahmen, die Heranwachsende online als solche erkennbar machten oder im Rahmen von Altersüberprüfungsverfahren zwingend neue Datensätze produzieren würden, z.B. Datenerhebung zu Zwecken des Datenschutzes. Auch die Online-Erkennbarkeit des Umstandes, dass es sich bei Nutzer*innen um eine minderjährige Person handelt – ggf. sogar mit Informationen zum konkreten Alter oder einer bestimmten Altersgruppe – hat aus Sicht des Jugendschutzes mehr Nach- als Vorteile (Dreyer 2018b). Zum Datenschutzdilemma hinzu träte also ein Erkennbarkeitsdilemma: Der Steuerungsansatz für einen besseren Datenschutz könnte im Extrem sogar zu einer Verschlechterung des Kinderschutzes führen.
- Auch ein gesetzliches Intervenieren in das Verhältnis von Kindern und Eltern, etwa durch die Konkretisierung elterlicher Schutzpflichten oder gar Untersagungsverbote bezüglich der kindlichen Nutzung bestimmter Dienste könnte zu einem Dilemma führen: Zum einen stehen Familienbeziehungen unter besonderem (Privatheits-)Schutz. Intrafamiliale Beziehungen bilden aus Sicht des Rechts zunächst eine Sphäre der rechtsaversen Selbstgestaltung und -verständigung. Es gilt das Primat des Erziehungsrechts der Eltern, vor allem gegenüber Eingriffen und Bevormundung durch den Staat. Untersuchungen zeigen allerdings eine hohe Zahl von Eltern, die Handlungserwartungen ausdrücklich an den Staat und die Anbieter*innen formulieren (Brüggen et al. 2017). Soweit man dadurch bereits in das Gebiet des Wächteramts des Staates als Kompensation elterlicher Motivations- oder Möglichkeitsausfälle bei der Übernahme ihrer Erziehungsverantwortung gelangen sollte (Dreyer 2019), müsste man in Kauf nehmen, dass der*die Gesetzge-

ber*in hier den Bereich unmittelbarer staatlicher Steuerung von Familienbeziehungen und Erziehungspraktiken regulieren würde (Dreyer 2018a: 191).

- Rechtliche Anknüpfungspunkte an Kommunikationen im Verhältnis von Minderjährigen zu ihren Freund*innen und Bekannten stoßen mit Blick auf das Fernmeldegeheimnis an verfassungsrechtliche Grenzen: Digital vermittelte Individualkommunikation ist ein Bereich, der besonders vor der Einsichtnahme durch den Staat und Dritte geschützt ist. Das Dilemma staatlicher Regelungen besteht hier darin, dass die Gesetzgebung etwas regeln würde, was der Staat nicht sehen soll.
- Ähnlich verhält es sich mit Regulierungsansätzen, die im Verhältnis von Heranwachsenden und unbekannten Dritten Wirkungen entfalten sollen. Auch hier besteht das Problem der vor Einsichtnahmen geschützten Individualkommunikation. Es bliebe theoretisch die Möglichkeit, die Offenbarung von Daten Minderjähriger durch Dritte strafrechtlich zu sanktionieren (über den Bereich hinaus, der derzeit von §§ 186, 187, 201, 201a StGB umfasst wird). Das Dilemma bleibt dann, dass klassisches Strafrecht nicht als unterstützende Steuerungsressource im Vorfeld von Datenweitergabe wirkt, sondern erst als repressive Sanktionierung.

6. *Fazit*

Aufwachsen heißt, sich auszuprobieren – auch im digitalen Raum. Die bei der Beobachtung dieser Interaktionen anfallenden Daten zeigen domänenspezifische Facetten von sich im Fluss befindlichen Selbstkonzepten der Heranwachsenden. Sie manifestieren sich durch die Beobachtungs- und Auswertungspraktiken im Netz in datenbasierten Gegenbildern, die relativ statisch, dekontextualisiert und kontextübergreifend vorgehalten werden. Die Profile dienen algorithmischen Selektionsverfahren als Input und bestimmen auf dieser Grundlage den Output automatisierter Verfahren, mit Einfluss auf die wahrgenommenen Informationen über die Welt, über Freund*innen und Dritte, und die Wahrnehmbarkeit eigener Informationen auf der Seite von Dritten. Damit weist die Beobachtbarkeit der Mediennutzung in mehrfacher Hinsicht Autonomiebezüge auf: Allein das Bewusstsein oder die Sorge um die Beobachtbarkeit der Kommunikation kann zu Verhaltensanpassungen führen. Die gewollte Unkenntnis der Beobachtbarkeit ist mit Blick auf zu sichernde Autonomie keine Alternative. Unabhängig von einer solchen Kenntnis potenzieren, prädiktieren und normalisieren algorithmische Selektionsverfahren auf Grundlage von Be-

obachtungsdaten die Persönlichkeitsentwicklung Heranwachsender. Sie weisen durch ihre Einflüsse auf das Informations-, Identitäts- und Beziehungsmanagement Heranwachsender ein hohes Beeinträchtigungspotenzial für die Persönlichkeitsentwicklung auf. Rechtliche Steuerungsmöglichkeiten zur Gewährleistung einer unbeeinträchtigten Persönlichkeitsentwicklung geraten hier indes gleich in mehrere Dilemmata; rechtliche Steuerung hat nur begrenzte Möglichkeiten. Wo es aber als Steuerungsressource genutzt werden kann, werden radikalere Vorgaben und konsequentere Durchsetzung dringend nötig.

Als spezifisch kinderbezogene Handlungsoptionen, durch die sich der Staat den aufgezeigten Regulierungsherausforderungen stellen könnte, erschienen vor allem ein Verbot nutzungsbasierten Trackings und Profilings, der Nicht-Einsatz prädiktiver Verfahren, altersangemessene Transparenzformen, kontextsensitive Informationen und „Tabula Rasa"-Möglichkeiten während und zum Ende der Kindheit.

Literatur

Albers, Marion (2017): *Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen*. In: Friedewald, Michael / Lamla, Jörn / Roßnagel, Alexander (Hg.): Informationelle Selbstbestimmung im digitalen Wandel. Wiesbaden: Springer, S. 11–35.

Andresen, Sabine (2018): *Kindheit*. In: Böllert, Katrin (Hg.): Kompendium Kinder- und Jugendhilfe. Wiesbaden: Springer, S. 365–379.

Becker, Carlos (2017a): *Privatheit und kommunikative Freiheit im Internet*. In: Jacob, Daniel / Thiel, Thorsten (Hg.): Politische Theorie und Digitalisierung. Baden-Baden: Nomos, S. 45–82.

Becker, Carlos (2017b). *Kritische Theorie des Privaten*. In: Friedewald, Michael / Lamla, Jörn / Roßnagel, Alexander (Hg.): Informationelle Selbstbestimmung im digitalen Wandel. Wiesbaden: Springer, S. 147–168.

Becker, Carlos / Seubert, Sandra (2016): *Privatheit, kommunikative Freiheit und Demokratie*. In: Datenschutz und Datensicherheit (DuD) 2, S. 73–78.

Berson, Ilene R. / Berson, Michael (2006): *Children and Their Digital Dossiers: Lessons in Privacy Rights in the Digital Age*. In: International Journal of Social Education 21 (1), S. 135-147.

Birkner, Enrico (2005): *Auswirkungen der Raumstruktur eines Kindergartens auf das kindliche Verhalten und Erleben*. Dresdner Arbeiten zur Architekturpsychologie. Online verfügbar unter: http://architekturpsychologie-dresden.de/ddarbeiten/birkner_kindergarten.pdf (Abfrage am: 10.06.2020).

BITKOM (Hg.) (2014): *Jung und vernetzt. Kinder und Jugendliche in der digitalen Gesellschaft*. Berlin. Online verfügbar unter: https://www.bitkom.org/noindex/Publikationen/2014/Studien/Jung-und-vernetzt-Kinder-und-Jugendliche-in-der-digitalen-Gesellschaft/BITKOM-Studie-Jung-und-vernetzt-2014.pdf (Abfrage am: 10.06.2020).

Brüggen, Niels / Dreyer, Stephan / Drosselmeier, Marius / Gebel, Christa / Hasebrink, Uwe / Rechlitz, Marcel (2017): *Jugendmedienschutzindex. Der Umgang mit onlinebezogenen Risiken*. In: FSM – Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V. (Hg.): Ergebnisse der Befragung von Heranwachsenden und Eltern. Berlin.

Di Fabio, Udo (2019): Art. 2 I Rn. 2. In: Maunz, Theodor / Dürig, Günter (Hg.): Grundgesetz-Kommentar, 89. EL, Oktober 2019. München: Beck.

DIVSI/SINUS-Institut Heidelberg (2014): *Kinder, Jugendliche und junge Erwachsene in der digitalen Welt*. DIVSI U25-Studie. Hamburg: DIVSI. Online verfügbar unter: https://www.divsi.de/wp-content/uploads/2014/02/DIVSI-U25-Studie.pdf (Abfrage am: 10.06.2020).

Dreyer, Stephan (2018a): *Entscheidungen unter Ungewissheit im Jugendmedienschutz. Untersuchung der spielraumprägenden Faktoren gesetzgeberischer und behördlicher Entscheidungen mit Wissensdefiziten*. Baden-Baden: Nomos.

Dreyer, Stephan (2018b): *On the Internet, nobody knows you're a kid. Zur (Nicht-)Erkennbarkeit Minderjähriger in digitalen Medienumgebungen*. In: Medien + Erziehung 62, S. 65-78.

Dreyer, Stephan (2018c): *Predictive Analytics aus der Perspektive von Menschenwürde und Autonomie*. In: Hoffmann-Riem, Wolfgang (Hg.): Big Data - Regulative Herausforderungen. Baden-Baden: Nomos, S. 135–143.

Dreyer, Stephan (2019): *Rechte von Kindern und Jugendlichen, Elternprivileg und Wächteramt des Staates: Medienerziehung aus der Perspektive der Verfassung*. In: Hajok, Daniel / Fleischer, Sandra (Hg.): Medienerziehung in der digitalen Welt. Grundlagen und Konzepte für Familie, Kita, Schule und Soziale Arbeit. Stuttgart: Kohlhammer, S. 86-102.

Dreyer, Stephan / Heldt, Amélie (im Druck): *Algorithmische Selektion und Privatheit. Aufmerksamkeitssteuerung durch Social Media-Plattformen als Autonomieeingriff?* In: Hennig, Martin et al. (Hg.): Verantwortung in digitalen Kulturen. Privatheit im Geflecht von Medien, Recht und Gesellschaft.

Dreyer, Stephan / Lampert, Claudia / Schulze, Anne (2014): *Kinder und Onlinewerbung: Erscheinungsformen von Werbung im Internet, ihre Wahrnehmung durch Kinder und ihr regulatorischer Kontext*. Leipzig: Vistas.

Einspänner-Pflock, Jessica (2017): *Privatheit im Netz: Konstruktions- und Gestaltungsstrategien von Online-Privatheit bei Jugendlichen. Medien-Kultur-Kommunikation*. Wiesbaden: Springer.

Greve, Werner / Thomsen, Tamara (2019): *Entwicklungspsychologie: Eine Einführung in die Erklärung menschlicher Entwicklung*. Wiesbaden: Springer.

Gusy, Christoph (2015): *Privatheit und Demokratie*. In: Kritische Vierjahreszeitschrift für Gesetzgebung und Rechtswissenschaft (KritV) 98 (4), S. 430–461.

Koops, Bert-Jaap / Newell, Bryce Clayton / Tjerk, Timan / Chokrevski, Tomislav / Gali, Maša (2017): *A Typology of Privacy*. In: University of Pennsylvania Journal of International Law 38 (2), S. 483-575.

Litt, Eden (2012): *Knock, Knock. Who's There? The Imagined Audience*. In: Journal of Broadcasting & Electronic Media 56(3), S. 330-345.

Livingstone, Sonia / Stoilova, Mariya / Nandagiri, Rishita (2018): *Children's Data and Privacy Online: Growing up in a Digital Age: An Evidence Review*. London: London School of Economics and Political Science. Online verfügbar unter: https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf (Abfrage am 3.10.2020).

Ochs, Carsten (2019): *Teilhabebeschränkungen und Erfahrungsspielräume: eine negative Akteur-Netzwerk-Theorie der Privatheit*. In: Behrendt, Hauke / Loh, Wulf / Matzner, Tobias / Misselhorn, Catrin (Hg.): Privatsphäre 4.0. Stuttgart: J.B. Metzler, S. 13–31.

Peter, Jochen / Valkenburg, Patti M. (2011): *Adolescents' Online Privacy: Toward a Developmental Perspective*. In: Trepte, Sabine / Reinecke, Leonard (Hg.): Privacy Online. Berlin / Heidelberg: Springer, S. 221-234.

Roosendaal, Arnold P. (2010): *Digital personae and profiles as representations of individuals*. In: Bezzi, Michele / Duquenoy, Penny / Fischer-Hübner, Simone / Hansen, Marit / Zhang, Ge (Hg.): Privacy and Identity Management for Life. Berlin, Heidelberg: Springer, S. 226-236.

Rössler, Beate (2001): *Der Wert des Privaten.* Frankfurt am Main: Suhrkamp.

Rössler Beate (2003): *Anonymität und Privatheit*. In: Bäumler, Herbert / von Mutius, Albert (Hg.): Anonymität im Internet. Wiesbaden: Vieweg+Teubner, S. 27-40.

Rössler, Beate (2018): *Privatheit, Autonomie, Recht*. In: Baer, Susanne / Sacksofsky, Ute (Hg.): Autonomie im Recht - Geschlechtertheoretisch vermessen. Baden-Baden: Nomos, S. 93–118.

Schenk, Michael / Niemann, Julia / Reinmann, Gabi / Roßnagel, Alexander (Hg.) (2012): *Digitale Privatsphäre: Heranwachsende und Datenschutz auf sozialen Netzwerkplattformen*. Berlin: Vistas.

Schmidt, Jan-Hinrik (2006): *Social Software: Onlinegestütztes Informations-, Identitäts- und Beziehungsmanagement*. In: Forschungsjournal Soziale Bewegungen 19(2), S. 37–47.

Schmidt, Jan-Hinrik (2017): *Das neue Netz: Merkmale, Praktiken und Folgen des Web 2.0*. Konstanz: Halem.

Siegler, Robert S. / Eisenberg, Nancy / DeLoache, Judy S. / Saffran, Jenny (2016): *Entwicklungspsychologie im Kindes- und Jugendalter*. Berlin, Heidelberg: Springer.

Spickhoff, Andreas (2018): *Vorbemerkung zu §§ 104 ff*. In: Säcker, Franz Jürgen et al.: Münchener Kommentar zum Bürgerlichen Gesetzbuch, 8. Auflage. Müchen: Beck.

Thimm, Caja / Bächle, Thomas C. (2019): *Autonomie der Technologie und autonome Systeme als ethische Herausforderung*. In: Rath, Matthias / Krotz, Friedrich / Karmasin, Matthias (Hg.): Maschinenethik. Ethik in mediatisierten Welten. Wiesbaden: Springer VS, S. 73-87.

Trepte, Sabine / Masur, Philipp K. (2015): *Privatheitskompetenz in Deutschland. Ergebnisse von zwei repräsentativen Studien*. Bericht vom 18. November 2015. Stuttgart: Universität Hohenheim.

Trepte, Sabine (2016): *Die Zukunft der informationellen Selbstbestimmung – Kontrolle oder Kommunikation?* In: Stiftung Datenschutz (Hg.): Die Zukunft der informationellen Selbstbestimmung. Berlin: Erich Schmidt, S. 159–170.

Weiß, Ralph / Groebel, Jo (2013): *Privatheit im öffentlichen Raum. Medienhandeln zwischen Individualisierung und Entgrenzung*. Wiesbaden: Springer VS.

Privatheit und Selbstbestimmung von Kindern in der digitalisierten Welt: Ein juristischer Blick auf die Datenschutz-Grundverordnung

Alexander Roßnagel

Abstract

Informationstechniken zu nutzen, ist für Kinder heute selbstverständlich. Viele von ihnen wachsen als „Digital Natives" auf. Sie leben bereits in der digitalen Welt. Andere werden im Freundeskreis, in den Familien oder in der Schule immer wieder mit der Nutzung von informationstechnischen Geräten konfrontiert. Alle sind jedoch von früher Kindheit an Objekt von informationstechnischen Überwachungspraktiken. Von Kindern werden daher vielfältig und umfangreich personenbezogene Daten verarbeitet. Da diese zwar die Vorteile der Datenverarbeitung in Anspruch nehmen, ihre Risiken aber nicht ausreichend erkennen und bewerten können, bedürfen sie eines besonderen – auch datenschutzrechtlichen – Schutzes. Der folgende Beitrag beschreibt diese besondere Schutzbedürftigkeit von Kindern bei der Verarbeitung personenbezogener Daten (1.), erläutert den völker- und verfassungsrechtlichen Rahmen ihres rechtlichen Schutzes (2.) und untersucht, wie dieser Schutzauftrag von der Datenschutzgrundverordnung ausgefüllt wird (3.). Anlässlich der Evaluation dieser Verordnung vier Jahre nach ihrem Inkrafttreten und zwei Jahre nach ihrem Geltungsbeginn in den Mitgliedstaaten prüft er, ob sie diesem Anspruch vollauf gerecht wird und entwickelt Vorschläge, den Schutz von Kindern in der Datenschutz-Grundverordnung zu verbessern (4.). Schließlich fasst er die Erkenntnisse dieser Untersuchung zusammen und benennt den rechtspolitischen Handlungsbedarf (5.).

1. Der besondere Datenschutzbedarf von Kindern

Kinder wachsen heute in einer digitalisierten Welt auf. Sie sind Objekte der Datenverarbeitung im Säuglingsalter etwa durch Baby-Fon-Apps, im Kinderzimmer durch Smart Toys, Sprachassistenten (Wissenschaftliche

Dienste des Deutschen Bundestages 2019) und Tablet-Computer und im Kindergarten durch Lernroboter und Videoüberwachung. In der Schule werden ihre Verwaltungs-, Verhaltens- und Leistungsdaten durch Schulmanagementsysteme, biometrische Daten zum Zugangsschutz und ihre Konsumdaten durch Systeme für bargeldloses Bezahlen in der Schulkantine verarbeitet (Artikel 29-Datenschutzgruppe 2008). Außerdem sind sie in der Welt des Electronic Commerce und der Social Networks, des Ubiquitous Computing und des Big Data den gleichen Praktiken der Datensammelei und der Profilbildung unterworfen wie die Erwachsenen (Roßnagel/Richter 2017: 205).

Kinder nutzen im Lauf ihrer Entwicklung selbst digitale Technologien und Dienste immer mehr und intensiver. Viele von ihnen können als „Digital Natives" gelten, die mit der vielfältigen Verwendung dieser Medien aufwachsen. Nahezu alle nutzen Smartphones, sind Mitglieder in Social Networks, verwenden Messenger-Dienste, informieren sich über Suchmaschinen und kaufen Waren oder Unterhaltung über das Internet. Z.B. nutzten in der Altersgruppe der 6- bis 13-jährigen im Jahr 2016 57% der Kinder WhatsApp, 50% YouTube und 30% Facebook mehrmals in der Woche oder am Tag (MPFS 2016: 33). Das durchschnittliche Alter der Erstanmeldung bei Facebook lag 2016 bei 10 Jahren (MPFS 2016: 41). 2018 nutzten z.B. 73% der 14- bis 17-jährigen Instagram (MPFS 2018: 39). Zunehmend tragen sie auch Informationstechnik – wie Fitness-Armbänder oder Smart Watches – an ihrem Körper. Zur Unterstützung des Unterrichts oder zur Hilfe bei Hausaufgaben nehmen Schulkinder vielfältige Apps als Lernassistenz in Anspruch. Die Verarbeitung von Kinderdaten ist somit keine Ausnahme, sondern ein Massenphänomen (BITKOM 2017: 8).

Digitale Technologien und Dienste bieten für Kinder Chancen für die Entfaltung der eigenen Persönlichkeit, die Gemeinschaftsbildung und die Wahrnehmung vieler weiterer Freiheits- und Entwicklungsziele. Sie können sich ungefiltert informieren, mit ihrem sozialen Umfeld einfach kommunizieren und ihre Meinung frei äußern. Sie können ihre Freizeit mit elektronischen Spielen verbringen und dabei viel Spaß haben. Insbesondere Multi-User-Online-Spiele erlauben den Teilnehmern, in neue Rollen zu schlüpfen und in einer Phantasiewelt unterschiedliche Rollen und Realitäten zu erproben und auszuleben. Außerdem ist das Internet ein geeignetes Forum für die Selbstdarstellung. Jedes Kind kann versuchen, durch die Präsentation von Informationen über sich selbst sein Erscheinungsbild in der öffentlichen Wahrnehmung zu beeinflussen und durch die Rückmeldungen zu einer eigenen Identität zu finden. Dabei erlaubt die Virtualität und grundsätzliche Anonymität des Internets, in ganz unterschiedlichen Kontexten unterschiedliche Identitäten anzunehmen und damit die Selbst-

darstellung sehr facettenreich zu gestalten. Digitale Technologien ermöglichen schließlich neue Formen des Lernens, die relativ einfach zu nutzen und von hoher Attraktivität sind, sodass Barrieren, sich zu engagieren, sich anzustrengen und sich zu bilden, fast spielerisch überwunden werden können. Sie können digitale Räume bieten, die den Kindern Freiheit, Entwicklung und Entfaltung ermöglichen.

Digitale Technologien und Dienste hinterlassen allerdings zwangsläufig auch Datenspuren, die zur Überwachung und Verhaltenssteuerung durch unterschiedliche Interessierte genutzt werden können. Beispiele bieten Eltern, die die Aufenthaltsorte ihrer Kinder durch smarte Schulranzen oder Schlüsselanhänger mit GPS-Trackingfunktion ständig verfolgen. Sie können mit Ausspähprogrammen die Smartphones ihrer Kinder überwachen, auslesen und manipulieren. Sprachassistenten – auch in Form von smarten Puppen oder Kuscheltieren –, denen die Kinder ihre geheimen Wünsche und Sehnsüchte mitteilen, können für die Eltern zu Spionen ihrer Kinder werden. Auch wenn nicht die Eltern die entstehenden Daten auswerten – sie werden jedenfalls immer an die Anbieter dieser Dienstleistungen, oft in die USA, übertragen (Wissenschaftliche Dienste des Deutschen Bundestags 2019), die sie zu Persönlichkeitsprofilen zusammenfassen und für Werbezwecke nutzen (Friedewald/Karaboga/Zoche 2015). Solche Überwachungstechniken erfassen auch die Umwelt der Kinder, insbesondere andere Kinder, mit denen sie sich treffen, unterhalten oder spielen.

Schulen, die elektronische Medien einsetzen, um die Lernprozesse der Schüler zu unterstützen, erheben dadurch Verhaltens- und Leistungsdaten für jedes Kind, die personalisiert Auskunft über dessen Fähigkeiten, Intelligenz, Leistungsvermögen, Lernbereitschaft oder inhaltliche Interessen geben. Mit Learning Analytics-Systemen sind Selektionen der Schüler in Leistungsgruppen und letztlich auch prädiktive Aussagen zu ihren Entwicklungschancen möglich.

Daten, die Kinder in Internetplattformen selbst eingeben, ebenso wie die Daten, die Kinder bei der Nutzung von Internetdiensten unvermeidbar verursachen, führen deren Anbieter meist zu Nutzerprofilen zusammen und nutzen diese dafür, die Kinder gezielt anzusprechen und in ihren Meinungen und Verhaltensweisen – vor allem zu Werbezwecken – zu beeinflussen (Roßnagel/Richter 2017: 205).

Kinder können diese Risiken weniger gut vermeiden und sich gegen Eingriffe in ihre Grundrechte weniger gut wehren, als Erwachsene dies können. Sie sind leichter beeinflussbar und erliegen schneller einem sozialen Nutzungsdruck, der von anderen Kindern, Eltern oder Lehrern ausgeht. Auch haben sie vielfach ein hohes intrinsisches Interesse, für sie attraktive Internetangebote zu nutzen. Kinder haben grundsätzlich Vertrau-

en (auch ohne Anhaltspunkte dafür) und erfüllen Anforderungen zur Datenpreisgabe mit wenig Bedenken.

Die Selbstverständlichkeit im Umgang mit digitalen Medien ist allerdings nicht gekoppelt mit einem ausgeprägten Bewusstsein für die Risiken, die mit der Mediennutzung verbunden sind. Auch ausreichendes Risikowissen und Vermeidungskenntnisse fehlen (Roßnagel/Richter 2017: 205). Kinder haben in der Regel keine Vorstellungen, was es für sie bedeutet[1], dass das Internet nichts vergisst, dass Verbreitung und Nutzung und Aggregation der Daten im Internet für sie nicht mehr kontrollierbar sind, wenn sie einmal preisgegeben worden sind (Jandt/Roßnagel 2011: 637).

Das Wissen über Handlungsfolgen und zu Verhaltensmöglichkeiten muss sich bei Kindern erst nach und nach herausbilden und festigen. Das komplexe Zusammenwirken mehrerer Datenverarbeitungssysteme ist ihnen nicht bekannt, ebenso wenig die eigentlichen Geschäftsmodelle insbesondere von digitalen Diensten, die ihnen ihre Dienste scheinbar kostenlos anbieten. Ihnen ist nicht klar, dass aus den Daten, die sie preisgeben und die durch die Beobachtung ihres Verhaltens entstehen, neue Daten über sie generiert werden, die ihr Weltverständnis bestimmen, ihre sozialen Beziehungen beeinflussen, ihr Selbstbild prägen und Vorhersagen über ihr Verhalten ermöglichen.[2] Kindern fehlt daher vielfach die Möglichkeit, künftige Nachteile zu erkennen, insbesondere die Fähigkeit, die negativen Folgen der umfassenden Datenverarbeitung und Profilbildung in den von ihnen genutzten Internetangeboten richtig zu bewerten.

Auch die Fähigkeit zu autonomer Entscheidung müssen Kinder erst noch ausbilden. Dies setzt zum einen ein gefestigtes Selbstkonzept voraus. Um dieses auszubilden, müssen Kinder ihre vielen Persönlichkeitsfacetten und Persönlichkeitseigenbilder ausprobieren. Sie müssen lernen, verschiedene soziale Rollen mit unterschiedlichen Verhaltenserwartungen je nach sozialem Kontext anzunehmen. Zum anderen erfordert eine autonome Entscheidung geeignete normative Kriterien. Vorstellungen von Fairness und Gerechtigkeit müssen Kinder aber ebenfalls erst noch ausbilden und erproben.[3]

Kinder unterliegen einer besonderen strukturell bedingten Gefährdungslage: Sie verstehen die meist langfristigen Nachteile der Verarbeitung ihrer personenbezogenen Daten noch unzureichend, sind aber für

1 S. z.B. den Beitrag von *Stapf*, Aufwachsen in überwachten Umgebungen, in diesem Band.
2 S. hierzu den Beitrag von *Dreyer*, Recht auf mein Selbst, in diesem Band.
3 S. hierzu den Beitrag von *Dreyer*, Recht auf mein Selbst, in diesem Band.

die meist kurzfristigen positiven Effekte der Nutzung von digitalen Technologien und Diensten sehr offen und für Verführungen zu ihrer Nutzung leicht zugänglich.

Schließlich ist zu berücksichtigen, dass Kinder in der Regel ihre eigenen Rechte als betroffene Person nicht kennen. Selbst wenn sie ihnen bekannt wären, wären sie unfähig, sie wahrzunehmen. Das Gleiche gilt für die Fähigkeit, die eigenen Grundrechte technisch selbst zu schützen. Selbst wenn es um einfache Selbstschutzmaßnahmen geht, sehen sie überwiegend nicht ein, warum sie zusätzliche Umständlichkeiten auf sich nehmen sollen, wenn die Nutzung der Dienste doch auch einfacher geht.

Aus diesen Gründen haben Kinder einen besonderen Bedarf an Schutz und Fürsorge – gerade in digitalen Kontexten (Artikel-29-Datenschutzgruppe 2008: 3). Ihre informationelle Selbstbestimmung und Handlungsautonomie sind in besonderer Weise gefährdet. Bei der Ausgestaltung von Schutz und Fürsorge ist jedoch zu berücksichtigen, dass Kinder auch einen Freiraum benötigen, um mit digitalen Angeboten Erfahrungen zu gewinnen und einen bewussten und verantwortlichen Umgang mit ihnen zu lernen. Den notwendigen Ausgleich zwischen Schutz und Fürsorge einerseits sowie Freiraum für Entwicklung und Entfaltung andererseits zu finden, ist auch eine Aufgabe des Datenschutzrechts.

2. Völker- und verfassungsrechtliches Schutzgebot

Der besondere Schutzbedarf von Kindern wird im internationalen Recht von der Kinderrechtskonvention (Artikel-29-Datenschutzgruppe 2008: 3), in der Europäischen Union von der Grundrechte-Charta und in der Bundesrepublik Deutschland vom Grundgesetz anerkannt.

2.1 Übereinkommen über die Rechte des Kindes der Vereinten Nationen

Dem Übereinkommen über die Rechte des Kindes von 1989 sind alle Mitgliedstaaten der Vereinten Nationen mit Ausnahme der USA beigetreten. Nach Art. 1 UN-KRK ist ein Kind jeder Mensch, der das achtzehnte Lebensjahr noch nicht vollendet hat. Art. 3 Abs. 1 UN-KRK verpflichtet alle öffentlichen oder privaten Einrichtungen der sozialen Fürsorge, Gerichte, Verwaltungsbehörden oder Gesetzgebungsorgane, bei allen Maßnahmen, die Kinder betreffen, das Wohl des Kindes vorrangig zu berücksichtigen. Zu diesem gehört auch nach Art. 16 UN-KRK der Schutz des Privatlebens,

des Schriftverkehrs und der Ehre eines Kindes vor willkürlichen oder rechtswidrigen Eingriffen. Diesem Schutz entspricht die Bundesrepublik Deutschland durch die Grundrechte auf freie Entfaltung und Schutz der Persönlichkeit nach Art. 2 Abs. 1 GG, auf Schutz von Ehe und Familie nach Art. 6 GG, auf Schutz des Brief- und Fernmeldegeheimnisses nach Art. 10 GG und auf Schutz der Wohnung nach Art. 13 GG (Bundesministerium für Familie, Senioren, Frauen und Jugend 2014).

In Deutschland ist das Übereinkommen 1992 nach seiner Ratifikation im Rang eines einfachen Gesetzes in Kraft getreten.[4] Aus Art. 4 Abs. 1 UN-KRK ergibt sich, dass aus dem Übereinkommen direkt keine individuellen Rechtsansprüche abgeleitet und vor Gericht eingeklagt werden können. Sie müssen erst im nationalen Recht begründet worden sein (Bundesministerium für Familie, Senioren, Frauen und Jugend 2014). Nach Art. 4 Abs. 1 UN-KRK treffen die Vertragsstaaten jedoch alle geeigneten Gesetzgebungs-, Verwaltungs- und sonstigen Maßnahmen, um die im Übereinkommen anerkannten Rechte zu verwirklichen.

2.2 Grundrechte-Charta

Nach Art. 24 Abs. 1 Satz 1 GRCh haben Kinder „Anspruch auf den Schutz und die Fürsorge, die für ihr Wohlergehen notwendig sind." Dieser eigenständige Anspruch des Kindes auf Schutz und Fürsorge[5] gilt für alle Lebenssituationen[6] – auch in Bezug auf die Verarbeitung ihrer Daten. Auch für Kinder gelten die Grundrechte auf Privatleben nach Art. 7 GRCh und auf Datenschutz nach Art. 8 GRCh.[7] Schutz und Fürsorge ist nicht nur Aufgabe staatlicher Stellen, sondern fällt auch in die Verantwortung privater Stellen. Daher bestimmt Art. 24 Abs. 2 GRCh: „Bei allen Kinder betreffenden Maßnahmen öffentlicher Stellen oder privater Einrichtungen muss das Wohl des Kindes eine vorrangige Erwägung sein."[8] Das Wohl des Kindes als Treuhänder seiner Interessen zu vertreten, ist nach Art. 24 Abs. 3 GRCh die Aufgabe seiner Eltern.

---

4 BGBl. II, 990.

5 S. z.B. *Kingreen*, in: Callies/Ruffert, EUV, AEUV mit EU-GRCh, 5. Aufl. 2016, Art. 24 GRCh, Rn. 1; *Jarass*, GRCh, 3. Aufl. 2016, Art. 24 Rn. 3f.

6 S. hierzu auch Art. 3 Abs. 3 UAbs. 2 und Abs. 5 EUV.

7 S. auch Art.-29-Datenschutzgruppe 2008, S. 5 und 7, die aber auch darauf hinweist, dass die Gewährleistung einer angemessenen Fürsorge auch eine Verarbeitung der Daten von Kindern erforderlich machen kann.

8 *Zur Verpflichtung privater Stellen s. Jarass,* GRCh, 3. Aufl. 2016, Art. 24 Rn. 6, 15.

Dem Wohl des Kindes entspricht es, seine Persönlichkeit zu entwickeln und zu entfalten.[9] Daher garantiert Art. 24 Abs. 1 Satz 2 und 3 GRCh auch Kindern, ihre Meinung frei zu äußern.[10] „Ihre Meinung wird in den Angelegenheiten, die sie betreffen, in einer ihrem Alter und ihrem Reifegrad entsprechenden Weise berücksichtigt." Eltern müssen dies dem Alter und Reifegrad des Kindes entsprechend berücksichtigen, wenn sie im Rechtsverkehr ihre Kinder vertreten oder im Kontext der Datenverarbeitung über eine Zustimmung zu einer Einwilligung des Kindes entscheiden[11].

2.3 Grundgesetz

Nicht ganz so eindeutig sind die Aussagen des Grundgesetzes. Nach Art. 6 Abs. 2 GG sind „Pflege und Erziehung der Kinder […] das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht. Über ihre Betätigung wacht die staatliche Gemeinschaft." Träger des Grundrechts sind die Eltern, nicht die Kinder. Verpflichtete sind alle Träger öffentlicher Gewalt. Das Grundrecht aus Art. 6 Abs. 2 GG schützt die Verantwortung der Eltern für die Lebens- und Entwicklungsbedingungen des Kindes und das Recht, Erziehungsziele und -mittel autonom festzulegen.[12] Für das Bundesverfassungsgericht ist das „Elternrecht ein Recht im Interesse des Kindes",[13] zumal das Kind auf Schutz und Hilfe angewiesen ist.[14] Maßgebliche Richtschnur für die Eltern muss das Wohl des Kindes sein.[15] Somit ist das Elternrecht ein treuhänderisches Recht.[16]

Allerdings hat das Kind auch eigene Grundrechte, die das Elternrecht einschränken können. Daher nehmen die im Elternrecht wurzelnden Rechtsbefugnisse mit fortschreitendem Alter des Kindes ab und erlöschen mit dessen Volljährigkeit.[17] Das Recht des Kindes gegen den Staat auf Sicherung seiner Pflege und Erziehung folgt aus Art. 2 Abs. 1 in Verbindung

---

9 S. auch *Jarass*, GRCh, 3. Aufl. 2016, Art. 24 Rn. 10, 16.
10 S. auch *Jarass*, GRCh, 3. Aufl. 2016, Art. 24 Rn. 15.
11 S. z.B. Klement, in: Simitis/Hornung/Spiecker, Datenschutzrecht – DSGVO mit BDSG, 2019, Art. 8 Rn. 27.
12 BVerfGE 107, 104 (117); *Jarass/Pieroth*, GG, 15. Aufl. 2018, Art. 6 Rn. 42.
13 BVerfGE 121, 68 (92); 72, 122 (137).
14 BVerfGE 79, 51 (73); 108, 52 (72).
15 BVerfGE 121, 68 (92).
16 BVerfGE 59, 360 (377); 64, 180 (189); 107, 104 (121); *Jarass*, GG, 15. Aufl. 2018, Art. 6 Rn. 45.
17 BVerfGE 59, 360 (382); 72, 122 (137); *Jarass*, GG, 15. Aufl. 2018, Art. 6 Rn. 44, 51.

mit Art. 6 Abs. 2 GG.[18] Aufgrund dessen hat der Staat eine Schutz- und Förderpflicht, dieses Grundrecht durch geeignete Rahmenbedingungen zu gewährleisten.[19] Er hat durch seine Gesetzgebung eine „kinderfreundliche Gesellschaft" zu fördern.[20] Dieses Ziel ist auch im Rahmen der mittelbaren Drittwirkung den für Unternehmen geltenden Rechtsregeln zugrunde zu legen.[21]

Da ein eigenes Kinderrecht im Grundgesetz fehlt, hat die Regierungskoalition in ihrem Vertrag beschlossen, Kinderrechte ausdrücklich im Grundgesetz zu verankern (Die Bundesregierung 2018: 20). Im November 2019 hat das Bundesjustizministerium einen Entwurf zur Änderung des Grundgesetzes vorgelegt.[22] Danach soll in Art. 6 GG ein neuer Abs. 1a mit folgendem Wortlaut aufgenommen werden: „Jedes Kind hat das Recht auf Achtung, Schutz und Förderung seiner Grundrechte einschließlich seines Rechts auf Entwicklung zu einer eigenverantwortlichen Persönlichkeit in der sozialen Gemeinschaft. Das Wohl des Kindes ist bei allem staatlichen Handeln, das es unmittelbar in seinen Rechten betrifft, angemessen zu berücksichtigen. Jedes Kind hat bei staatlichen Entscheidungen, die seine Rechte unmittelbar betreffen, einen Anspruch auf rechtliches Gehör." Mit dieser Ergänzung sollen „die Grundrechte von Kindern im Text des Grundgesetzes besser sichtbar werden". Eine inhaltliche Änderung von Elternrechten und Elternverantwortung soll damit jedoch nicht erreicht, das Verhältnis zwischen Eltern, Kindern und Staat „bewusst nicht angetastet werden".

3. Datenschutz von Kindern in der Datenschutz-Grundverordnung

Diese besondere Schutzpflicht hat auch der Gesetzgeber der Europäischen Union erkannt. Nach Erwägungsgrund 38 Satz 1 DSGVO verdienen Kinder „bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind". Wen die Datenschutz-Grundverordnung unter den Begriff

18 BVerfGE 133, 59, Rn. 43; 135, 48 Rn. 98.
19 BVerfGE 130, 240 (252, 256).
20 BVerfGE 88, 203 (260).
21 S. z.B. Jarass/Pieroth, GG, 15. Aufl. 2018, Art. 6 Rn. 53.
22 Süddeutsche Zeitung vom 26.11.2019, S. 1.

„Kinder" fasst, hat sie nicht definiert.[23] Aus dem systematischen Zusammenhang ist jedoch zu schließen, dass die Datenschutz-Grundverordnung unter „Kindern" alle Personen versteht, die das 18. Lebensjahr noch nicht erreicht haben.[24]

Den Begriff „Jugendliche" kennt die Datenschutz-Grundverordnung dementsprechend nicht.[25] Die besondere Schutzbedürftigkeit von Kindern berücksichtigt die Datenschutz-Grundverordnung in sechs Regelungen für unterschiedliche datenschutzrechtliche Zusammenhänge.

3.1 Einwilligung von Kindern

Willigen Kinder in die Verarbeitung ihrer Daten ein, gelten auch für sie die allgemeinen Regelungen zur Definition einer wirksamen Einwilligung in Art. 4 Nr. 11 DSGVO, zur grundsätzlichen Erlaubniswirkung der Einwilligung in Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO, zur ausdrücklichen Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten in Art 9 Abs. 2 lit. a DSGVO und in automatisierte Entscheidungen nach Art. 22 Abs. 2 lit. c DSGVO sowie zu weiteren Voraussetzungen jeder Einwilligung in Art. 7 DSGVO.

Da eine Einwilligung nach Art. 4 Nr. 11 DSGVO Freiwilligkeit voraussetzt und diese fehlt, wenn der Erklärende nicht fähig ist, den Gegenstand der Einwilligung, ihre Bedeutung und ihre Folgen kognitiv zu erfassen und seinen Willen selbstbestimmt zu bilden und zu betätigen, ist ein Kind nicht einwilligungsfähig, wenn es zu dieser Einsicht und Handlung noch nicht in der Lage ist. Diese Einsicht ist in der Regel im Einzelfall je nach

---

23 Anders als der Entwurf der Kommission und des Parlaments, die in Art. 4 Nr. 18 Kind als „jede Person bis zur Vollendung des achtzehnten Lebensjahres" definierten.

24 Art. 29-Datenschutzgruppe, Leitlinien für Transparenz, WP 260 rev.01, 2018, 12; *Schwartmann/Hilgen*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO, 2018, Art. 8 Rn. 1, 24; *Ernst*, ZD 2017, 110 (111); s. hierzu auch Art.-29-Datenschutzgruppe, Schutz der personenbezogenen Daten von Kindern, WP 147, 2.

25 Im deutschen Recht wird der Begriff „Jugendliche" unterschiedlich gebraucht. Das Zivilrecht unterscheidet nur zwischen Volljährigen und Minderjährigen, das GG spricht nur von „Kindern" und meint damit Minderjährige unter 18 Jahren. Dagegen kennen etliche Vorschriften des Sozialrechts den Begriff der „Jugendlichen" und meinen damit meist jungen Menschen unter 25 Jahren. Das Jugendschutzrecht versteht unter Jugendlichen Minderjährige zwischen 14 und 17 Jahren. Ebenso sieht das Strafrecht die Jugendlichen, kennt aber zusätzlich noch die Heranwachsenden zwischen 18 und 21 Jahren – s. hierzu *Wabnitz* 2017: 13 ff.

Umfang und Bedeutung der Datenverarbeitung, dem Inhalt der Einwilligung und den Fähigkeiten des Kindes zu beurteilen.[26]

Die Verordnung regelt jedoch keine Altersgrenze, von der an das Kind als einsichtsfähig gilt. Nach Art. 8 Abs. 1 UAbs. 1 Satz 1 DSGVO gilt die Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft (Simitis/Hornung/Spiecker 2019),[27] das einem Kind direkt unterbreitet wird,[28] als rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat.[29] Mit dieser starren Altersgrenze, die einen Kompromiss zwischen sehr unterschiedlichen Vorstellungen im Gesetzgebungsprozess darstellt,[30] soll im Internet, in dem die Einsichtsfähigkeit nicht durch Augenschein festgestellt werden kann, Rechtssicherheit für alle Beteiligte gewährleistet werden. Von dieser typisierenden Festlegung der Einwilligungsfähigkeit kann im Einzelfall in Bezug auf die Altersgrenze weder nach unten noch nach oben abgewichen werden.

Nach der Öffnungsklausel des Art. 8 Abs. 1 UAbs. 2 DSGVO dürfen jedoch Mitgliedstaaten durch gesetzliche Regelung diese Grenze bis zur Vollendung des dreizehnten Lebensjahres senken. Diese Grenze richtet

---

26 S. z.B. *Klement*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 8 Rn. 1 und 10; *Däubler*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG-neu, 2018, Art. 8 DSGVO, Rn. 2; *Schulz*, in: Gola, DSGVO, 2. Aufl. 2018, Art. 8 Rn. 9f.; ebenso nach dem bisherigen deutschen Datenschutzrecht – s. z.B. *Roßnagel/Richter*, Aufwachsen in virtuellen und technologisierten Welten, 2017, 205 (243); *Jandt/Roßnagel*, in: Schenk/Niemann/Reimann/Roßnagel, Digitale Privatsphäre, 2012, 309 ff.; *dies*., MMR 2011, 637 ff.

27 Ein „Dienst der Informationsgesellschaft" ist nach der Definition des Art. 4 Nr. 25 DSGVO eine Dienstleistung im Sinn des Art. 1 Nr. 1 lit. b der Richtlinie (EU) 2015/1535 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, EU ABl. L 241 vom 17.9.2015, 1. Praktisch greift diese Regelung bei allen über das Internet angebotenen Diensten – s. z.B. *Klement*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 4 Nr. 25 Rn. 5 ff. und Art. 8 Rn. 1; *Weichert*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG-neu, 2018, Art. 4 DSGVO, Rn. 173 ff.

28 Dies soll nur dann der Fall sein, wenn der Dienst ausdrücklich Kinder anspricht – s. *Kampert*, in: Sydow, DSGVO, 2. Aufl. 2018, Art. 8 Rn. 9.

29 Nach der bisherigen herrschenden Meinung in Deutschland bestand ein informeller Richtwert von 14 Jahren – s. z.B. OVG Lüneburg, NJW 2015, 502; *Holznagel/Sonntag*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 4.8 Rn. 22; *Gola/Schulz*, ZD 2013, 475 (478).

30 Der Entwurf der Kommission und des Parlaments sahen in Art. 8 Abs. 1 eine feste Altersgrenze von 13 Jahren ohne Möglichkeit davon abzuweichen, vor, nach Art. 8 Abs. 1 des Entwurfs des Rats sollte die Einwilligung eines Kindes bis zum Alter von 18 Jahren unwirksam sein.

sich wohl nach den Nutzungsbedingungen der großen amerikanischen Plattformen wie Facebook, WhatsApp, Twitter und YouTube, die die Nutzung ab 13 Jahren zulassen. Von dieser Öffnungsklausel haben die Mitgliedstaaten sehr unterschiedlich Gebrauch gemacht. Die Altersgrenze auf 13 Jahre festgesetzt haben Belgien, Dänemark, Estland, Finnland, Lettland, Malta, Portugal und Schweden. Ab 14 Jahren dürfen Kinder in Bulgarien, Italien, Litauen, Österreich, Spanien und Zypern ohne Zustimmung ihrer Eltern in die Datenverarbeitung von Diensten der Informationsgesellschaft einwilligen. Eine Grenze mit 15 Jahren sehen Frankreich, Griechenland, Slowenien und Tschechien vor. Die Altersgrenze der Datenschutz-Grundverordnung haben nur Deutschland, Irland Kroatien, Luxemburg, Niederlande, Polen, Rumänien, Slowakei und Ungarn beibehalten.[31]

Die starre Altersgrenze gilt jedoch nur für die Datenverarbeitung, um Dienste der Informationsgesellschaft zu erbringen. Für alle anderen Datenverarbeitungen muss anhand der Einsichts- und Handlungsfähigkeit des Kindes individuell festgestellt werden, ob die Einwilligung freiwillig ist. Auf diese Feststellung übt allerdings die gesetzliche Festlegung der Einwilligungsfähigkeit bei 16 Jahren für Dienste der Informationsgesellschaft einen indirekten Einfluss aus. Es wird vertreten, dass unterhalb dieser Altersgrenze im Streitfall der Verantwortliche die Einwilligungsfähigkeit und oberhalb der Altersgrenze die betroffene Person die fehlende Einwilligungsfähigkeit nachweisen muss.[32]

Hat das Kind die festgesetzte Altersgrenze oder die individuelle Einwilligungsfähigkeit[33] noch nicht erreicht, so ist die Datenverarbeitung nach Art. 8 Abs. 1 UAbs. 1 Satz 2 DSGVO „nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird". Art. 8 Abs. 2 DSGVO verpflichtet den Verantwortlichen, dass er „unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen unternimmt, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde" (Roßnagel/Richter 2017: 205). In der Praxis hat sich das Verfahren des Double-Opt-in als bevorzugte Lösung etabliert: Der Anbieter

31 S. die Übersicht von *Nebel/Dräger*, Altersgrenzen in den Mitgliedstaaten, ZD-aktuell 8/2019, VIII.

32 S. z.B. *Klement*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 8 Rn. 12.

33 Dies muss auch für die nicht von Art. 8 Abs. 1 UAbs. 1 Satz 1 DSGVO erfassten Fälle gelten – s. z.B. *Klement*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 8 Rn. 25.

schickt eine E-Mail an die E-Mail-Adresse der Sorgeberechtigten und lässt sich ihre Einwilligung oder Zustimmung per E-Mail erteilen oder bestätigen.[34]

Die Regelung in Art. 8 DSGVO lässt nach dessen Abs. 3 „das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt". Dies bedeutet zweierlei: Erstens kommt es für die Einwilligungsfähigkeit nicht auf die Geschäftsfähigkeit der betroffenen Person an, sondern auf die Freiwilligkeit der Einwilligung. Zum anderen kann in Deutschland eine betroffene Person erst einen Vertrag abschließen und damit den Erlaubnistatbestand der Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO begründen, wenn sie mit 18 Jahren die Geschäftsfähigkeit erlangt hat (Jandt/Roßnagel 2011: 637, Roßnagel/Richter 2017: 205).

3.2 Abwägung mit schutzwürdigen Interessen von Kindern

Nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO ist eine Verarbeitung personenbezogener Daten zulässig, wenn sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich" ist, „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen" (Nebel 2018: 106). An diese Zulässigkeitsvoraussetzung schließt der Nebensatz an: „insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt". Diese unglückliche Formulierung soll zum Ausdruck bringen, dass bei der notwendigen Interessenabwägung die der Datenverarbeitung entgegenstehenden Interessen oder Grundrechte und Grundfreiheiten in besonderer Weise berücksichtigen müssen, „wenn es sich bei der betroffenen Person um ein Kind handelt".[35] Allerdings werden kein bestimmter Zweck und keine bestimmte Form der Datenverarbei-

34 S. z.B. *Däubler*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG-neu, 2018, Art. 8 DSGVO, Rn. 9.

35 Nach *Buchner/Petri*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 6 DSGVO, Rn. 155, sollen bei einem Kind unter 16 Jahren regelmäßig die schutzwürdigen Interessen überwiegen; ähnlich Art.-29-Datenschutzgruppe, Schutz der personenbezogenen Daten von Kindern, WP 147, 14, für die Verarbeitung von Kinderdaten für Werbezwecke; s. dagegen *Reimer*, in: Sydow, DSGVO, 2. Aufl. 2018, Art. 6 Rn. 64: nur „besonders gewichtig".

tung zum Schutz des Kindes ausgeschlossen, sondern überwiegend nur eine intensivere Abwägung durch den Verantwortlichen gefordert.[36]

3.3 Informationen für Kinder

Nach Art. 12 Abs. 1 Satz 1 DSGVO sind Informationen nach Art. 13 und 14 DSGVO und alle Mitteilungen gemäß den Art. 15 bis 22 und 34 DSGVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln". „Dies gilt insbesondere für Informationen, die sich speziell an Kinder richten". Damit soll erreicht werden, dass auch Kinder aufgrund dieser Informationen ihre informationelle Selbstbestimmung ausüben können. Die Informationen müssen daher in kindgerechter Sprache abgefasst sein.[37] Dies gilt auch dann, wenn die Träger der elterlichen Verantwortung in die Datenverarbeitung einwilligen (Artikel-29-Datenschutzgruppe 2018: 12f). „Wenn sich die Verarbeitung an Kinder richtet, sollten" nach Erwägungsgrund 58 Satz 4 DSGVO „aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann".[38] „Speziell an Kinder" richten sich Informationen, wenn sie Datenverarbeitungen betreffen, die Grundlage für spezifische Angebote sind, die von Kindern oder auch nicht unerheblich von Kindern genutzt werden.

3.4 Löschung der personenbezogenen Daten von Kindern

Nach Art. 17 Abs. 1 DSGVO hat jede betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer

---

36 S. z.B. *Schantz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 6 Abs. 1 Rn. 112.

37 *Dix*, in: Simitis/Hornung/Spiecker, Datenschutzrecht – DSGVO mit BDSG, 2019, Art. 12 Rn. 16; *Herbst*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 12 DSGVO, Rn. 11.

38 Hier verweist die Art. 29-Datenschutzgruppe, Leitlinien für Transparenz, WP 260 rev.01, 2018, 12, auf die „Konvention über die Rechte des Kindes – Für Kinder erklärt" des Kinderhilfswerks der Vereinten Nationen als gelungenes Beispiel für kindgerechte Sprache.

der in Abs. 1 genannten Gründe zutrifft. In lit. f wird der Grund genannt, dass „die personenbezogenen Daten […] in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 erhoben" wurden.[39] Die Vorschrift knüpft daran an, dass Kinder häufig Daten über sich im Internet preisgeben, deren Preisgabe sie später bereuen könnten, und scheint dieser Schutzbedürftigkeit besonders Rechnung zu tragen (Roßnagel/Richter 2017: 205). Mit diesem Löschungsanspruch soll erreicht werden, dass Kinder beim Übergang in das Erwachsenenalter nicht von „Jugendsünden" verfolgt werden, deren langfristige Folgen sie im Kindesalter noch nicht abschätzen konnten.[40] Dieses Recht soll einen Ausgleich dazu darstellen, dass Art. 8 Abs. 1 DSGVO den Verantwortlichen erlaubt, bei Diensten der Informationsgesellschaft, d.h. praktisch allen über das Internet angebotenen Diensten, die personenbezogenen Daten ohne Einwilligung der Eltern zu verarbeiten, wenn ein Kind, das bereits 16 Jahre alt ist, in die Datenverarbeitung einwilligt.[41] Nach anderer Meinung sind nur die Fälle erfasst, in denen das Kind – je nach mitgliedstaatlicher Regelung der Einwilligungsfähigkeit – unter 13 bis 16 Jahren seine Einwilligung mit Zustimmung seines gesetzlichen Vertreters gegeben hat.[42] Nach wieder anderer Meinung besteht der Löschanspruch nur, wenn das Kind unter 16 Jahren ohne Zustimmung der Träger der elterlichen Verantwortung eingewilligt hat.[43] Hier ist eine gesetzliche Klarstellung erforderlich.

3.5 Verhaltensregeln von Verbänden

Nach Art. 40 und 41 DSGVO können Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln für ihre jeweilige Branche beschließen, mit denen die Anwendung der Verordnung präzisiert wird. Diese Verhaltensregeln sind den Aufsichtsbehörden vorzulegen und von diesen zu genehmigen,

39 Diese Regelung gilt somit auch, wenn Mitgliedstaaten nach der Öffnungsklausel des Art. 8 Abs. 1 UAbs. 2 DSGVO die Altersgrenze für eine wirksame Einwilligung weiter gesenkt haben – s. hierzu Kap. 3.1.

40 S. Erwägungsgrund 65; s. hierzu z.B. *Herbst*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 17 DSGVO, Rn. 31.

41 S. Kap. 3.1.

42 S. *Däubler*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG-neu, 2018, Art. 17 DSGVO, Rn. 18; *Herbst*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 17 DSGVO, Rn. 34.

43 S. *Peuker*, in: Sydow, DSGVO, 2. Aufl. 2018, Art. 17 Rn. 30.

wenn sie der Datenschutz-Grundverordnung entsprechen. Sie sind dann für die weitere Aufsichtstätigkeit verbindlich.[44] Art. 40 Abs. 2 DSGVO nennt Beispiele für Inhalte solcher Verhaltensregeln. Nach lit. g sind auch „Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist," mögliche Regelungsgegenstände. Damit reagiert die Verordnung auf ihre eigene Abstraktheit und Unterkomplexität (Roßnagel 2018a: 27), überlässt aber Konkretisierungen und Spezifizierungen nicht der Kommission oder den Mitgliedstaaten, sondern Branchenverbänden.[45] Dabei geht es grundsätzlich um den Schutz von Kindern in der Datenverarbeitung, aber vor allem geht es um die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Satz 1 lit. f DSGVO, um die Bestimmung der Einwilligungsfähigkeit nach Art. 4 Nr. 11 DSGVO, um die Information von Kindern nach Art. 12 Abs. 1 DSGVO und um die Einwilligung oder Zustimmung des Trägers der elterlichen Verantwortung zur Verarbeitung von Daten ihres Kindes nach Art. 8 Abs. 1 UAbs. 1 Satz 2 DSGVO und deren Einholung durch den Verantwortlichen nach Art. 8 Abs. 2 DSGVO. Zu diesen Themen können Branchenverbände, deren Mitglieder sich an Kinder wenden oder deren Angebote stark von Kindern genutzt werden, die offenen Regelungen der Verordnung jeweils spezifisch für sich präzisieren und konkretisieren.

3.6 Aufklärung der Öffentlichkeit durch Aufsichtsbehörden

Nach Art. 57 Abs. 1 lit. b DSGVO ist es eine von vielen Aufgaben der Aufsichtsbehörden, „die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung (zu) sensibilisieren und sie darüber auf(zu)klären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder." Diese Aufklärungsmaßnahmen sollen die rechtlichen und technischen Maßnahmen zum Datenschutz unterstützen. Sie sollen besonders sowohl auf den Schutz von Kindern gerichtet sein als auch sich an Kinder richten.[46] Bei solchen spezifischen Maßnahmen für Kinder sind deren informationstechnische Praktiken, deren Auf-

---

44 S. hierzu *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 40 Rn. 67 ff.

45 S. z.B. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 40 Rn. 45.

46 *Polenz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 57 Rn. 11 und 20.

fassungs- und Handlungsfähigkeit sowie mögliche Vermittlungswege (z.B. Eltern, Schule, Verein) zu berücksichtigen.[47]

3.7 Generelle Gleichbehandlung von Kindern mit Erwachsenen

Alle anderen Regelungen der Datenschutz-Grundverordnung behandeln Kinder so wie Erwachsene. Für sie gelten beispielsweise die gleichen Regelungen zur Erlaubnis von Datenverarbeitungen und die gleichen Verarbeitungsgrundsätze. Sie haben als betroffene Personen die gleichen Rechte wie Erwachsene. Die Verantwortlichen haben ihnen gegenüber grundsätzlich die gleichen Verpflichtungen wie gegenüber erwachsenen betroffenen Personen und ihre personenbezogenen Daten können unter den gleichen Voraussetzungen in Staaten außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung übertragen und dort verarbeitet werden. In all diesen Fällen fordert die Datenschutz-Grundverordnung nicht, die Schutzbedürftigkeit von Kindern besonders zu berücksichtigen.

4. Notwendige Verbesserungen des Schutzes von Kindern

Die Datenschutz-Grundverordnung trat am 25. Mai 2016 in Kraft und gilt seit dem 25. Mai 2018 in allen Mitgliedstaaten der Europäischen Union unmittelbar. Bereits zwei Jahre später sollte eine erste Evaluation dieses Normenwerks vorliegen. Nach Art. 97 DSGVO musste die Europäische Kommission bis zum 25. Mai 2020 einen Bericht über die Bewertung und Überprüfung der Datenschutz-Grundverordnung veröffentlichen. Danach sollen Evaluationen alle vier Jahre erfolgen. Für die Evaluationen sind jeweils „die Standpunkte und Feststellungen des Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen" zu berücksichtigen. Soweit erforderlich, soll die Kommission Änderungen der Datenschutz-Grundverordnung vorschlagen. Sie soll dabei insbesondere „die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft" berücksichtigen.

---

47 S. z.B. *Weichert*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG-neu, 2018, Art. 57 DSGVO, Rn. 11; *Polenz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 57 Rn. 20.

Die Kommission legte ihren Bericht – um einen Monat verspätet – am 24. Juni 2020 vor.[48] Sie stellt in ihrem nur 18 Seiten umfassenden Bericht[49] zwar fest, dass es zwei Bereiche gäbe, in denen in der Zukunft Verbesserungen möglich seien, schlägt jedoch keine Änderungen des Verordnungstextes vor, die diese Schwachstellen beseitigen.[50] Sie beschränkt sich ausschließlich auf ausgewählte Fragen des Umgangs mit der Verordnung. Bezogen auf diese hat sich die Datenschutz-Grundverordnung aus Sicht der Kommission bewährt.[51] Mit diesem Bericht enttäuscht die Kommission alle Stellen, die wie der Rat, die Mitgliedstaaten, die Bundesregierung, der Bundesrat, die Konferenz der unabhängigen Datenschutzaufsichtsbehörden sowie viele Verbände, Organisationen und Initiativen aus ganz Europa viele (auch unterschiedliche) Vorschläge zur Verbesserung der Verordnung vorgelegt haben, die ihre Praktikabilität, Effizienz und Rechtssicherheit erhöhen sollten.[52]

Dieser Verbesserungsbedarf gilt auch für den Schutz von Kindern. Die Datenschutz-Grundverordnung enthält zwar punktuelle Regelungen zum Schutz von Kindern, diese betreffen jedoch nicht alle Situationen, in denen der besondere Schutz von Kindern erforderlich ist oder ihre besonderen Interessen zu berücksichtigen sind. Außerdem wird hinter diesen wenigen Regelungen kein Gesamtkonzept eines Kinderdatenschutzes sichtbar.[53] Daher sollte die Kommission in der Evaluation überprüfen, wo und wie sie diesen Schutz verbessern kann. Dies hat sie versäumt. Dennoch unterbreitet der Beitrag im Folgenden beispielhafte Vorschläge, wie die Verordnung – in der Reihenfolge ihrer Vorschriften – in ihrem Wortlaut diesen besonderen Aspekt zusätzlich und ausdrücklich berücksichtigen kann (Roßnagel/Geminn 2020).

---

48 Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition -two years of application of the General Data Protection Regulation, COM(2020) 264 final (SWD(2020) 115 final).

49 Dieser wird ergänzt um ein inoffizielles Commission Staff Working Document von 52 Seiten.

50 S. hierzu näher und kritisch *Roßnagel*, MMR 2020, 657 ff..

51 *Jourová*, Pressemitteilung der Europäischen Kommission vom 24.6.2020.

52 S. zu den Stellungnahmen ausführlich *Roßnagel*, DuD 2020, 287.

53 So auch *Däubler*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG-neu, 2018, Art. 8 DSGVO, Rn. 2.

4.1 Änderung des Verarbeitungszwecks

Nach dem Datenschutzgrundsatz der Zweckbindung des Art. 5 Abs. 1 lit. b DSGVO dürfen personenbezogene Daten nur „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden". Nach dem Wortlaut dieses Grundsatzes ist nicht jede Zweckänderung unzulässig, sondern nur diejenige, die mit dem ursprünglichen Zweck nicht zu vereinbaren ist.[54] Wie die Prüfung der Vereinbarkeit eines neuen Verarbeitungszwecks mit dem bisherigen Verarbeitungszweck erfolgen soll und wann eine Vereinbarkeit anzunehmen ist, regelt Art. 6 Abs. 4 DSGVO. Um diese Feststellung treffen zu können, nennt diese Regelung fünf Aspekte, die der Verantwortliche unter anderem berücksichtigen soll.[55] Zum Schutz von Kinder, die nicht erkennen oder erahnen können, für welche vereinbaren Zwecke ihre Daten später noch verwendet werden können, sollte der Gesetzgeber außerdem vorschreiben, dass der Verantwortliche auch zu berücksichtigen hat, wenn die Daten eines Kindes für einen anderen Zweck verwendet werden sollen. In diesem Fall sollte die Feststellung der Vereinbarkeit einer Zweckänderung mit dem ursprünglichen Zweck restriktiver erfolgen als bei Daten von Erwachsenen.

4.2 Keine Datenverarbeitung für Zwecke der Werbung und der Erstellung von Profilen

Nachdem Satz 1 des Erwägungsgrunds 38 DSGVO feststellt, dass Kinder bei ihren personenbezogenen Daten besonderen Schutz verdienen, konkretisiert Satz 2 diese Aussage dahingehend, dass ein solch besonderer Schutz „insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen" sollte. Erwägungsgründe erläutern jedoch nur die Gründe, die den Gesetzgeber veranlasst haben, die betreffende Regelung in den Normtext der Verordnung aufzunehmen, und die Ziele, die er damit ver-

54 S. z.B. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 5 Rn. 96 ff.

55 S. z.B. *Roßnagel*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 6 Abs. 4 Rn. 32 ff.

folgen will. Sie sind bei dessen Auslegung zu berücksichtigen, sie sind aber nicht Teil der normativen Anordnungen der Verordnung.

Wenn der Unionsgesetzgeber den von ihm angestrebten besonderen Schutz von Kindern rechtlich wirksam werden lassen will, sollte er die Wertung des Erwägungsgrunds 38 DSGVO in den Normtext des Art. 8 DSGVO übernehmen. Er sollte dort festlegen, dass die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen unzulässig ist. Ein solches Verbot würde die Werbung für Spiele und Spielsachen nicht ausschließen, sondern nur die Nutzung von Persönlichkeits- oder Nutzerprofilen und andere Sammlungen von Kinderdaten für Werbezwecke. Dabei sollte es keinen Unterschied machen, ob diese Datenverarbeitung auf eine Einwilligung des Kindes oder seiner Erziehungsberechtigten oder auf überwiegende berechtigte Interessen gestützt wird.

Die Risiken für Kinder werden allein durch die jeder betroffenen Person zustehenden Opt-out-Möglichkeit nach Art. 21 Abs. 2 DSGVO, gegen die Datenverarbeitung zur Direktwerbung und gegen ein „Profiling, soweit es mit solcher Direktwerbung in Verbindung steht", jederzeit Widerspruch einzulegen,[56] nicht ausreichend ausgeglichen. In diesem Fall darf zwar der Verantwortliche gemäß Art. 21 Abs. 3 DSGVO die personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten. Diese Opt-out-Möglichkeit ist für Kinder jedoch ein ungenügendes Schutzinstrument. Erstens besteht ein solches Recht nicht, wenn die Daten für eine andere Form der Werbung als Direktwerbung verarbeitet werden oder die Profilbildung auch anderen Zwecken dient. Zweitens erfordert es, dass Kinder die Bedeutung dieses Rechts und seine Rechtsfolgen kennen und erkennen. Drittens müssen sie im Regelfall in vierfacher Weise initiativ werden. Sie müssen den Verantwortlichen ausfindig machen, bei diesem eine Auskunft zu den über sie gespeicherten Daten und ihren Zweck einfordern, schließlich den Widerspruch einlegen und über eine weitere Einforderung einer Auskunft die Umsetzung seiner Rechtsfolgen überprüfen. Die Wahrnehmung dieser Opt-out-Möglichkeit ist sehr umständlich und kann Kindern im Regelfall nicht zugemutet werden. Sie erfasst außerdem nur einen Bruchteil des von Erwägungsgrund 38 Satz 2 DSGVO angesprochenen Schutzes.[57] Der Schutz der Kinder kann daher nicht allein auf diese nachträgliche Ab-

---

56 Für dieses Recht gelten die Voraussetzungen des Art. 21 Abs. 1 Satz 1 DSGVO nicht – s. z.B. *Caspar*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 21 Rn. 20.

57 Dies gilt auch für eine Wahrnehmung des Widerspruchsrechts nach Art. 21 Abs. 1 DSGVO.

wehrmöglichkeit gestützt werden. Daher ist ein präventiver Schutz von Kindern gegen die Datenverarbeitung für alle Werbezwecke und der damit zusammenhängenden Profilbildung erforderlich.

4.3 Keine Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten

Art. 9 Abs. 1 DSGVO untersagt „die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person". Von diesem Verbot, besondere Kategorien personenbezogener Daten zu verarbeiten, sieht Art. 9 Abs. 2 DSGVO zehn Ausnahmen vor. Nach Abs. 2 lit. a gilt das Verbot nicht, wenn „die betroffene Person […] in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt" hat. Diese Einwilligungsmöglichkeit gilt unabhängig davon, ob ein Erwachsener oder ein Kind einwilligt.[58]

Von der Ausnahme des Verbots der Verarbeitung besonderer Kategorien von personenbezogenen Daten bei einer Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO sollte die Einwilligung eines Kindes ausgenommen werden. Kinder können noch zu wenig die künftigen Folgen einer Einwilligung gerade in die Verarbeitung solcher, besonders schützenswerter Daten erkennen und darüber frei und informiert entscheiden. Das Schadenspotential der Verarbeitung solcher Daten ist sehr groß. Die Schwierigkeiten, nach einer positiven Einschätzung der Einwilligungsfähigkeit durch den Verantwortlichen die Datenverarbeitung in der Praxis wieder rückgängig zu machen und alle Daten bei allen Verantwortlichen löschen zu lassen, sind ebenfalls beträchtlich. Daher ist die Verankerung dieser Rückausnahme in Art. 9 Abs. 2 lit. a DSGVO – sowohl für Angebote von Diensten der Informationsgesellschaft als auch für alle anderen Fälle der Einwilligung eines Kindes – sowohl notwendig als auch gerechtfertigt.

Eine Einwilligung oder Zustimmung durch den Träger der elterlichen Verantwortung bleibt dadurch weiterhin möglich. Die Zielsetzung des Er-

58 S. z.B. *Weichert*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 9 DSGVO, Rn. 47 ff.

wägungsgrunds 38 Satz 3 DSGVO, dass „die Einwilligung des Trägers der elterlichen Verantwortung […] im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein" sollte, hat im Text der Verordnung keinen Ansatzpunkt gefunden. Sie könnte ebenfalls in Art. 8 oder in Art. 9 DSGVO geregelt werden. Ein Kind sollte in psychischen Zwangslagen z.B. eine Sucht- oder Schwangerschaftsberatung in Anspruch nehmen können, ohne befürchten zu müssen, dass die Eltern davon erfahren.[59]

4.4 Recht auf Widerspruch

Nicht nur bei der Forderung der betroffenen Person nach Löschung ihrer personenbezogenen Daten nach Art. 17 DSGVO,[60] sondern auch beim Widerspruch nach Art. 21 Abs. 1 DSGVO sollte die Verordnung in besonderer Weise berücksichtigen, wenn die personenbezogenen Daten im Kindesalter erhoben worden sind.

Nach Art. 21 Abs. 1 Satz 1 DSGVO hat jede betroffene Person „das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten […] Widerspruch einzulegen" (Hohmann/Miedzianowski 2018: 128f). Dieses Recht gilt allerdings nur, wenn die Daten aufgrund überwiegender berechtigter Interessen gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO oder für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, gemäß Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO verarbeitet werden. Das Widerspruchsrecht erstreckt sich auch auf ein Profiling, das der Verantwortliche auf diese beiden Erlaubnistatbestände stützt. Das Widerspruchsrecht besteht nicht, wenn die Datenverarbeitung aufgrund einer Einwilligung oder zur Erfüllung eines Vertrags, zur Durchführung vorvertraglicher Maßnahmen oder zur Erfüllung einer rechtlichen Verpflichtung erfolgt.

Hat die betroffene Person einen Widerspruch eingelegt, prüft der Verantwortliche dessen Berechtigung. Nach Art. 21 Abs. 1 Satz 2 DSGVO darf er die personenbezogenen Daten nicht mehr verarbeiten, wenn seine Prüfung ergibt, dass er keine zwingenden schutzwürdigen Gründe für die Ver-

---

59 S. hierzu auch *Klement*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 8 Rn. 16.

60 S. hierzu Kap. 3.4.

arbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Er darf die Daten weiterhin verarbeiten, wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Im Wesentlichen hat er also die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO unter Berücksichtigung der von der betroffenen Person neu vorgebrachten Argumente zu wiederholen.[61]

Welche Gründe, die sich aus der besonderen Situation der betroffenen Person ergeben, zu berücksichtigen sind, ist umstritten. Zum einen wird vertreten, dass es sich um atypische Konstellationen besonders schutzwürdiger persönlicher Interessen handeln muss.[62] Zum anderen wird dem entgegengehalten, dass diese Sichtweise zu eng sei und das Recht der betroffenen Person zu stark beschneide. Es müsse genügen, wenn diese konkrete Umstände des Einzelfalls vorträgt, die eine Beeinträchtigung ihrer Datenschutzrechte möglich erscheinen lassen.[63] Ob solche besonderen Gründe auch vorliegen, wenn die betroffene Person den Widerspruch damit begründet, dass der Verantwortliche die Daten eines Kindes erhoben und dabei dessen besondere Schutzbedürftigkeit nicht erkannt hat (Artikel-29-Datenschutzgruppe 2008: 12), ist somit unklar, weil die Verarbeitung personenbezogener Daten von Kindern nicht atypisch sein muss.

Zu beachten ist jedoch, dass der Verantwortliche die in Erwägungsgrund 38 Satz 1 DSGVO in Erinnerung gerufene besondere Schutzpflicht für Kinder ausreichend beachten muss. Sie sind „sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst". Um hier Missverständnisse auszuschließen und Rechtsklarheit zu schaffen, sollte der Wortlaut des Art. 21 Abs. 1 DSGVO klarstellen, dass der Verantwortliche bei der Prüfung der Berechtigung des Widerspruchs den Umstand, dass er Daten von Kindern verarbeitet, berücksichtigen muss.

Dies wäre auch systematisch korrekt. Wenn der Verantwortliche nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO bei seiner Interessenabwägung, die der Datenverarbeitung entgegenstehenden Interessen oder Grundrechte und Grundfreiheiten in besonderer Weise berücksichtigen muss, „wenn es sich bei der betroffenen Person um ein Kind handelt", dann muss dies auch für

61 S. auch *Caspar*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 21 Rn. 12.

62 S. z.B. *Martini*, in: Paal/Pauly, DSGVO, 2. Aufl. 2018, Art. 21 Rn. 30; *Herbst*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 21 DSGVO, Rn. 15 ff.

63 S. z.B. *Caspar*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 21 Rn. 7.

den Widerspruch gelten. Denn dieser ist das Recht der betroffenen Person, das diesem Erlaubnistatbestand korrespondiert. Wenn der Verantwortliche die Daten aufgrund seiner überwiegenden berechtigten Interessen auch gegen den Willen der betroffenen Person verarbeiten darf, dann muss sich ihre Möglichkeit des Opt-out darauf erstrecken können, dass der Verantwortliche die entgegenstehenden Interessen eines Kindes gerade nicht ausreichend berücksichtigt hat.

4.5 Keine Einwilligung in automatisierte Entscheidungen

Die betroffene Person hat nach Art. 22 Abs. 1 das Recht, „nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt". Von diesem Verbot gewährt Art. 22 Abs. 2 lit. c DSGVO eine Ausnahme, wenn die automatisierte Entscheidung auf einer ausdrücklichen Einwilligung beruht.[64] Zwar stellt Erwägungsgrund 71 Satz 5 DSGVO fest, dass „diese Maßnahme […] kein Kind betreffen" sollte. Diese Wertung ist jedoch nicht in der Vorschrift wiederzufinden. Auch gibt es im Normtext keine Anhaltspunkte, auf die sich diese Wertung im Sinn eines Verarbeitungsverbots stützen ließe. Daher sollte sie im Normtext des Art. 22 Abs. 2 lit. c DSGVO wiederzufinden sein. Die Einwilligung eines Kindes in eine auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung sollte ausdrücklich ausgenommen sein.[65] Die Wahrscheinlichkeit, dass ein Kind die Wirkungsweise, die Bedeutung und die Folgen einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung nicht ausreichend erkennt[66] und bewertet, und das Schadenspotential, das für das Kind aus dieser Datenverarbeitung erwachsen kann, sind hoch und rechtfertigen diese Regelung. Diese Ausnahme schließt die Einwilligung oder die Zustimmung eines Trägers der elterlichen Verantwortung zu einer Einwilligung des Kindes nicht aus.

---

64 Zu den Voraussetzungen diese Einwilligung s. *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 22 Rn. 52 ff.; *Buchner*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 22 DSGVO, Rn. 41f.

65 Noch weitergehender vzbv, Modernisierung des Datenschutzrechts, 2013, 17.

66 S. zu den Informationspflichten vor einer Einwilligung nach Art. 22 Abs. 2 lit. c DSGVO s. z.B. *Scholz*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 22 Rn. 54.

4.6 Datenschutzgerechte Systemgestaltung

Eine besondere Innovation der Datenschutz-Grundverordnung ist die in Art. 25 Abs. 1 geforderte datenschutzgerechte Systemgestaltung (Roßnagel 2019: 467). Die Vorschrift verpflichtet den Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu ergreifen, die die Datenschutzgrundsätze wirksam umsetzen und den Schutz der Rechte der betroffenen Personen garantieren.[67] Die Pflicht ist allerdings sehr weich formuliert und hochgradig unbestimmt. Hinzu kommen fünf Einschränkungen, diese Pflicht zu erfüllen. So sollen der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und der Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen Berücksichtigung finden. Die Bestimmung und Abwägung dieser Faktoren sind jedoch äußerst schwierig und geben dem Datenverarbeiter einen sehr großen Entscheidungs- und Gestaltungsspielraum.[68]

Damit dieser Spielraum nicht zu Lasten oder unter Vernachlässigung der Schutzpflicht gegenüber Kindern ausgenutzt wird, sollte die Vorschrift zur datenschutzgerechten Systemgestaltung den Schutz der Grundrechte und Interessen von Kindern in besonderer Weise einfordern (Datenethikkommission der Bundesregierung 2019: 115). Gerade bei der Systemgestaltung wäre ein grundlegender Schutz von Kindern – vor allem in Social Networks und anderen Angeboten mit datengetriebenen Geschäftsmodellen – besonders wichtig – und meist auch leicht zu realisieren.

4.7 Datenschutzfreundliche Voreinstellungen

Eine besondere Gestaltungspflicht des Verantwortlichen enthält auch Art. 25 Abs. 2 DSGVO. Nach dieser Vorschrift trifft der Verantwortliche geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung[69] grundsätzlich nur personenbezogene Daten,

67 S. hierzu ausführlich *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 25 Rn. 28 ff.

68 S. z.B. *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 25 Rn. 37f.; *Hartung*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 25 DSGVO, Rn. 19 ff.

69 S. zur Bedeutung und zu Beispielen vor Voreinstellungen *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 25 Rn. 41 ff.

deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung unterliegt nicht den einschränkenden Bedingungen der datenschutzgerechten Systemgestaltung gemäß Art. 25 Abs. 1 DSGVO.[70] Die Verpflichtung zur datenschutzfreundlichen Voreinstellung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Auch für datenschutzfreundliche Voreinstellung nach Art. 25 Abs. 2 DSGVO sollte die Vorschrift den Schutz von Kindern in besonderer Weise einfordern. Sie übernehmen – mehr noch als Erwachsene – die voreingestellten Werte und konzentrieren sich allein auf die Nutzung des Geräts oder des Dienstes. Diese spezifische Voreinstellung für Kinder ist vor allem für Social Networks wichtig (Roßnagel/Richter 2017: 205). In diesen ist oft die Weitergabe von Nutzungsdaten an Trackingdienste oder Werbenetzwerke voreingestellt. Gerade von Kindern kann nicht angenommen werden, dass sie Voreinstellungen erkennen und deren Bedeutung für ihre informationelle Selbstbestimmung verstehen. Auch kann nicht erwartet werden, dass sie sich mühsam durch die Einstellmöglichkeiten in den Menüs der Software klicken und die geeigneten Einstellungen finden, um ihre Selbstbestimmungsmöglichkeiten in dem von ihnen gewünschten Umfang zu wahren. Sie sind in besonderer Weise darauf angewiesen, dass die Grundeinstellungen das geringstmögliche Risiko für ihren Datenschutz aufweisen.

4.8 Datenschutz-Folgenabschätzung

Ein innovatives Instrument zur Durchsetzung von Datenschutzanforderungen ist die Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO (Friedewald/Schiering/Martin 2019: 473, Roßnagel 2019: 467). Eine solche hat der Verantwortliche nach Abs. 1 bei jeder Form der Datenverarbeitung, insbesondere bei Verwendung neuer Technologien, durchzuführen, wenn diese „aufgrund der Art, des Umfangs, der Umstände und der Zwe-

70 S. z.B. *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 25 Rn. 45; *Hartung*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 25 DSGVO, Rn. 27.

cke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat (Marschall 2018: 193ff). In diesem Fall hat er vor dem Beginn der Verarbeitung „eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten“ vorzunehmen.[71]

Aus den bereits vielfach genannten Gründen besteht bei der Verarbeitung personenbezogener Daten von Kindern ein besonderes Risiko und ein besonderer Schutzbedarf. Daher sollte sowohl für die Bestimmung der Notwendigkeit einer Datenschutzfolgenabschätzung nach Abs. 2 bis 4 als auch bei der Risikoanalyse und bei der Festlegung der Schutzmaßnahmen nach Abs. 7 dem Schutz der Grundrechte und Interessen von Kindern eine besondere Aufmerksamkeit entgegengebracht werden.[72]

4.9 Ergänzungen des Datenschutz-Grundverordnung

Diese Schutzregelungen können mit geringem Aufwand, aber hoher Wirkung in den Text der jeweiligen Vorschrift aufgenommen werden.[73] Hiermit sollte nicht bis zur nächsten Evaluation der Verordnung im Jahr 2024 gewartet werden. Über die besondere Schutzbedürftigkeit von Kindern dürfte auch kein politischer Streit entstehen.

5. Zusammenfassung und Ausblick

Die Datenschutz-Grundverordnung hat die Aufgabe eines besonderen Datenschutzes für Kinder erkannt, aber bisher nur punktuell und daher weder konzeptionell noch situativ ausreichend gelöst. Der Beitrag unterbreitet acht Vorschläge, die aus der besonderen Schutzbedürftigkeit von Kindern in der digitalen Welt abgeleitet sind. Diese sollte die Kommission auch außerhalb eines Evaluationsverfahrens aufnehmen und in eine rechtspolitische Diskussion zur praxisgerechten Fortentwicklung der Datenschutz-Grundverordnung einbringen. Sie würde damit einen wesentlichen

71 S. z.B. *Jandt*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl. 2018, Art. 35 DSGVO, Rn. 31 ff.

72 So noch der Kommissionsentwurf in Art. 32 Abs. 2 lit. d, der eine Datenschutzfolgenabschätzung forderte, wenn Daten von Kindern verarbeitet werden.

73 S. hierzu ausführlich mit Formulierungsvorschlägen *Roßnagel/Geminn*, Datenschutz-Grundverordnung verbessern, 2020.

Beitrag zur Erfüllung ihres Schutzauftrags und zur Akzeptanzsteigerung der Datenschutz-Grundverordnung leisten.

Neben der rechtspolitischen Fortbildung von Schutzstandards ist zu berücksichtigen, dass Datenschutz von Kindern auch eine Bildungs- und Erziehungsaufgabe ist. Das normative Konzept der informationellen Selbstbestimmung enthält grundsätzlich kein paternalistisches Schutzprogramm, sondern die Zielsetzung einer *Selbst*bestimmung. Die datenschutzrechtliche Einwilligung bietet dem Einzelnen die Möglichkeit, mit seinen personenbezogenen Daten so freizügig oder so restriktiv umzugehen, wie er selbst es möchte. Auch wenn diese Möglichkeit für Kinder wie dargestellt noch eingeschränkt ist, wachsen sie doch stetig weiter in die Eigenverantwortlichkeit hinein und sollten daher mit Erreichen des Erwachsenenalters ein aufgeklärtes, verantwortungsvolles Verhältnis zu ihren personenbezogenen Daten entwickelt haben, um ihre Selbstbestimmung auch wirklich ausüben zu können. Hieraus ergibt sich politisch und gesellschaftlich ein besonderer Bildungs- und Erziehungsauftrag (Roßnagel/Richter 2017: 205).

Literatur

Artikel-29-Datenschutzgruppe (2008): *Arbeitspapier zum Schutz der personenbezogenen Daten von Kindern* (Allgemeine Leitlinien und Anwendungsfall Schule, WP 147, Brüssel. Online verfügbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP147_WorkingDoc12008OnProtectionOfChildren.pdf?__blob=publicationFile&v=2 (Abfrage am: 05.10.2020).

Artikel 29-Datenschutzgruppe (2018): *Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, Brüssel*. Online verfügbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP260_LeitlinienFuerDieTransparenz.pdf;jsessionid=5D6705E60980393E0CC6EA2B35D8511C.1_cid344?__blob=publicationFile&v=2 (Abfrage am: 05.10.2020).

BITKOM (2017): *Kinder und Jugend in der digitalen Welt*. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/170512-Bitkom-PK-Kinder-und-Jugend-2017.pdf (Abfrage am: 05.10.2020).

Buchner, Benedikt (2018) in Kühling, Jürgen / Buchner, Benedikt (Hg.): *Datenschutz-Grundverordnung/BDSG. Kommentar*. 2. Aufl., München: C.H. Beck.

Bundesministerium für Familie, Senioren, Frauen und Jugend (2014): *Übereinkommen über die Rechte des Kindes. VN-Kinderrechtskonvention im Wortlaut mit Materialien*. Berlin. Online verfügbar unter: https://www.bmfsfj.de/blob/93140/78b9572c1bffdda3345d8d393acbbfe8/uebereinkommen-ueber-die-rechte-des-kindes-data.pdf (Abfrage am: 05.10.2020).

Callies, Christian / Ruffert, Matthias (2016): *EUV, AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtcharta*. 5. Aufl. München.

Caspar, Johannes (2019) in Simitis, Spiros /. Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht, DSGVO mit BDSG*. Baden-Baden: Nomos.

Däubler, Wolfgang (2018) in Däubler, Wolfgang / Wedde, Peter / Weichert, Thilo / Sommer, Imke (2018): *EU-DSGVO und BDSG*. Frankfurt/M.: Bund-Verlag.

Datenethikkommission der Bundesregierung (2019): *Gutachten der Datenethikkommission der Bundesregierung*. Berlin. Online verfügbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.html (Abfrage am: 05.10.2020).

Die Bundesregierung (2018): *Koalitionsvertrag CDU, CSU und SPD*. Online verfügbar unter: https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1 (Abfrage am: 05.10.2020).

Dix, Alexander (2019) in: Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (2019): *Datenschutzrecht, DSGVO mit BDSG*. Baden-Baden: Nomos.

Ernst, Stefan (2017): *Die Einwilligung nach der Datenschutzgrundverordnung. Anmerkungen zur Definition nach Art. 4 Nr. 11 DS-GVO*. In: Zeitschrift für Datenschutz (ZD) (3), S. 110–114.

Friedewald, Michael / Karaboga, Murat / Zoche, Peter (2015): *Das versteckte Internet – zu Hause – im Auto – am Körper. Whitepaper der Forums Privatheit und selbstbestimmtes Leben in der digitalen Welt*. Karlsruhe. Online verfügbar unter: http://friedewald.website/wp-content/uploads/2015/05/White-Paper-2-Final.pdf (Abfrage am: 05.10.2020).

Friedewald, Michael / Schiering, Ina / Martin, Nicholas (2019): *Datenschutz-Folgenabschätzung in der Praxis. Herausforderungen bei der Implementierung eines innovativen Instruments der DSGVO*. Datenschutz Datensich 43, S. 473–477. https://doi.org/10.1007/s11623-019-1146-y.

Gola, Peter (2018): *Datenschutz-Grundverordnung VO (EU)*. 2016/679, 2. Aufl. München: C.H. Beck.

Gola, Peter / Schulz, Sebastian (2013): *DS-GVO – Neue Vorgaben für den Datenschutz bei Kindern? Überlegungen zur einwilligungsbasierten Verarbeitung von personenbezogenen Daten Minderjähriger*. In: Zeitschrift für Datenschutz (ZD) (10), S. 475-480.

Hansen, Marit (2019) in Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht, DSGVO mit BDSG*, Baden-Baden: Nomos.

Hartung, Jürgen (2018) in Kühling, Jürgen / Buchner, Benedikt (Hg.): *Datenschutz-Grundverordnung/BDSG. Kommentar*. 2. Aufl., München: C.H. Beck.

Herbst, Tobias (2018) in Kühling, Jürgen / Buchner, Benedikt (Hg.): *Datenschutz-Grundverordnung/BDSG. Kommentar*. 2. Aufl., München: C.H. Beck.

Hohmann, Carolin / Miedzianowski, Nadine (2018) in Roßnagel, Alexander (Hg.): *Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze*, Baden-Baden: Nomos.

Holznagel, Bernd / Sonntag, Matthias (2003) in Roßnagel, Alexander (Hg.): *Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung*. 1.Aufl., München: C.H. Beck.

Jandt, Silke / Roßnagel, Alexander (2012): *Rechtsgutachten zum Datenschutz und zu Persönlichkeitsrechten im Social Web, insbesondere von Social Networking-Sites*. In: Schenk, Michael / Niemann, Julia / Reinmann, Gabi / Roßnagel, Alexander: Digitale Privatsphäre – Heranwachsende und Datenschutz auf sozialen Netzwerkplattformen (Hg.). Berlin: Vistas, S. 308-373.

Jandt, Silke / Roßnagel, Alexander (2011): *Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?* In: MultiMedia und Recht (10), S. 637–642.

Jandt, Silke (2018) in Kühling, Jürgen / Buchner, Benedikt (Hg.): *Datenschutz-Grundverordnung/BDSG. Kommentar*. 2. Aufl., München.

Jarass, Hans D. (2016): *Charta der Grundrechte der Europäischen Union. Kommentar.* 3. Aufl. München: C.H. Beck.

Jarass, Hans D. / Pieroth, Bodo (2018): *Grundgesetz für die Bundesrepublik Deutschland*. Kommentar. 15. Aufl. München: C.H. Beck.

Kampert, David (2018) in Sydow, Gernot (Hg.): *Europäischen Datenschutz-Grundverordnung. Handkommentar*. 2. Aufl., Baden-Baden: Nomos.

Kingreen, Thorsten (2016) in Callies, Christian / Ruffert, Matthias (Hg.): *EUV, AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtcharta*. 5. Aufl. München: C.H. Beck.

Klement, Jan Hendrik (2019) in Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht, DSGVO mit BDSG*. Baden-Baden: Nomos.

Kühling, Jürgen / Buchner, Benedikt (2018): *Datenschutz-Grundverordnung/BDSG. Kommentar*. 2. Aufl., München: C.H. Beck.

Marschall, Kevin (2018) in Roßnagel, Alexander (Hg.): *Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze*. Baden-Baden: Nomos.

MPFS – Medienpädagogischer Forschungsverbund Südwest (2016): *KIM-Studie 2016. Kindheit, Internet, Medien*. Online verfügbar unter https://www.mpfs.de/fileadmin/files/Studien/KIM/2016/KIM_2016_Web-PDF.pdf (Abfrage am: 05.10.2020).

MPFS – Medienpädagogischer Forschungsverbund Südwest (2018): *JIM-Studie 2018. Jugend, Information, Medien*. Online verfügbar unter: https://www.mpfs.de/fileadmin/files/Studien/KIM/2018/KIM-Studie_2018_web.pdf (Abfrage am: 05.10.2020).

Nebel, Maxi (2018) in Roßnagel, Alexander (Hg.): *Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze*. Baden-Baden: Nomos.

Nebel, Maxi / Dräger, Magdalena (2019): *Altersgrenzen für die Einwilligung von Kindern nach Art. 8 DS-GVO in den einzelnen Mitgliedstaaten*. In: ZD-aktuell, 06645, Heft 8/2019, VIII.

Martini, Mario (2018) in Paal, Boris P. / Pauly, Daniel (Hg.): *Datenschutz-Grundverordnung, Kommentar*, 2. Aufl. München: C.H. Beck.

Paal, Boris P. / Pauly, Daniel (2018): *Datenschutz-Grundverordnung, Kommentar*, 2. Aufl. München: C.H. Beck.

Peucker, Enrico (2018) in Sydow, Gernot (Hg.): *Europäischen Datenschutz-Grundverordnung. Handkommentar*. 2. Aufl. Baden-Baden: Nomos.

Polenz, Sven (2019) in Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht, DSGVO mit BDSG*. Baden-Baden: Nomos.

Reimer, Philipp (2018) in Sydow, Gernot (Hg.): *Europäischen Datenschutz-Grundverordnung. Handkommentar*. 2. Aufl. Baden-Baden: Nomos.

Roßnagel, Alexander (2018a), *Das neue Datenschutzrecht – Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze*. Baden-Baden: Nomos.

Roßnagel, Alexander (2018b): *Umsetzung der Unionsregelungen zum Datenschutz – Erste Erfahrungen mit der Datenschutz-Grundverordnung aus rechtswissenschaftlicher Sicht*. In: Datenschutz und Datensicherheit, S. 741-745.

Roßnagel, Alexander (2019): *Innovationen der Datenschutz-Grundverordnung*. In: Datenschutz und Datensicherheit, S. 467-472.

Roßnagel, Alexander (2019) in Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht, DSGVO mit BDSG*. Baden-Baden: Nomos.

Roßnagel, Alexander (2020): *Evaluation der Datenschutz-Grundverordnung. Verfahren – Stellungnahmen – Vorschläge*. In: Datenschutz und Datensicherheit, S. 287-292.

Roßnagel, Alexander (2020): *Die Evaluation der Datenschutz-Grundverordnung – Eine vertane Chance zur Verbesserung der Verordnung*. In: MMR 2020, S. 657-661.

Roßnagel, Alexander / Geminn, Christian (2020): *Datenschutz-Grundverordnung verbessern – Änderungsvorschläge aus Verbrauchersicht*. Baden-Baden: Nomos.

Roßnagel, Alexander / Richter, Philipp (2017): *Aufwachsen in virtuellen und technologisierten Welten: Herausforderungen der Datensammlung, Vernetzung, Kommerzialisierung und neuen Überwachungstechnologien für Jugendliche*. In: Sachverständigenkommission 15. Kinder- und Jugendbericht: Materialien zum 15. Kinder- und Jugendbericht: Zwischen Freiräumen, Familie, Ganztagsschule und virtuellen Welten – Persönlichkeitsentwicklung und Bildungsanspruch im Jugendalter. München, S. 205-260.

Schantz, Peter (2019) in Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht, DSGVO mit BDSG*. Baden-Baden: Nomos.

Scholz, Philip (2019) in Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hg.): *Datenschutzrecht, DSGVO mit BDSG*. Baden-Baden: Nomos.

Schwartmann, Rolf / Jaspers, Andreas /Thüsing, Gregor / Kugelmann, Dieter (2018): *DS-GVO/BDSG. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*. München: C.F. Müller.

Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (2019): *Datenschutzrecht, DSGVO mit BDSG*. Baden-Baden: Nomos.

Sydow, Gernot (2018): *Europäischen Datenschutz-Grundverordnung. Handkommentar*. 2. Aufl. Baden-Baden: Nomos.

Verbraucherzentrale Bundesverband (2013): *Modernisierung des europäischen Datenschutzrechts. Änderungsvorschläge der Verbraucherzentrale Bundesverbandes*. Berlin. Online verfügbar unter: https://diedatenschuetzerrheinmain.files.wordpress.com/2013/02/eu-datenschutz-grundverordnung-aenderungen-vzbv-2013-01-04.pdf (Abfrage am: 05.10.2020).

Wabnitz, Reinhard J. (2017): *Rechtliche Rahmung von Jugend (einschließlich der Rechte von jungen Erwachsenen) und persönliche Rechte von Jugendlichen (mit Blick auf die föderalen Ebenen und die unterschiedlichen Rechtsgebiete)*. Online verfügbar unter: https://www.dji.de/fileadmin/user_upload/bibs2017/15_KJB_Wabnitz_b.pdf (Abfrage am: 05.10.2020).

Weichert, Thilo (2018) in Däubler, Wolfgang / Wedde, Peter / Weichert, Thilo / Sommer, Imke: *EU-DSGVO und BDSG*. Frankfurt/M.: Bund-Verlag.

Wissenschaftliche Dienste des Deutschen Bundestags (2019): *Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon*. WD 10-3000-032/19. Online verfügbar unter: https://www.bundestag.de/resource/blob/650728/3f72e6abc1c524961e5809002fe20f21/WD-10-032-19-pdf-data.pdf (Abfrage am: 05.10.2020).

Digitales Lernen – Datenschutzrechtliche Rechtsgrundlagen von Lernplattformen für Kinder und Erwachsene

Maxi Nebel

Abstract

Lernplattformen bieten vielfältige Möglichkeiten des interaktiven, selbstbestimmten Lernens für Kinder und Erwachsene. Dabei gibt es eine große Bandbreite hinsichtlich der Systeme und deren Eigenschaften. Der folgende Beitrag untersucht, getrennt nach den verschiedenen Einsatzgebieten in der Schule einerseits und kommerzieller Angebote für Kinder und Erwachsene andererseits, welche Rechtsgrundlagen im jeweiligen Fall zum Einsatz kommen und welche datenschutzrechtlichen Anforderungen sich hieraus ergeben.

1. Einleitung

Ob virtuelles Klassenzimmer, Hausaufgaben, Nachhilfe, Ausbildung, berufsbegleitende Weiterbildung oder schlicht zur Freizeitgestaltung – webgestützte Lernplattformen bieten eine Reihe von Einsatzmöglichkeiten für alle Bevölkerungsgruppen. Dabei handelt es sich um Softwaresysteme zur Wissensvermittlung und Kommunikation zwischen Lernenden und Lehrenden. Sie bieten vielfältige Funktionalitäten: Neben dem Bereitstellen von Lerneinheiten, Arbeitsplänen, Arbeitsblättern, Tutorials und Videos bieten sie interaktive Übungen und kooperative Wikis sowie Kommunikationskanäle zwischen und unter Lehrenden und Lernenden.

Es gibt Softwarelösungen, die eigens für Schulen entworfen wurden und mithilfe derer jede Schule eine eigene Lernplattform nur für ihre Schülerinnen und Schüler[1] betreiben kann. Bekanntes Beispiel hierfür ist die Software Moodle. Weiterhin gibt es allgemein zugängliche Lernplattformen, die von Verlagen, Softwareherstellern oder Medienanstalten be-

1 In diesem Beitrag wird aus Gründen der besseren Lesbarkeit im Folgenden das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint.

trieben werden. Deren Zielpublikum erstreckt sich von Kindern im Vorschulalter über Schüler bis hin zu spezifischen Angeboten im Bereich der Erwachsenenbildung.[2]

Mit der Nutzung solcher Lernplattformen geht eine umfangreiche Datenverarbeitung einher. Da Lernplattformen sowohl im Schulunterricht eingesetzt als auch durch privatwirtschaftliche Dienstleister angeboten werden, ist bei der datenschutzrechtlichen Beurteilung eine Differenzierung vorzunehmen. Plakativ ist dabei die Unterscheidung zwischen dem so genannten Vormittagsmarkt für die Verwendung von Lernplattformen in der Schule und dem Nachmittagsmarkt für die Verwendung von privatwirtschaftlich betriebenen, vielleicht auch kostenpflichtigen Lernplattformen, die außerhalb des Schulbetriebs von Kindern, aber auch von erwachsenen Lernenden genutzt werden. Der folgende Beitrag untersucht zunächst die Chancen und Risiken, die sich aus der Nutzung von Lernplattformen ergeben können. Anschließend werden die personenbezogenen Daten kategorisiert, die regelmäßig auf entsprechenden Plattformen erhoben werden, um sodann die zu deren Verarbeitung notwendigen Rechtsgrundlagen zu identifizieren. Rechtsgrundlagen entscheiden über die weiteren datenschutzrechtlichen Anforderungen, auf die aus Gründen des Umfangs in diesem Beitrag nicht im Detail eingegangen werden kann. Der Beitrag schließt mit technischen und organisatorischen Gestaltungsvorschlägen.

2. *Chancen und Risiken von Lernplattformen*

Lernplattformen bieten vielfältige Chancen für die Bildung von Menschen: Sie ermöglichen eine multimediale, interaktive und kooperative Lernumgebung sowie eine flexible Nutzung, ohne örtlich oder zeitliche gebunden zu sein. Durch sie können an die Bedürfnisse des Einzelnen angepasste Lernziele verfolgt und individuelle Lernfortschritte erfasst werden. Lerninhalte können gezielt auf die jeweilige Person ausgerichtet werden und sich somit an den Stärken und Schwächen eines jeden Lernenden orientieren. Interaktive Arbeitsformen ermöglichen eine Kooperation zwischen Lehrenden und Lernenden und zwischen Lernenden untereinander.[3] Durch den Einsatz in Schulen wird die Medienkompetenz der Schüler von einem jungen Alter an gestärkt. Im Bereich der Erwachsenenbil-

2 Zum Datenschutz im E-Learning an Hochschulen s. Roßnagel 2020b: 296.
3 DSK 2018: 2 f.

dung verstärkt die Niedrigschwelligkeit der Angebote (keine formalen Zugangsvoraussetzungen, kostengünstige Programme) die Wahrscheinlichkeit, dass sich Lernende leichter zu allgemeinen oder berufsrelevanten Themen weiterbilden können (Life Long Learning).

Für die informationelle Selbstbestimmung und das Recht auf Datenschutz bergen Lernplattformen hingegen auch Risiken. Die umfassende Datenerhebung zu Art, Weise und Dauer der Nutzung, die Aufzeichnung des Lernfortschritts, -tempos und -inhalts verschafft einen Einblick in durchaus sensible Bereiche der persönlichen Fähigkeiten und Fertigkeiten und eröffnet damit die Möglichkeit, auf Charakter- und persönliche Eigenschaften rückzuschließen und Persönlichkeitsprofile zu erstellen.[4]

3. Kategorisierung der personenbezogenen Daten auf Lernplattformen

Bei der Nutzung von Lernplattformen werden eine Vielzahl verschiedener Daten verarbeitet. Diese lassen sich wie folgt kategorisieren. Notwendig sind zunächst der – möglichst pseudonyme – Benutzername und das Passwort.[5] Handelt es sich jedoch um eine geschlossene Plattform, etwa die einer Schule, an der nur Schüler und Lehrkräfte dieser Schule teilnehmen dürfen, werden weitere Daten zur Identifizierung der Person benötigt. In diesem Fall ist der Klarname der betroffenen Person erforderlich. Bei Kostenpflicht des Dienstes sind weiterhin Zahlungsdaten erforderlich. Lernplattformen können überdies so gestaltet sein, dass der Nutzer ein eigenes personalisiertes Profil anlegen kann. Entsprechend der Ausgestaltung kann es Möglichkeiten geben, individuelle Angaben zur Person zu machen und ein Profilbild auf die Plattform zu laden.[6] Da sich privatwirtschaftlich betriebene Lernplattformen an alle Schulformen in allen Bundesländern richten, sind überdies häufig Angaben zum Bundesland, zum besuchten Schultyp und Jahrgangsstufe notwendig.

Sind die Nutzer von Lernplattformen Kinder, muss die Einwilligung des Sorgeberechtigten eingeholt werden. Da der Verantwortliche diese dokumentieren und die Identität des Sorgeberechtigten verifizieren muss, werden je nach Ausgestaltung der Dokumentation auch personenbezogene Daten der Sorgeberechtigten erhoben und mit dem Profil des Nutzers verknüpft.

---

4 DSK 2018: 3 f.
5 DSK 2018: 6 spricht von Stammdaten.
6 DSK 2018: 7 spricht von optionalen Daten.

Weiterhin werden Daten zur Nutzung des Systems durch die betroffene Person erhoben. Zu diesen Nutzungsdaten gehören zum Beispiel IP-Adresse, An- und Abmeldezeit und damit Dauer der Nutzung, genutzte Dienste und anderes.[7]

Schließlich werden durch die Nutzung des Systems Daten mit inhaltlicher Relevanz zur Lernplattform erhoben. Man kann diese Kategorie als „Pädagogische Prozessdaten" bezeichnen.[8] Sie dienen dazu, dem Lehrenden den Lernprozess jedes einzelnen Nutzers oder einer ganzen Gruppe nachvollziehbar zu machen und anhand dessen das jeweilige Lernprogramm zu organisieren. Pädagogische Prozessdaten umfassen beispielsweise Kommentare und Nachrichten, Einträge in gemeinschaftlich bearbeiteten Datenbanken oder Dokumenten sowie Daten zur Bearbeitung von Lernobjekten, Aufgaben und Tests. Hinzukommen können weitere personenbezogene Daten durch zusätzlich implementierte Module (SCORM-, LTI-Module, Live Classroom, Plagiatsüberprüfung),[9] sofern der Verantwortliche entsprechende Funktionen in die Lernplattform eingebunden hat.

Weitere personenbezogene Daten können durch die Einbindung von Webanalyse-Diensten und Social Plug-ins entstehen. Webanalyse-Dienste sind spezielle Software-Tools, die Informationen zum Nutzungsverhalten, dem verwendeten Browser und dessen Einstellungen erheben. Sie werden eingesetzt, um beispielsweise Funktionalität der Website zu verbessern, zum Tracking der Nutzer und zum Einblenden personalisierter Werbung. Social Plug-ins sind Programmcodes, die Social Networks für Website-Betreiber zur Verfügung stellen und die diese in ihren Internetauftritt integrieren können. Bei Aufruf der Seite werden automatisch Daten an das Social Network geschickt, mindestens die aufgerufene URL und die IP-Adresse des Nutzers.[10] Ist der Nutzer gegenüber dem Social Network authentifiziert, können ihm die erhobenen Daten zugeordnet werden. Betätigt der Nutzer das Social Plug-in, bekommt das Social Network die Möglichkeit, Cookies im Browser des Nutzers zu speichern.[11] Mithilfe der Social Plug-ins wird es den Anbietern des Social Network erlaubt, über die Grenzen des Social Network hinaus Daten über Internetnutzer zu sammeln. Dies betrifft nicht nur eingeloggte Mitglieder, deren Daten mithilfe von Cookies direkt an das Social Network gesendet und ihrem Profil zugeordnet

7 DSK 2018: 8.
8 DSK 2018: 8 f.
9 DSK 2018: 9.
10 Z. B. Karg/Fahl 2011: 454; Jandt/Schaar/Schulz 2013: Rn. 117; Hornung 2015: Rn. 38. Zum Persönlichkeitsschutz in Social Networks ausführlich Nebel 2020.
11 Karg/Thomsen 2012: 731; Hornung 2015: Rn. 38.

werden. Aber auch nicht eingeloggte Mitglieder sowie Nicht-Mitglieder können aufgrund von Social Plug-ins verfolgt und zu einem Profil zusammengeführt werden.[12]

4. Rechtsgrundlagen für Schule als Verantwortliche

Der Verantwortliche bedarf für die Datenverarbeitung auf seiner Lernplattform einer Rechtsgrundlage. Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dies kann ein privatwirtschaftliches Unternehmen, eine Einzelperson, aber auch eine Schule sein. Für die Bestimmung der maßgeblichen Rechtsgrundlagen ist relevant, ob es sich um ein Unternehmen/eine Einzelperson oder um eine Behörde – bzw., da der Begriff Behörde funktional zu verstehen ist,[13] jede öffentliche Anstalt – handelt. Diese werden daher im Folgenden getrennt betrachtet.

Die Datenschutz-Grundverordnung (DSGVO) ist auf Schulen sachlich anwendbar nach Art. 2 DSGVO. Der Ausschluss des Art. 2 Abs. 2 lit. a DSGVO greift nicht, wonach die DSGVO auf Bereiche keine Anwendung findet, die nicht im Anwendungsbereich des Unionsrechts liegen. Zwar ist Bildung Sache der Länder, die Union hat aber Kompetenz zu Unterstützungs-, Koordinierungs- und Ergänzungsmaßnahmen nach Art. 5 und 165 AEUV in Verbindung mit der Zuständigkeit im Rahmen des Datenschutzes nach Art. 16 AEUV.[14] Sie ist auch örtlich anwendbar nach Art. 3 DSGVO, weil und sobald die Schule nach Abs. 1 in der Union niedergelassen ist oder nach Abs. 2 lit. b, weil die Lernplattform der Beobachtung des Verhaltens der Lernenden dient.

Betreibt eine Schule eine Lernplattform, so kommen als Ermächtigungsgrundlage einzig die Erfüllung einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO sowie die Wahrnehmung von Aufgaben im öffentlichen Interesse nach lit. e in Betracht. Auf berechtigte Interessen nach lit. f kann sich eine öffentliche Anstalt gemäß UAbs. 2 ebenso wenig stützen wie auf eine wirksame Einwilligung.

---

12 Z. B. Karg/Fahl 2011: 454; Karg/Thomsen 2012: 731.
13 Schantz 2019: Rn. 97.
14 So auch Sassenberg 2019: Rn. 2.

4.1 Datenverarbeitung aufgrund gesetzlicher Ermächtigung

Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO können selbst keine Datenverarbeitung rechtfertigen, sondern bedürfen in Verbindung mit Abs. 2 und 3 der Rechtsgrundlage eines Mitgliedstaates.[15] Ermöglicht ein Gesetz der Schule die Nutzung einer Lernplattform, kommt Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO zur Anwendung. Die Nutzung einer Lernplattform im Rahmen des Unterrichts dient zudem der Unterrichtsgestaltung und Schülerausbildung. Sie liegt damit im öffentlichen Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO. Die Datenverarbeitung muss erforderlich sein und es muss eine Rechtsgrundlage im mitgliedstaatlichen Recht vorliegen. Da das Schulwesen gemäß Art. 70 Abs. 1 in Verbindung mit Art. 72 ff. GG Sache der Länder ist, muss es sich bei dem mitgliedstaatlichen Recht um Landesrecht handeln, beispielsweise als Schuldatenschutz- oder Schulgesetz.

Im Hessischen Schulgesetz (HessSchulG) findet sich keine ausdrückliche Ermächtigung zum Einsatz von Lernplattformen.[16] Daher ist zu prüfen, inwiefern allgemeine Regelungen anwendbar sind. Das Landesrecht muss im Wortlaut eindeutig sein, also die Nutzung einer interaktiven Plattform zur Gestaltung des Unterrichts ermöglichen. Formulierungen wie die datenschutzrechtliche Generalklausel in § 83 HessSchulG „zur Durchführung schulorganisatorischer Maßnahmen erforderlich" ist nicht ausreichend, da sie nur das für die Verwaltung von Schulen Unabdingbare regelt[17] und schulorganisatorische Maßnahmen und der Unterrichtsauftrag auch durch weniger datenintensive Mittel erreicht werden können. Diese Annahme stützt auch die hessische Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen,[18] die das Schulgesetz ergänzt und genau auflistet, welche personenbezogene Daten erhoben werden dürfen. Diese enthält jedenfalls keine Erlaubnis für Lernplattform-Daten.

Die Erlaubnis zur Datenverarbeitung ergibt sich damit beispielsweise für hessische Schulen aus dem Hessischen Datenschutz- und Informationsfreiheitsgesetz (HDSIG). Nach § 3 Abs. 1 HDSIG ist die Datenverarbeitung zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der Schule lie-

15 Roßnagel 2019: Art. 6 Abs. 1 DSGVO, Rn. 52, 71; Schaller 2018: Rn. 8.
16 Anders hingegen z. B. § 38b SächsSchulG.
17 Profit 2018: 3.
18 https://www.rv.hessenrecht.hessen.de/bshe/document/hevr-SchulStatErhVHEpAnlage1.

genden Aufgabe oder in Ausübung öffentlicher Gewalt erforderlich ist.[19] Der Bildungs- und Erziehungsauftrag der Schule ergibt sich aus § 2 HessSchulG. Diesen hat die Schule selbständig und in Eigenverantwortung umzusetzen, §§ 127 ff. HessSchulG. Die Schulkonferenz beschließt im Rahmen ihrer gesetzlichen Befugnisse zum Entscheidungsrecht über das Schulprogramm die Bestimmung über den Einsatz einer Lernplattform an der jeweiligen Schule, § 129 Nr. 1 in Verbindung mit § 127b HessSchulG. Beschließt sie den Einsatz einer Lernplattform, dürfen dafür erforderliche personenbezogene Daten nach § 3 Abs. 1 HDSIG verarbeitet werden. Für besondere Kategorien personenbezogener Daten gelten mangels Einschlägigkeit des § 20 HDSIG für Lernplattformen die Vorgaben des Art. 9 DSGVO.

Der Einsatz einer Lernplattform kann grundsätzlich nicht auf eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 7 DSGVO gestützt werden, da die Wirksamkeitsvoraussetzungen insbesondere der Freiwilligkeit nicht erfüllt werden können.[20] Nach Erwägungsgrund 42 Satz 5 DSGVO ist eine Einwilligung etwa dann freiwillig, wenn die betroffene Person tatsächlich in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Sie muss also eine echte Wahlmöglichkeit haben und keine Nachteile befürchten müssen. Die Freiwilligkeit der Einwilligung ist auch dann in Frage gestellt, wenn zwischen dem Verantwortlichen und der betroffenen Person ein klares Ungleichgewicht besteht. Beispielhaft für ein klares Ungleichgewicht ist nach Erwägungsgrund 43 DSGVO das Verhältnis von Behörden zu betroffenen Personen. Für die Tätigkeiten von Behörden stellt die DSGVO dafür gesonderte Ermächtigungstatbestände und Öffnungsklauseln für eigene Regelungen der Mitgliedstaaten auf. Da zwischen Schule und Schüler ein Über-/Unterordnungsverhältnis besteht, dem sich der Schüler durch die bestehende Schulpflicht nicht entziehen kann, ist eine freiwillige Entscheidung unmöglich. Wird der Einsatz einer Lernplattform in der Klasse von der Einwilligung aller Schüler abhängig gemacht, kann sich der einzelne Schüler nicht entziehen, ohne Nachteile befürchten zu müssen. Dennoch wird beispielsweise in Sachsen-Anhalt beim Einsatz von Lernplattformen eine Einwilligung der Schüler bzw. der Eltern gefordert.[21] Dies ist, wie dargelegt, unrechtmäßig.

---

19 Für Hochschulen s. Roßnagel 2020b: 296.

20 Anders hingegen in Hochschulen, s. Roßnagel 2020b: 296.

21 Vgl. Vereinbarung über die Bereitstellung und Nutzung einer Instanz der Lernplattform Moodle für Schulen in Sachsen-Anhalt 2018, https://www.bildung-lsa.d

Mittels Lernplattformen können auch automatisierte Einzelentscheidungen wie Versetzungsentscheidungen, Leistungsbewertungen, Kurseinstufungen oder ähnliches gefällt werden. Die Zulässigkeit von automatisierten Einzelentscheidungen richtet sich nach Art. 22 DSGVO. Art. 22 Abs. 1 DSGVO gibt der betroffenen Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise beeinträchtigt. Die automatisierte Generierung von Einzelentscheidungen – oder vielmehr: algorithmenbasierte Entscheidung im Einzelfall – ist nach Abs. 2 lit. b und c dann zulässig, wenn unions- oder mitgliedstaatliches Recht sie erlaubt oder die betroffene Person eingewilligt hat. Im Schulrecht obliegen diese Entscheidungen ausschließlich den zuständigen Lehrkräften und der Klassenkonferenz und sind damit nach Art. 22 Abs. 2 DSGVO nicht zulässig.[22]

Die sonstigen Voraussetzungen der DSGVO sowie spezifischer landesgesetzlicher Regelungen – soweit vorhanden – sind einzuhalten. Zu beachten ist aber, dass in den landesgesetzlichen Regelungen gemäß Art. 6 Abs. 2 DSGVO spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder eingeführt werden können, sofern sie die Vorgaben der DSGVO präzisieren und konkretisieren.[23]

Der Verantwortliche hat also vor allem Informationspflichten einzuhalten, Betroffenenrechte zu gewährleisten und die Vorgaben zum Datenschutz durch Technik umzusetzen. Eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO ist notwendig, wenn die Datenverarbeitung ein hohes Risiko für die betroffenen Personen zur Folge hat. Da der Einsatz von Lernplattformen nur aufgrund einer gesetzlichen Grundlage möglich ist, ist eine Datenschutz-Folgenabschätzung gemäß Abs. 10 vorzunehmen, wenn nicht bereits eine allgemeine Folgenabschätzung im Zusammenhang mit dem Erlass der Rechtsgrundlage erfolgte und dies nach Einschätzung des zuständigen Gesetzgebers nötig ist.[24]

---

e/files/b91568b2b16749b6bd47d9d05ff2c859/LISA_Nutzungsvereinbarung_Schulinstanz.pdf.

22 In Hessen ergeben sich die Befugnisse zu Versetzungsentscheidungen, Leistungsbewertungen und Kurseinstufungen aus § 73 Abs. 3, § 75 Abs. 4, § 76 Abs. 2 HessSchulG.

23 Zum Regelungsumfang des Art. 6 Abs. 2 DSGVO Roßnagel 2019: Art. 6 Abs. 2 DSGVO, Rn. 22 ff.

24 Ausführlich zum Verfahren nach Art. 35 Abs. 10 DSGVO Roßnagel/Geminn/Johannes 2019: 435.

4.2 Social Media an Schulen

Eine gesonderte Betrachtung verdient der Einsatz von Social Media an Schulen. WhatsApp wird regelmäßig zur Kommunikation unter Schülern sowie zwischen Schülern und Lehrern genutzt. Video-Plattformen wie YouTube fungieren bei vielen Kindern und Jugendlichen als Online-Lehrer.[25] Auch andere Social Media-Kanäle eignen sich nicht nur zum Kommunizieren, sondern auch zum Lernen, Recherchieren und Analysieren. Ein gezielter Einsatz von Social Media im Unterricht hätte für Schulen den Vorteil, Medienkompetenz quasi nebenbei zu vermitteln, und zwar auf Plattformen, die Kinder ohnehin nutzen.

Die Regelungen der einzelnen Bundesländer reichen – sofern sie sich überhaupt zu dem Thema positionieren – von einem ausdrücklichen Nutzungsverbot bis hin zum erwünschten Einsatz für Lehrzwecke. Das Bremische Schuldatenschutzgesetz erlaubt in § 4 Abs. 4 den Einsatz von Social Media, wenn dies dem Schulleben dient, die spezifische Plattform der DSGVO entspricht und die Schulleitung eingewilligt hat. In Baden-Württemberg untersagt das Kultusministerium etwa den Einsatz von Social Media zur Kommunikation zwischen Lehrkräften und Schülern, verweist aber stattdessen auf Lernplattformen wie Moodle. Nach einer Handreichung des hessischen Kultusministeriums sollte „[d]ie Nutzung von öffentlichen oder kommerziellen Sozialen Netzwerken im Bereich der schulischen und unterrichtsrelevanten Kommunikation (…), wenn überhaupt, nur sehr eingeschränkt erfolgen. Das Hessische Kultusministerium empfiehlt vielmehr die Nutzung von schulinternen Lernplattformen, wie beispielsweise Schul-Moodle Hessen (…).“[26]

Aus datenschutzrechtlicher Sicht sprechen viele Gründe gegen den Einsatz von Social Media.[27] Wenn ein Schulgesetz oder eine Schule den Gebrauch von Social Media im Unterricht vorschreibt, benötigt jedes Kind ein entsprechendes Nutzerkonto, da eine Nutzung ohne eigenes Konto regelmäßig nicht möglich ist. Die Voraussetzungen der Einwilligung nach Art. 7 und 8 DSGVO müssen auch hier beachtet werden. Allerdings kann von einer freiwilligen Einwilligung kaum die Rede sein. Bei der datenschutzrechtlichen Beurteilung bleiben viele Punkte problematisch, etwa zur Frage der Verantwortlichkeit für die Datenverarbeitung. Ob die Haus-

25 *Ratzsch* 2019.

26 https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/nutzung-sozialer-netzwerke-durch-lehrkräfte.

27 Zum Persönlichkeitsschutz in Social Networks ausführlich Nebel 2020.

haltsausnahme des Art. 2 Abs. 2 lit. c DSGVO greift, muss bezweifelt werden, da im schulischen Kontext schwerlich von einer ausschließlich privaten und familiären Nutzung ausgegangen werden kann.[28] Da jeder Nutzer, also auch jedes Kind, personenbezogene Daten anderer Nutzer verarbeitet und für diese dann datenschutzrechtlich verantwortlich ist, treffen diesen auch die Pflichten zum Einholen einer Einwilligung und zur Gewährleistung der Betroffenenrechte. Problematisch ist außerdem die Datenübertragung in Drittstaaten, wenn das Unternehmen – wie Facebook oder Google – seinen Sitz nicht in der Union hat. Setzt eine Schule Social Media ein, gilt es alles dies zu bedenken, da datenschutzrechtliche Pflichten von der Schule auf die Nutzer abgewälzt würden, wenn der Einsatz von Social Media vorgeschrieben wäre.

Ebenso problematisch ist die eigenständige Nutzung von Social Media durch die Schule. Bindet eine Schule das Social Network in ihre eigene Kommunikationsstruktur ein, indem sie eine öffentliche Profilseite bei einem Social Network – etwa Fanpages bei Facebook oder einen Videokanal bei YouTube – für ihren Öffentlichkeitsauftritt betreibt oder um Informationen an ihre Schüler zu vermitteln, stellt sich die Frage, inwiefern sie für die dabei verarbeiteten personenbezogenen Daten der Nutzer verantwortlich ist. Der Europäische Gerichtshof hat sich zur Frage der Verantwortlichkeit von Fanpage-Betreibern eindeutig geäußert. Die Verarbeitung personenbezogener Daten ermöglicht Facebook nicht nur, das werbebasierte Geschäftsmodell zu verbessern. Es ermöglicht darüber hinaus den Betreibern der Fanpage, Kenntnis über die Profile der Besucher zu erlangen. Damit verfolgt der Fanpage-Betreiber eigene Zwecke und trägt durch das Einrichten der Fanpage maßgeblich dazu bei, dass personenbezogene Daten der Besucher durch Facebook erhoben werden.[29] Dadurch ist der Fanpage-Betreiber ebenso gemäß Art. 4 Nr. 7 DSGVO Verantwortlicher für die Datenverarbeitung, und zusammen mit dem Anbieter sind beide gemeinsam im Sinne des Art. 26 DSGVO für die Verarbeitung verantwortlich.[30] Die Schule muss also gemäß Art. 26 Abs. 1 DSGVO eine Vereinbarung mit dem Social Network treffen, wer welche Verpflichtungen aus der DSGVO, insbesondere hinsichtlich der Informationspflichten und Gewährleistung der Betroffenenrechte, zu erfüllen hat. Aus diesen Gründen ist es grundsätzlich nicht empfehlenswert, als Schule eine öffentliche Profilseite oder einen Videokanal bei einem Social Network zu betreiben.

28 Ausführlich Roßnagel 2019: Art. 2 DSGVO, Rn. 23 ff.
29 EuGH, Urt. v. 5.6.2018, Rs. C-210/16, ECLI:EU:C:2018:388, Rn. 34-36 – Fanpage.
30 EuGH, Urt. v. 5.6.2018, Rs. C-210/16, ECLI:EU:C:2018:388, Rn. 39, 43 – Fanpage.

4.3 Altersgrenze zur Geltendmachung von Betroffenenrechten

Als Verantwortliche hat die Schule die Betroffenenrechte der Schüler zu gewährleisten. Diese ergeben sich in erster Linie aus Art. 15 ff. DSGVO. Im Rahmen des Art. 23 DSGVO können Mitgliedstaaten durch eigene Rechtsvorschriften von den Vorgaben der DSGVO abweichen. Ist die Schule für die Datenverarbeitung verantwortlich, sind zur Bestimmung der Ausgestaltung der Betroffenenrechte auch die Landesvorschriften, in Hessen beispielsweise §§ 31 ff. HDSIG, zu beachten. Ab wann Kinder als betroffene Personen ihre Betroffenenrechte selbst wahrnehmen dürfen, ist gesetzlich nicht festgelegt. Da die DSGVO keine Regelungen hierzu trifft, richtet sich die Beurteilung der Altersgrenze nach der Einsichtsfähigkeit des jeweiligen Kindes und bedarf damit einer Einzelfallentscheidung. Der Landesgesetzgeber darf grundsätzlich eine Typisierung nach dem Alter der Schüler vornehmen, um einheitliche Regelungen zu erlassen und nicht in jedem Einzelfall nach der Einsichtsfähigkeit entscheiden zu müssen. Da dies einen Eingriff in die informationelle Selbstbestimmung der Schüler darstellt, muss ein entsprechendes Gesetz angemessen und erforderlich sein. Besser noch wäre ein gemeinsamer Standpunkt der Kultusministerkonferenz, um gleichmäßige Altersgrenzen in allen Bundesländern zu etablieren. Dies ist bisher nicht geschehen.[31]

5. Rechtsgrundlage für sonstige Betreiber als Verantwortliche

Lernplattformen werden nicht nur von Schulen betrieben, sondern beispielsweise auch von privatwirtschaftlichen Unternehmen oder Verlagen. Die DSGVO ist anwendbar nach Art. 3 DSGVO, wenn der Verantwortliche nach Abs. 1 in der Union niedergelassen ist oder nach Abs. 2 lit. a, wenn er der betroffenen Person Waren oder Dienstleistungen, also etwa elektronische Lernplattformen, anbietet. Diese dienen auch der Beobachtung des Verhaltens, so dass die DSGVO auch nach Abs. 2 lit. b Anwendung findet. Als Rechtsgrundlage kommt die Einwilligung nach Art. 6

31 Einzig der Freistaat Sachsen hat eine Vorschrift erlassen, und in Abschnitt IV Nr. 2 der sächsische Verwaltungsvorschrift Schuldatenschutz eine Altersgrenze von 14 Jahren zur selbständigen Geltendmachung von Betroffenenrechten festgelegt. Die Regelung ist inhaltlich nicht zu beanstanden, allerdings formell rechtswidrig, da es sich nicht um ein parlamentarisches Gesetz handelt.

Abs. 1 UAbs. 1 lit. a DSGVO in Frage, die Verarbeitung zur Vertragserfüllung nach lit. b sowie berechtigte Interessen nach lit. f.

Die Systematik des Art. 6 Abs. 1 DSGVO sieht vor, dass grundsätzlich mehrere Erlaubnistatbestände einschlägig sein und alternativ herangezogen werden können („mindestens"). Gerade im Verhältnis von Einwilligung nach lit. a und berechtigtem Interesse nach lit. f kommt es aber zu Spannungen zwischen dem Interesse des Verantwortlichen und der Erwartungshaltung der betroffenen Person hinsichtlich der Kontrolle über ihre personenbezogenen Daten.[32] Der Verantwortliche muss sich vor der Datenverarbeitung für den jeweiligen Zweck verbindlich auf die konkrete Rechtsgrundlage festlegen und die betroffene Person darüber entsprechend informieren, sonst widerspräche er dem Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a DSGVO, wenn er sich nachträglich auf eine andere Rechtsgrundlage berufen würde.

5.1 Verarbeitung aufgrund eines Vertrags

Nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO ist eine Verarbeitung rechtmäßig, wenn sie zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist. Erforderlich ist die Datenverarbeitung, wenn sie zur Erfüllung von Pflichten aus dem Vertrag benötigt werden.[33] Die vertragscharakteristische Leistung bei Lernplattformen ist die Bereitstellung von Alter und besuchtem Schulzweig der betroffenen Person abhängigen Lerninhalten sowie gegebenenfalls andere Leistungen wie Videoübertragung oder Möglichkeiten zur Plagiatsprüfung.[34] Erforderlich sind Stammdaten zum Einloggen auf die Plattform (Nutzername und Passwort) sowie Angaben zur Jahrgangsstufe, Schulzweig sowie Bundesland des Wohnortes. Auch die pädagogischen Prozessdaten lassen sich über lit. b rechtfertigen, da sie zur Erfüllung der Aufgaben der Lehrpersonen und damit zur Erbringung der Dienstleistung erforderlich sind. Erforderlich sind außerdem etwa die IP-Adresse und Session-Cookies, die während der Sitzung zur Aufrechterhaltung des Dienstes benötigt werden.[35]

32 Dazu Schantz 2019: Rn. 88 ff. sowie Nebel 2020: 178 f.
33 Z. B. Schantz 2019: Rn. 24 ff., Nebel 2020: 198 ff.
34 Vgl. DSK 2018: 9.
35 So auch Schulz 2018: Art. 6 DSGVO, Rn. 34.

Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO setzt voraus, dass die betroffene Person Vertragspartei ist. Ist die betroffene Person volljährig, ist dies unproblematisch. Im Falle von Lernplattformen für Kinder heißt das aber, dass der Verantwortliche einen wirksamen Vertrag mit dem Kind abschließen muss. Das Kind muss nach den Regeln des §§ 104 ff. BGB vom Sorgeberechtigten vertreten werden. Da der Abschluss eines Dienstleistungsvertrags – in der Regel bereits aufgrund der Zahlungspflicht – nicht ausschließlich rechtlich vorteilhaft ist, muss der Sorgeberechtigte gemäß § 107 BGB einwilligen. In der Praxis werden auf Lernplattformen regelmäßig die Eltern angesprochen, einen Vertrag abzuschließen, damit deren Kind die Plattform nutzen kann. Der Wortlaut der DSGVO ist in dieser Hinsicht eindeutig: Es bedarf einer entsprechenden Ausgestaltung des Vertrags, in denen die Eltern nicht als eigener Vertragspartner, sondern nur in Vertretung des betroffenen Kindes handeln.

5.2 Verarbeitung aufgrund berechtigter Interessen

Kann sich der Verantwortliche aus rechtlichen Gründen nicht auf Art. 6 Abs. 1 lit. b DSGVO stützen, wird er ein berechtigtes Interesse an der Verarbeitung der Stamm- und pädagogischen Prozessdaten geltend machen. Eine Datenverarbeitung ist nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zulässig, wenn die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Der Verantwortliche ist verpflichtet, eine umfassende Interessenabwägung vorzunehmen und zu dokumentieren. Lit. f legt aber fest, dass die Interessen oder Grundrechte und Grundfreiheiten in der Regel überwiegen, wenn die betroffene Person ein Kind ist, denn die Schutzbedürftigkeit der Kinder, insbesondere derer unter 16 Jahren, gebietet es, die Eltern in die Entscheidung über die Datenverarbeitung mit einzubinden,[36], also deren Einwilligung einzuholen. Daher kann lit. f in der Regel nicht für die Rechtfertigung der Verarbeitung der Stamm- und pädagogischen Prozessdaten der Kinder herangezogen werden.

Häufig wird der Verantwortliche als berechtigtes Interesse zudem die Verarbeitung personenbezogener Daten zu Werbezwecken geltend machen. Nach Erwägungsgrund 47 DSGVO „kann“ Direktwerbung als be-

36 Buchner/Petri 2018: Rn. 155.

rechtigtes Interesse betrachtet werden. Dies schließt personalisierte Werbung grundsätzlich mit ein.[37] Diese ist jedoch wesentlich eingriffsintensiver als herkömmliche Werbung, da hierfür ein umfassendes Persönlichkeitsprofil erstellt wird. Je umfassender das Persönlichkeitsprofil der betroffenen Person, desto eher überwiegen ihre Interessen, Grundrechte und Grundfreiheiten dem Werbeinteresse des Anbieters. Zu berücksichtigen ist auch die Möglichkeit der betroffenen Person zur Wahrnehmung ihrer Betroffenenrechte. So ist etwa das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO nur bei einer Einwilligung als Rechtsgrundlage möglich, nicht hingegen bei einer Interessenabwägung. Datenverarbeitung zum Zwecke personalisierter Werbung wird daher nicht über lit. f gerechtfertigt werden können, erst recht nicht, wenn es sich bei der betroffenen Person um ein Kind handelt. Auch wenn die Sorgeberechtigten die Vertragspartner der Plattformbetreiber sind, so werden die Plattformen doch durch die Kinder genutzt und diese sind damit auch die betroffenen Personen, deren Verhalten getrackt wird und denen personenbezogene Werbung präsentiert wird. Dieser „Missverhältnis" spricht noch mehr dafür, in jedem Fall eine ausdrückliche Einwilligung einzuholen.

Im Ergebnis kann eine Datenverarbeitung für Werbezwecke nicht über Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt werden. Gleiches gilt für die personenbezogenen Daten von Kindern, die Lernplattform nutzen. Vielmehr bedarf es in beiden Fällen einer Einwilligung.

5.3 Datenverarbeitung aufgrund einer Einwilligung

Kann sich der Verantwortliche nicht auf die Vertragsdurchführung oder berechtigte Interessen berufen, muss er eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO in Verbindung mit Art. 7 DSGVO einholen. Die Voraussetzungen der Einwilligung ergeben sich aus einem Zusammenspiel von Art. 4 Nr. 11 mit Art. 6 Abs. 1 UAbs. 1 lit. a sowie Art. 7 DSGVO[38] und werden zusätzlich durch die allgemeinen Verarbeitungsgrundsätze des Art. 5 DSGVO ergänzt. Es müssen also alle Voraussetzungen einer wirksamen Einwilligung vorliegen. Handelt das Kind als betroffene Person selbst, gilt zusätzlich die Regelung des Art. 8 DSGVO.

37 Z. B. Schantz/Wolff 2017: Rn. 666, Gierschmann 2018: 9 ff.; Nebel 2020: 206 ff., Helfrich 2020: Rn. 77. A. A. Schulz 2018: Art. 21 DSGVO, Rn. 20.

38 Kritisch zum Regelungskonzept Heckmann/Paschke 2018: Art. 7 DSGVO, Rn. 2.

Gemäß Art. 4 Nr. 11 DSGVO handelt es sich bei der Einwilligung um eine unmissverständlich abgegebene Willensbekundung „in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung". Die „eindeutige bestätigende Handlung" besteht nach Erwägungsgrund 32 DSGVO zum Beispiel in einer schriftlichen, elektronischen oder mündlichen „Erklärung", mit der die betroffene Person ihr Einverständnis mit der Datenverarbeitung signalisiert. Diese Erklärung kann auch durch das Anklicken eines Kästchens, durch „Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft" oder andere Verhaltensweisen abgegeben werden. Stillschweigen, Inaktivität und vorangekreuzte Kästchen sind nach Erwägungsgrund 32 DSGVO ebenso wenig ausreichend wie die schlichte Inanspruchnahme eines Dienstes.[39] Die DSGVO fordert somit ein Opt-in in die Datenverarbeitung. Die Opt-out-Lösung des Bundesgerichtshofs[40] ist nach der DSGVO nicht mehr zulässig.[41]

Die Willensbekundung muss „in informierter Weise" abgegeben worden sein. Die betroffene Person muss die Möglichkeit gehabt haben, den Inhalt der Erklärung zur Kenntnis nehmen[42] und Auswirkungen, Umstände und Tragweite der Datenverarbeitung erkennen zu können.[43] Die Einwilligung ist für einen oder mehrere bestimmte eindeutige und legitime Zwecke zu geben, sie muss demnach bestimmt genug sein. Der Zweck der Datenverarbeitung muss vom Verantwortlichen zum Zeitpunkt der Einwilligung so präzise festgelegt werden, dass die betroffene Person in der Lage ist zu beurteilen, aus welchem Grund der Verantwortliche bestimmte personenbezogene Daten verarbeiten möchte.

Schließlich muss die Einwilligung freiwillig erteilt worden sein. Eine Einwilligung ist freiwillig, wenn sie auf der freien Entscheidung der betroffenen Person beruht und ohne Zwang gegeben wurde. Die betroffene Person muss also eine echte Wahl haben.[44] Da die Freiwilligkeit der Einwilligung in vielen Konstellationen problematisch ist und war, hat die DSGVO einige zusätzliche Erfordernisse formuliert, die bei der Beurteilung der Freiwilligkeit herangezogen werden können. Dazu gehören die Feststellung von Nachteilen für die betroffene Person, ein mögliches Un-

39 Zu letzterem Art.-29-Datenschutzgruppe 2018: 16.
40 BGHZ 117, 253 – Payback; BGH, Urt. v. 11.11.2009, Az. VIII ZR 12/08 – Happy Digits.
41 Z. B. Schantz/Wolff 2017: Rn. 492, Ingold 2020: Rn. 43; Art.-29-Datenschutzgruppe 2018: 16, Nebel 2018: Rn. 95.
42 Ernst 2018: Rn. 79.
43 Buchner/Kühling 2018: Art. 4 Nr. 11 DSGVO, Rn. 8 und Art. 7 DSGVO, Rn. 59.
44 Z. B. Erwägungsgrund 42 DSGVO, Heberlein 2018: Rn. 7.

gleichgewicht zwischen betroffener Person und Verantwortlichem sowie die Koppelung der Einwilligung an andere Leistungen. Dabei sind in jedem Fall alle Umstände des Einzelfalls heranzuziehen.[45]

5.4 Besonderheiten der Einwilligung von Kindern

Ist die Einwilligung eines Kindes einzuholen, ist Art 8 DSGVO zu beachten.[46] Nach diesem ist die Verarbeitung von personenbezogenen Daten im Rahmen von Diensten der Informationsgesellschaft, die Kindern direkt angeboten werden, dann rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat oder die Einwilligung oder Zustimmung des Sorgeberechtigten eingeholt wurde.

Lernplattformen sind Dienste der Informationsgesellschaft nach Art. 4 Nr. 25 DSGVO in Verbindung mit Art. 1 Nr. 1 lit. b der Informationsverfahrensrichtlinie.[47] Sie sind elektronisch und auf individuellen Abruf des Empfängers erbrachte Dienstleistungen. Sie sind im Fernabsatz erbracht und erfolgen gegen Entgelt, entweder in Form einer Geldzahlung oder durch die Kommerzialisierung der Nutzerdaten.[48]

Der Dienst muss dem Kind direkt angeboten werden. Unstrittig sind Dienste, die sich durch die Art der Dienstleistung, die optische Gestaltung, kindgerechte Sprache und Anrede sowie Art der Werbung direkt an Kinder richten.[49] Daneben sind auch solche Dienste erfasst, die sich sowohl an Erwachsene als auch an Kinder richten, indem sie keine konkrete Zielgruppe ansprechen („dual use")[50] oder minderjährige Nutzer durch ihre Allgemeinen Geschäftsbedingungen zulassen.[51] Lernplattformen für Schüler richten sich naturgemäß an Kinder, aber auch an deren Sorgeberechtigten. Die Art der Dienstleistung bringt es zwingend mit sich, dass zumindest die Kinder diejenigen sind, die die Plattform nutzen, selbst wenn der Plattformbetreiber eher die Eltern anspricht. Daher gelten auch Lernplattformen für Schüler als direkt einem Kind angeboten.

---

45 Ausführlich zur Einwilligung Nebel 2020: 177 ff. mit weiteren Nachweisen.
46 Ausführlich zur Einwilligung bei Kindern auch Nebel 2020: 225 ff. mit weiteren Nachweisen.
47 Richtlinie 2015/1535/EU, ABl. EU 2015, L 241, 1.
48 Buchner/Kühling 2018: Art. 4 Nr. 25 DSGVO, Rn. 6.
49 Z. B. Buchner/Kühling 2018: Art. 8 DSGVO, Rn. 16, Klement 2019: Rn. 14.
50 Z. B. Buchner/Kühling 2018: Art. 8 DSGVO, Rn. 16, Frenzel 2018: Rn. 7, Klement 2019: Rn. 14.
51 So auch Kampert 2020: Rn. 9.

Hat das Kind das 16. Lebensjahr noch nicht vollendet, so ist die Verarbeitung der personenbezogenen Daten des Kindes nur rechtmäßig, wenn und soweit der Träger der elterlichen Verantwortung – der Sorgeberechtigte, im Regelfall also die Eltern – eingewilligt oder zugestimmt haben.[52] Da die informationelle Selbstbestimmung ein höchstpersönliches Rechtsgut ist, muss die Einwilligung im Interesse des Kindes und Kindswohles erfolgen.[53] Vom Sorgeberechtigten erfordert dies eine eigene, intensive Auseinandersetzung mit den Möglichkeiten und Risiken moderner Datenverarbeitungstechnologien.[54] Nach Art. 8 Abs. 2 DSGVO hat der Verantwortliche unter Berücksichtigung der verfügbaren Technologien angemessene Anstrengungen zu unternehmen, um sich zu vergewissern, dass die Einwilligung durch den Sorgeberechtigten oder mit dessen Zustimmung gegeben wurde. Da ein Verstoß gegen Art. 8 DSGVO nach Art. 83 Abs. 5 lit. a DSGVO bußgeldbewehrt ist, kommt der Frage der Umsetzung des Art. 8 Abs. 2 DSGVO eine nicht zu unterschätzende Bedeutung zu.

In Deutschland hat das sich das sogenannte Double-Opt-in-Verfahren als Maßnahme zur Einholung der Einwilligung oder Zustimmung in der Praxis durchgesetzt.[55] Dabei wird eine E-Mail an die E-Mail-Adresse der Sorgeberechtigten geschickt, mittels derer diese ihre Einwilligung oder Zustimmung erteilen können. Zwar besteht ein gewisses Missbrauchsrisiko durch das Kind, indem dieses eine zweite E-Mail-Adresse einrichtet, die den Anschein erweckt, dem Sorgeberechtigten zu gehören oder ohne deren Wissen die tatsächliche Mail-Adresse der Sorgeberechtigten nutzt. Formal wird es jedoch als ausreichend angesehen; die Umgehungsmöglichkeiten sind hinzunehmen, da dies zu verhindern der elterlichen Verantwortung obliegt und nicht den Verantwortlichen für die Datenverarbeitung.[56]

6. Gestaltungsvorschläge und Fazit

Lernplattformen sind eine wichtige Ergänzung sowohl im Rahmen des Schulalltags als auch außerhalb. Insbesondere wenn Kinder die Zielgruppe sind, ist jedoch ganz besonders auf den datenschutzkonformen Einsatz

52 Zur Abgrenzung von Einwilligung und Zustimmung z. B. Heckmann/Paschke 2018: Art. 8 DSGVO, Rn. 26 f.
53 Ausführlich Heckmann/Paschke 2018: Art. 8 DSGVO, Rn. 28 f.
54 AG Bad Hersfeld, Beschl. v. 15.5.2017, F 120/17 EASO.
55 Z. B. Schulz 2018: Art 8 DSGVO, Rn. 21, Heckmann/Paschke 2018: Art. 8 DSGVO, Rn. 37, Buchner/Kühling 2018: Art. 8 DSGVO, Rn. 24.
56 Z. B. Schulz 2018: Art 8 DSGVO, Rn. 21.

und die Gestaltung der Plattformen Wert zu legen. Dies beginnt mit der Ermittlung der korrekten Rechtsgrundlage, die in der Praxis bisher nicht immer gelingt, da dies häufig mit Unsicherheiten und einigen rechtlichen Fallstricken behaftet ist. Der Beitrag hat erläutert, dass der Einsatz einer Lernplattform an einer Schule nicht auf Basis von Einwilligungen der Schüler bzw. deren Sorgeberechtigten erfolgen darf. Der zuständige Landesgesetzgeber muss vielmehr gesetzlich festlegen, dass eine Schule eine Lernplattform einsetzen darf. Er kann gemäß Art. 6 Abs. 2 und 3 DSGVO gleichzeitig spezifische Anforderungen für die Datenverarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten. Ebenso sollte unter den gleichen Voraussetzungen der Einsatz von Social Media an Schulen gesetzlich geregelt werden. Betreiber kommerzieller Plattformen müssen sich andererseits um eine wirksame Einwilligung der betroffenen Personen, im Falle von Kindern um die Einwilligung der Sorgeberechtigten, bemühen. Ein Rückgriff auf berechtigte Interessen oder die Verarbeitung zu Vertragszwecken ist häufig in diesem Fall nicht möglich.[57]

Für die organisatorische und technische Gestaltung von Lernplattformen sind weitere Faktoren wichtig, um eine datenschutzkonforme Nutzung zu gewährleisten. Hierzu zählen etwa die Schutzbedarfsanalyse der konkret zu verarbeitenden Daten und darauf aufbauende Ermittlung der zu ergreifenden Schutzmaßnahmen.[58] Dazu gehört weiterhin die Datentrennung nach Nutzern und erhobenen Zwecken, um Risiken eines Datenmissbrauchs vorzubeugen. Wichtig ist außerdem die Umsetzung von Rollen- und Berechtigungskonzepten und Zugriffsrechten, welche vorab zu definieren sind, um sicherzustellen, dass nur berechtigte Personen und nur im notwendigen Umfang Zugriff auf die Daten haben. Insbesondere im schulischen Bereich ist darauf zu achten, dass Datenverarbeitung nur in dem Rahmen zulässig ist, wie das jeweilige Landes(schul)gesetz dies erlaubt.[59] Bei der Implementierung der einzelnen Funktionalitäten der Plattform ist dies zu beachten. Weiterhin sind Löschkonzepte zu erstellen, um nicht mehr benötigte Daten rechtskonform löschen zu können. Es ist auf datenschutzfreundliche Voreinstellungen zu achten. Diese Pflicht ergibt sich bereits aus Art. 25 DSGVO. Schließlich ist die Anpassungsfähigkeit des Systems sicherzustellen, um auf rechtliche Änderungen reagieren zu

57 S. zu Vorschlägen für eine Fortentwicklung der DSGVO bezüglich des Datenschutzes von Kindern Roßnagel 2020a: 88 ff.

58 Hierfür bietet sich der Rückgriff auf das Standard-Datenschutzmodell der Datenschutzkonferenz an: DSK 2020.

59 DSK 2018: 5.

können. Für eine ausführliche Darstellung dieser und weiterer Gestaltungsvorschläge sei auf die Hinweise der Datenschutzkonferenz verwiesen.[60]

Literatur

Art.-29-Datenschutzgruppe (2018): *Guidelines on consent*. Working Paper 259 rev.01. Online verfügbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (Abfrage am: 07.10.2020).

Buchner, Benedikt / Petri, Thomas (2018): *Art. 6 DSGVO*. In: Kühling, Jürgen / Buchner, Benedikt (Hg.): DS-GVO/BDSG, Kommentar (2). München: C.H.Beck.

Buchner, Benedikt / Kühling, Jürgen (2018): *Art. 4 Nr. 11 DSGVO* sowie *Art. 4 Nr. 25 DSGVO* sowie *Art. 7 DSGVO* sowie *Art. 8 DSGVO*. In: Kühling, Jürgen / Buchner, Benedikt (Hg.): DS-GVO/BDSG, Kommentar (2). München: C.H.Beck.

Datenschutzkonferenz (DSK) (2018): *Orientierungshilfe der Datenschutzbehörden für Online-Lernplattformen im Schulunterricht*. Online verfügbar unter: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html (Abfrage am: 07.10.2020).

Datenschutzkonferenz (DSK) (2020): *Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Version 2.0b*. Online verfügbar unter: https://www.datenschutzzentrum.de/sdm/ (Abfrage am: 07.10.2020).

Ernst, Stefan (2018): *Art. 4 DSGVO*. In: Paal, Boris / Pauly, Daniel (Hg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar (2). München: C.H.Beck.

Frenzel, Eike Michael (2018): *Art. 8 DSGVO*. In: Paal, Boris / Pauly, Daniel (Hg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar (2). München: C.H.Beck.

Gierschmann, Sibylle (2018): *Gestaltungsmöglichkeiten bei Verwendung von personenbezogenen Daten in der Werbung*. In: MultiMedia und Recht (1), S. 7-12.

Heberlein, Johanna (2018): *Art. 6 DSGVO*. In: Ehmann, Eugen / Selmayr, Martin (Hg.): DS-GVO, Kommentar (2). München: C.H.Beck.

Heckmann, Dirk / Paschke, Anne (2018): *Art. 7 DSGVO* sowie *Art. 8 DSGVO*. In: Ehmann, Eugen / Selmayr, Martin (Hg.): DS-GVO, Kommentar (2). München: C.H.Beck.

Helfrich, Marcus (2020): *Art. 21 DSGVO*. In: Sydow, Gernot (Hg.): Europäische Datenschutzgrundverordnung (2). Baden-Baden: Nomos.

60 DSK 2018: 12 ff.

Hornung, Gerrit (2015): *Datenschutzrechtliche Aspekte der Social Media*. In: Hornung, Gerrit / Müller-Terpitz, Ralf (Hg.): Rechtshandbuch Social Media. Berlin, Heidelberg: Springer, S. 79-130.

Ingold, Albert (2020): *Art. 7 DSGVO*. In: Sydow, Gernot (Hg.): Europäische Datenschutzgrundverordnung (2). Baden-Baden: Nomos.

Jandt, Silke / Schaar, Peter, / Schulz, Wolfgang (2013): *§ 13 TMG*. In: Roßnagel, Alexander (Hg.): Recht der Telemediendienste. München: C.H.Beck.

Kampert, David (2020): *Art. 8 DSGVO*. In: Sydow, Gernot (Hg.): Europäische Datenschutzgrundverordnung (2). Baden-Baden: Nomos.

Karg, Moritz / Fahl, Constantin (2011): *Rechtsgrundlagen für den Datenschutz in sozialen Netzwerken*. In: Kommunikation & Recht (7/8), S. 453-458.

Karg, Moritz / Thomsen, Sven (2012): *Tracking und Analyse durch Facebook*. In: Datenschutz und Datensicherheit 36 (10), S. 729-736.

Klement, Jan Henrik (2019): *Art. 8 DSGVO*. In: Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hg.): Datenschutzrecht, Kommentar. Baden-Baden: Nomos.

Nebel, Maxi (2018): *Erlaubnis zur Datenverarbeitung (§ 3)*. In: Roßnagel, Alexander (Hg.): Das neue Datenschutzrecht, Nomos: Baden-Baden, S. 104-115.

Nebel, Maxi (2020): Persönlichkeitsschutz in Social Networks, Technische Unterstützung eines grundrechtskonformen Angebots von Social Networks. Wiesbaden: Springer.

Profit (2018): *§ 83 HessSchulG Erhebung und Verarbeitung personenbezogener Daten.* In: Köller / Achilles: Hessisches Schulgesetz. Wiesbaden: Kommunal- und Schulverlag.

Ratzsch, Jörg (2019): Studie: Viele Kinder nutzen Youtube zum Lernen für die Schule. Online verfügbar unter: https://heise.de/-4438484 (Abfrage am: 07.10.2020).

Roßnagel, Alexander (2019): *Art. 2 DSGVO* sowie *Art. 6 Abs. 1 DSGVO* sowie *Art 6 Abs. 2 DSGVO*. In: Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hg.): Datenschutzrecht, Kommentar. Baden-Baden: Nomos.

Roßnagel, Alexander / Geminn, Christian / Johannes, Paul C. (2019): *Datenschutz-Folgenabschätzung im Zuge der Gesetzgebung*. In: Zeitschrift für Datenschutz (10), S. 435-440.

Roßnagel, Alexander (2020a): *Der Datenschutz von Kindern in der DS-GVO*. In: Zeitschrift für Datenschutz (2), S. 88-92.

Roßnagel, Alexander (2020b): *Datenschutz im E-Learning.* In: Zeitschrift für Datenschutz (6), S. 296-302.

Sassenberg, Elke (2019): *Datenschutz in Schule und Schulverwaltung (§ 24)*. In: Specht, Louisa / Mantz, Reto (Hg.): Handbuch Europäisches und deutsches Datenschutzrecht. München: C.H.Beck, S. 672-698.

Schaller, Fabian: *Datenschutz im öffentlichen Bereich (§ 7)*. In: Roßnagel, Alexander (Hg.): Das neue Datenschutzrecht. Baden-Baden: Nomos, S. 270-281.

Schantz, Peter (2019): *Art. 6 Abs. 1 DSGVO*. In: Simitis, Spiros / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hg.): Datenschutzrecht, Kommentar. Baden-Baden: Nomos.

Schantz, Peter / Wolff, Heinrich A. (2017): *Das neue Datenschutzrecht*. München: C.H.Beck.

Schulz, Sebastian (2018): *Art. 6 DSGVO* sowie *Art. 8 DSGVO* sowie *Art. 21 DSGVO*. In: Gola, Peter (Hg.): Datenschutz-Grundverordnung, Kommentar. 2. Aufl. München: C.H.Beck.

Data and privacy literacy: the role of the school in educating children in a datafied society[1]

Sonia Livingstone, Mariya Stoilova und Rishita Nandagiri

Abstract

What should children be taught about their online privacy and the uses that others may make of their personal data, and why? This chapter reports on a systematic mapping of the available evidence followed by child-centered, qualitative research interviews with children aged 11-16 years old in the UK. The aim was to discover what children of different ages already know about privacy and data online, to ask them what they want to know, and then to reflect on the educational challenges posed by the answers. For its conceptual framing, the chapter distinguishes three contexts for data use online – interpersonal, institutional (including the school) and commercial. Since these are increasingly interconnected, it is argued that children should be taught about each, to gain a critical understanding of the data ecology and business models which are driving the datafication of society and, thereby, childhood. Finally, it is proposed that, if schools could themselves demonstrate best practice in data processing – explaining school policy, practice, and opportunities for redress to their students – this might prove a more effective means of improving children's understanding than via the taught curriculum.

Introduction

Of the many calls upon educators, one of the most recent is that children should be taught about their online privacy and data, given today's increasingly datafied society (Lupton/Williamson 2017: 780-794). The transforma-

1 **Acknowledgments:**
This research was funded by the UK's Information Commissioner's Office. An earlier version of this chapter was originally published in Frau-Meigs, D. et al (Eds.), *Handbook on Media Education Research*. London: Routledge.

tion of ever more human activities into data means that managing one's privacy is becoming highly complex, and ever more part of institutional practices of state control and evolving business models. People's online data selves (or 'digital footprints') are increasingly the means by which their options become determined for them by others, according to the interests of those others rather than, or at best, as well as the interests of the data subject (Zuboff 2019). Consequently, it is important to recognize the interdependence of digital media literacy (what children can and should be taught about the digital environment) and digital design and regulation (how the digital environment does, could and should address children, use their data or offer redress).

This poses a new challenge for schools already struggling to address e-safety, online identity and reputation, coding, information navigation, misinformation and "fake news," digital dimensions of sex and relationships education, screen time and mindfulness, and more, all under the loose rubric of "media literacy" (Bulger/Davison 2018). How can children be educated about commercial and state uses of their data, when this involves complexities of data protection and privacy regulation that most adults – including parents and teachers – hardly understand? Can such digital literacy education, even if implemented, manage sufficiently to empower children when companies obscure how they operate with children's data, conceal children's privacy rights, or fail to anticipate their needs in designing services? The risk is that the result may disempower children further by confusing them with quickly out-of-date complexities or inculcating the dystopian message that they can only lose control of their online privacy if they wish to participate fully in the digital age.

This chapter draws on the project, "Children's data and privacy online: growing up in a digital age" (Livingstone/Stoilova/Nandagiri 2019a), funded by the UK's data protection authority. This takes a child-centred approach, prioritising children's voices, experiences and rights within a wider framework of evidence-based policy development. The research began with a systematic evidence mapping of current research (Livingstone/Stoilova/Nandagiri 2019a), followed by 28 workshop-style focus group discussions with children of secondary school age (11-16 years old) and, separately, interviews with parents and educators (for a detailed description of the methodology see Livingstone/Stoilova/Nandagiri 2019b). Both the evidence mapping and the empirical work have informed this chapter. Real-life scenarios and exemplar digital experiences were used to facilitate the discussions and to ensure that children were engaged in deliberating on the opportunities, risks, and practical dilemmas posed by the digital environment. Guided throughout by an international expert advisory board,

and working with children themselves, the project concluded by creating an online, open-access toolkit to support and promote children's data and privacy literacies.

The analysis starts by asking: what do children know, what do they want to know and what do they need to know about their privacy and data online? Then, given their professed knowledge gaps, the research considers the role of the school, asking what the teachers know and think they should teach, and considering also how the school as an institution, through its own policies and procedures, models a particular approach to children's data and privacy; this latter tends to undercut the curricular challenge by modelling an opaque approach to data protection. Finally, after hearing from students and parents what they expect of the school and from teachers on their struggles to grasp the data and privacy literacy challenge facing them, the chapter concludes by asking whether the responsibility for children's privacy be better apportioned between school, home, business, regulators and children themselves.

1. *Conceptualizing data and privacy literacy*

Children's digital literacy plays an important part in how children understand, manage and safeguard their privacy. Privacy involves considerably more than simply providing, guarding or withholding one's personal information. Drawing on Nissenbaum's (2004: 119–157) notion of privacy as *contextual integrity*, and recognizing that contexts emerge from the mutual interaction between people and their environments, privacy online is conceptualized in this chapter as depending, on the one hand, on the design, infrastructure and political economy of the digital environment and, on the other, on users' agency and knowledge (as data subjects, individually and collectively) regarding what they wish or judge appropriate to share within specific digital contexts. While many digital contexts can be identified, a primary distinction can be made among:

(i) interpersonal privacy (how my 'data self' is created, accessed and multiplied via my online social connections);
(ii) institutional privacy (how public agencies like government, educational and health institutions gather and handle data about me);
(iii) commercial privacy (how my personal data is harvested and used for business and marketing purposes).

Online, interactions are encoded and mediated by data, and users are learning to recognize how their social interactions are transformed into da-

ta in ways that may or may not respect their agency. The digital environment is developing too – increasingly structuring, managing and potentially exploiting users' data in ways that generally lack transparency and accountability. Three types of data can be distinguished when considering what children need to understand about their online privacy: data contributed by individuals about themselves or others (data given); the data left, mostly unknowingly, and captured via data-tracking technologies (data traces); and data derived from analyzing data given, data traces, and possibly other sources (inferred data, also referred to as 'profiling') (typology adapted from van der Hof 2016: 409-45, building on Goffman 1971).

Given the importance of these distinctions and complexities, we argue that a functional skills-based approach to the digital interface (learning practically how to navigate terms and conditions, age requirements, privacy settings, etc.) is necessary but not sufficient to protect and empower children in a datafied society. Children's autonomy and dignity as actors in the world depends on both their freedom to engage and their freedom from undue persuasion or influence. To exercise their rights as agents and citizens in a digital world, children need a deeper, critical understanding of both the digital environment (including its business models, uses of data and algorithms, forms of redress, commercial interests, systems of trust and governance) and, indeed, of social relations and interactions. Arguably this would traditionally fall within media education, but it sits uncomfortably with standard definitions focused on mediated forms of communication – such as the ability to access, analyze, evaluate and create messages across a variety of contexts (Aufderheide 1993) – because what is critical in relation to data and privacy is an understanding of the digital environment behind the interface of the screen. It is also more demanding than many media literacy curricula (McDougall/Livingstone/Sefton-Green/Fraser 2014, European Audiovisual Observatory 2016).

This may seem daunting to teachers, and understandably so, given the technological complexities, rapid pace of innovation, regulatory challenges and relative unaccountability of digital businesses, not to mention the crowded curriculum, limited opportunities for in-service training and many other pressures on teachers (National Literacy Trust 2018). However, critical approaches to media education have long urged that children are taught not only about mediated representations and influences but also about the production context and political economy of the media and the consequences for power, profit and possibilities of resistance (Kellner/Share 2007: 59-69, Hartley 2011, Buckingham 2015: 21-35). In the light of today's growing digital challenges, one might wish that this task had been begun by schools earlier.

2. Children's understanding of data and privacy online

Children's capacity to manage their privacy in the digital environment depends on many factors. Educators, regulators and parents are particularly keen to know when and how data and privacy online should be addressed – in the curriculum, in framing regulation - for children of different ages (Livingstone 2018: 18-23, Livingstone/Ólafsson 2018, Livingstone/Blum-Ross/Zhang 2018). While cautioning that most research focuses on adolescents to the exclusion of younger children, and that differences within as well as across age groups can be substantial, findings for children aged 5-7, 8-11 and 12-17 years old were grouped together based on the age groups used most often in the available research.

Table 1 provides a summary of the results of the systematic evidence mapping of recent empirical research on children's understanding of their privacy online (Livingstone/Stoilova/Nandagiri 2019a). It suggests that children give considerable thought to interpersonal privacy, although they may struggle with how to negotiate sharing or withholding personal information in networked contexts which demand they trade privacy for opportunities for participation, self-expression and belonging (Micheti/Burkell/Steeves 2010: 130-43, Hasselbalch Lapenta/Jørgensen 2015).

By contrast, children are generally less aware of how institutions or commerce operate in the digital environment, and so they may reveal personal data without recognizing the potential for data breaches on the one hand or exploitative practices by businesses on the other. It can be noted, however, that most research considers only interpersonal contexts, whereas this research had to combine the limited findings from institutional and commercial contexts for privacy, notwithstanding the important difference between organizations acting in the public and private interest (see table 1 for summary of answers).

Table 1: Children's developing data and privacy literacy

	Interpersonal privacy	Institutional and commercial privacy
5- to 7-year-olds	• A developing sense of ownership, fairness and independence • Learning about rules but may not follow, and don't get consequences • Use digital devices confidently, for a narrow range of activities • Getting the idea of secrets, know how to hide, but tend to regard tracking/monitoring by a trusted adult as helpful	• Limited evidence exists on understanding of the digital world • Low risk awareness (focus on device damage or personal upset) • Few strategies (can close the app, call on a parent for help) • Broadly trusting
8- to 11-year-olds	• Starting to understand risks of sharing but generally trusting • Privacy management means rules not internalized behavior • Still see monitoring by a parent or other trusted adult positively, to ensure their safety • Privacy risks linked to 'stranger danger' and interpersonal harms • Struggle to identify risks or distinguish what applies offline/online	• Still little research available • Gaps in ability to decide about trustworthiness or identify adverts • Gaps in understanding privacy terms and conditions • Interactive learning shown to improve awareness and transfer to practice
12- to 17-year-olds	• Online as 'personal space' for expression, socializing, learning • Concerned about parental monitoring yet broad trust in parental and school restrictions • Aware of/attend to privacy risks, but mainly seen as interpersonal • Weigh risks and opportunities, but decisions influenced by desire for immediate benefits	• Privacy tactics focus on online identity management not data flows (seeing data as static and fragmented) • Aware of 'data traces' (e.g., ads) and device tracking (e.g., location) but less personally concerned or aware of future consequences • Willing to reflect and learn but do so retrospectively • Media literacy education is most effective if adolescents can use their knowledge to make meaningful decisions in practice

The focus groups with children aged 11 to 12, 13 to 14 and 15 to 16 years old confirmed this finding. The research began with an open discussion of privacy, and how children use and think about the internet. It then sought to focus their discussion on the privacy and data practices of the commercial apps and services they use and, later, on the practices of their school and other institutions such as health or transport services. But over and again, children responded in interpersonal terms, even when institutional or commercial practices were really at issue (Stoilova/Livingstone/Nandagiri 2020). They discussed the people running Instagram or Snapchat, and their teachers, notwithstanding that these are organizational relationships. This may partly be due to their greater familiarity with interpersonal contexts, and the ways in which privacy in that domain is managed and valued. It may also be because, in interpersonal contexts, privacy is largely mediated by the personal information people choose to reveal to the those they know or meet, involving practices with which children are familiar.

Yet this is not, by and large, how privacy works online, especially in relation to institutions and commerce, where the relation between user agency and digital design can be very different, mediated by data protection regulation, on the one hand, and the data economy or business of "datafication," on the other hand (O'Hara 2016: 86-91, Lupton/Williamson 2017: 780-794).

3. *What children want to know about data and privacy online*

Towards the end of each session, the children were asked what they wanted to know, and what they thought companies should do differently (see Table 2 for summary of answers). Their primary concern, irrespective of age – and admittedly after a lively discussion of their data and privacy online – is: who has got their data, what is done with it, and why. Few had a good understanding of how data profiling is conducted or the data economy of which profiling is a part. When the researchers explained something of this to them, many were both puzzled and outraged – "it's none of their business" was a common response to learning about the widespread collection of their personal data although, ironically, it is precisely the companies' business model (Zuboff 2019).

The tabulated responses provide some interesting hints about how children of different ages approach the problem – younger children are concerned with the privacy options provided by apps, for instance, while older children are beginning to think also about data governance. Also, younger

children think of personal information in terms of phone numbers and other data given, while older children are more aware of data taken (via facial recognition technology, for instance), and of different kinds of data (sensitive, biometric, profiled). The youngest group wants more protections while those in the middle age group are "naughtier" (asking about the dark web, hacking, etc.). From the focus group discussions, a growing awareness of all three data types seemed roughly linked to age, with the younger children focusing most on data given, and the teenagers increasingly aware of data taken and inferred– though all had some awareness of profiling, because all had had the experience of searching for something and later receiving related advertising.

More striking, however, was that across the age range, a strong assumption of fairness pervaded what the children said: companies *should* explain better, improve services, be age-appropriate, provide options that users want, respond to users' concerns, and treat users well. They did not really question whether it is in companies' interest to act in this way; if practices are judged by children as unfair, then something should be done. Similarly, if an organization is trusted (whether a big brand or their school) then it was assumed that they would treat children's data fairly. Here the logic of interpersonal contexts is at work, with which children are familiar, being extended to the institutional and, especially, commercial contexts, with which they often have little experience (Stoilova/Livingstone/Nandagiri 2020).

Indeed, since interpersonal lives are now often conducted in proprietary environments, each interaction has a double significance – sharing an image with a friend on Instagram means also sharing that image with Instagram. Thus, the interpersonal and commercial contexts – traditionally so different, become blurred, confusing not only children but also the adults who try to guide them. Confusions arose from the use of terms from interpersonal or everyday contexts being used for technical processes – how can companies still know all about you if you've put your "privacy" settings on or dissemble your name, age or gender; why aren't things you "deleted" truly deleted; why are companies who have no personal relation with you so interested in your 'personal' life? The tendency to extend interpersonal expectations into commercial contexts was also evident when things go wrong – children express frustrations about companies proving unresponsive to their reports or complaints; they would expect family or friends to respond, after all, so why not the companies?

Table 2: Children's views of how their data and privacy online should be addressed: what they want to know, and what they think should be changed (entries paraphrased and summarized)

	What children want to know about their data and privacy online	What children think companies should do differently
All ages	• Who has got my personal data, how long do they keep it and what do they do with it • Why do they collect, share and sell my information • Where does deleted data go, is it really gone	• Make deleted apps or information permanently gone • Provide more and better privacy, security and safety options • Make accounts private, turn off geo-location and disable cameras by default • Don't share my data with other sites or services • Better responsiveness to user concerns and complaints • Make Terms and Conditions understandable, short and visual
11-to 12-year olds	• Why do apps need to know your phone number • Who controls the websites • Who can find out about my information • Why do they set age restrictions so high (e.g. WhatsApp) • Why don't companies remove scamming sites • Why is reporting stuff so hard • Why do they make mistakes about who you are	• Let under 13s use social media but keep their account private • Make online content more appropriate for our age • Take down hostile content (e.g. fat shaming)

	What children want to know about their data and privacy online	What children think companies should do differently
13-to 14- year olds	• Who can see what I search • Can people see me through my camera or hear my voice • What social media sites do with your information • What happens when you get hacked • What happens to your data when you die • What is the dark web • What do they do with your face when you use facial recognition	• Allow paid-for but private apps • Not sell our data • Not show me what I'm not interested in • Make it easier to erase your account
15-to 16-year olds	• Where is data kept, how does it travel across the internet, and what is shared with other companies • Why do they need to know so much about me (e.g. my gender) • Is sensitive data shared	• Leave me alone • Keep biometric data safely • Delete our data after a certain time (e.g. two years) • Only ask for information when relevant • Allow you to opt out of data collection • Better checks on age restrictions • Explain to you what information they have about you

4. The role of the school in teaching children about data and privacy online

Institutional practices related to privacy (e.g., digital learning platforms, fingerprint access to meals or buildings, profiling of attendance and performance) are often presented as "revolutionary" and transformational to parents (Williamson 2017: 59-82). But one study in American schools found that commercial monitoring software, instituted to tackle bullying, monitored public social media posts made by students aged 13+ when both on and also off campus, with reports flagged to school administrators (Shade/Singh 2016: 1-12). Not only does this mean that efforts professing to protect children can both infringe their privacy and position them as perpetrators, but it is often unclear to schools whether the businesses providing educational services also cross-reference their data with other records or information available, creating an assemblage of surveillance which may exceed what parents or children believe they have consented to and which may have adverse consequence they do not anticipate.

Several parents and teachers in the research project expressed concern about this reliance on commercial business models and for-profit platforms for educational purposes, echoing the concerns of critical scholars regarding the risk to and exploitation of student data (Shade/Singh 2016: 1-12, Bulger/McCormick/Pitcan 2017, Lievens/Livingstone/McLaughlin/O'Neill /Verdoodt 2018: 1-27). A father mentioned parent concerns over school use of children's thumbprints (to pay for lunch), noting ruefully that the school implemented this use of biometric data notwithstanding:

> Well, the thing is information is collected everywhere even if you're not aware it's being collected, isn't it, nowadays? So, when a child's at school, I know the school has those biometric [thumb prints] ... There was a bit of hoo-ha about it, but it still went ahead. So that information's collected, isn't it? Someone's got the thumb print somewhere stored.

Such concerns are motivated – perhaps also reinforced– by the increasing sponsorship of schools by big companies (in the UK, the pressing decision is, as it is colloquially expressed, whether to become a "Google" or a "Microsoft" school).

In general, however, the children, parents and teachers interviewed were very confident of their interpersonal privacy management – asking permission before taking or posting photos of the students, for instance; and fairly confident of their institutional privacy management (describing the GDPR (General Data Protection Regulation) training and procedures, assuring us of the school's trustworthy approach to storing sensitive data

on special educational needs or family problems or student grades). They were also excited about the involvement in education of big companies, seeing this as a way of preparing for the "digital future," hoping to benefit from the latest opportunities rather than being stuck behind the times.

But their accounts faltered when they were asked about commercial privacy management – as one parent noted, when discussing the tracking that might occur when iPads are provided to students, "our kids are the guinea pig generation." Parents and teachers seemed uncertain, for instance, about the use of student data for tracking and learning analytics by Capita SIMS or ClassDojo or Show My Homework or cloud storage services or any of the commonly used software – at first telling the researchers confidently that student data never leaves the school, then realizing they might, then looking worried as they have no answer to questions about third party sharing ("that's not at our level," one told the researchers). One school's "technical learning officer" admitted that he was not aware of what kind of data are being gathered about the children or how identifiable they are but expects that data are both detailed and shared with the council, researchers and companies (in this case, Google). Children in his school are, as he put it, "tracked all the time," and he was optimistic that the school will gain better intelligence it can use to the benefit of the students. More commonly, a sense of fatalism regarding the data economy pervaded the interviews, with the exception of one business studies teacher who pushes back robustly that it is how the economy works:

> I'm just looking at it from a business point of view. I don't see why that is a concern […] It just drives the economy forward. We've been doing this for 50 years in a sense of after cartoons, there's toy adverts… So it's not. No real difference. It's just a clever, more advanced way of doing it.

The recent and widespread success of introducing e-safety into British schools, however, combined with the tendency to conceive of privacy primarily in interpersonal terms, means that children – and, indeed, parents and teachers, are tempted to think that privacy and data literacy could be incorporated within existing lessons about personal safety online. Ironically, it is not until one recognizes the existence and complexity of the political economy and commercial infrastructure of the emerging digital environment that the need for a critical knowledge of it is fully appreciated. Again, this is the case with most curriculum subjects, and why a pedagogic solution which goes beyond what children may initially ask for is needed.

The findings suggest that such a solution will be welcome. In focus groups, children were keen to discuss the tech news they hear through the

mass media – often the scandals involving the major platforms, the latest data breach or tragic suicides linked to social media, but also news about emerging innovations – smart devices, robots, and developments in artificial intelligence. The message was clear: they consider themselves the generation that will live their lives in and through technology, so they want to understand it. But their enthusiasm for discussing the latest tech news, sharing stories of what went wrong or figuring out for themselves how things work is often a world away from how they talk about lessons. In a rapidly changing digital environment children often feel that the curriculum is lagging behind and educational interventions at school happen mainly when something goes wrong. Much less involved in using the apps and devices, parents and teachers have limited knowledge, at best, and children often prefer to learn by trial and error on their own.

Parents, however, both trust and rely on the school to teach their children data and privacy literacy, not least because their own knowledge is hugely variable. One mother had been hacked, found it terrifying, and had relatives engaged in an online privacy-related court case; yet when asked how the school protected sensitive data regarding her autistic son, she said "I don't know" and "I haven't really thought about it." A father who worked in the digital sector knew so much that, after regaling us with all the risks – cybercrime, fraud, identity theft, etc. – he concluded that there is nothing really to be done, "that's just the nature of the internet" and it's a scary world. Another father, who had "worked in the internet since it started," wants data profiling and discrimination taught in citizenship classes as it would be unfair and unequal to demand that parents understand such things:

> I think that should be part of citizenship, that they're learning in schools about how all of this impacts. Because, I don't know much about profiling, to be honest.

Certainly, some parents know very little: one mother was unaware of privacy-protecting tactics such as incognito browsing or deleting one's search history but had a daughter with good digital privacy skills.

Existing research shows that, while most teachers (99%) believe they have the greatest responsibility for helping children develop online literacy skills, more than half (54%) think that the national curriculum does not teach children the digital literacy skills they need, and over a third (35%) feel that the digital literacy skills taught in schools are not transferable to the 'real world' (National Literacy Trust 2018). The teachers interviewed were ambivalent about teaching data and privacy literacy – they felt they keep telling the students to be careful and sensible but found repeating the

same message over and again ineffective. They are keen that parents should take more responsibility to bring up their children to be aware, critical and cautious about the digital environment, and that secondary school (in the UK, from 11 years old) is already late to begin educating tomorrow's "digital citizens."

At the same time, teachers are critical of parents – seeing them as too disengaged, or unaware, or panicky. They also worry about being overwhelmed by parental demands when they use messaging systems to communicate with parents, while children told us they distrust this form of tracking or that their parents are reluctant to download the apps in the first place. As regards social media use, teachers tended to be critical of the children also, disapproving of their fascination with selfies, susceptibility to online persuasion and peer pressure, dishonesty in lying about their age or setting up fake profiles, foolishness for posting indecent images, naivety about the future consequences of their actions, and overconfidence in thinking they know it all.

Still, both parents and teachers recognized that children need to discover how to behave online, to be allowed the freedom to make mistakes and learn from them, and not to be overburdened by expectations to understand a very complicated, and generally not child-friendly, digital environment. Parents and teachers trusted the children to know what they are doing and to seek help when they need it and wanted to create a learning environment where children are active and independent agents.

4. Conclusion

The main purpose of this chapter has been to identify what children understand about their data and privacy online, in order to frame the educational challenge for teaching data and privacy literacy, whether within the media education curriculum or elsewhere – for instance, in the computing or citizenship curricula. From the systematic evidence mapping and primary research with children, parents and teachers, it can be argued first, that it is not enough for children to gain functional skills to consider what personal data they provide, manage their privacy settings or respond to data protection options provided by online services. To enact their rights as agents and citizens in a complex datafied society, they also need some measure of critical understanding of the networked data economy which is fueled not only by data given but also data traces and inferred or profiled data.

Improving children's data and privacy literacy is a demanding media education task in its own right. It is made more complex by the fact that children are already familiar with interpersonal privacy contexts, with younger children especially tending to assume that values and practices appropriate to interpersonal relations also apply in institutional and commercial contexts, even though this is often inappropriate and results in misunderstandings. However, the workshops with children revealed that they are keen to deepen their understanding of data and privacy online, wanting to know who has their data, what they do with it and why. None of these questions can be answered by simple answers, awareness-raising campaigns or other quick fixes. Add to this the complexity involved in answering the other questions children ask, and it is clear that an educational strategy is needed. In other words, children implicitly recognize this as an expert domain which they should be taught something about.

Although many are tempted to assimilate data and privacy literacy to the now-familiar teaching of e-safety, the knowledge required, and the implications for the curriculum, are distinctive and, therefore, best addressed separately. However, the very complexity of today's data economy places limits on what teachers can be trained and resourced to teach. Nor can either parents or teachers be burdened with ensuring children understand a digital environment which governments, regulators and businesses are all struggling to manage.

A second purpose of this chapter, therefore, has been to call attention to the complementary obligations and responsibilities of others, especially businesses and regulators. Children not only want to know more but they want changes from the digital environment and, reasonably so, whether or not such changes are feasible or forthcoming. Media literacy is always co-dependent on the nature of the media environment – if the latter is opaque or "illegible" (Livingstone 2008: 51-62), the task of media educators is made all the more difficult. Conversely, the more the media environment adjusts to meet the needs and rights of its users, the more media education can focus on empowerment rather than harm mitigation.

By conceptualizing privacy in contextual terms, this argument can be extended directly to the present case. In short, to the extent that the commercial digital environment is opaque and unaccountable or even exploitative in its treatment of users' data (Norwegian Consumer Council 2018), the more knowledge and support users will require to maintain the privacy necessary to human agency and dignity in the digital age. Thus, at a policy level, the provision of digital literacy in schools must be considered hand in hand with questions of data protection regulation.

In the process of researching this question through fieldwork in schools highlights the unique position of the school in this regard, being an institution tasked both with educating its students and managing their personal data. Just as with citizenship education, in relation to data protection the school is not only the site of education but also a microcosm of the wider society: if children are not treated as independent rights-holders at school, the teachers will lack credibility in teaching them about democracy (Frau-Meigs/Hibbard 2016). Similarly, unless schools are transparent and accountable in their processing of student data, they can hardly teach data and privacy literacy to those same students. Put positively, it is open to schools as institutions with considerable data protection responsibilities to become beacons of good practice, thereby demonstrating to children and parents how their privacy rights can be realized in the digital environment and influencing their expectations for other, usually commercial contexts. This would surely ease the increasingly important task of providing data and privacy literacy education for children.

References

Aufderheide, Patricia (1993): *Media Literacy: A Report of the National Leadership Conference on Media Literacy*. Aspen Institute, Communication and Society Program. Retrieved from: https://files.eric.ed.gov/fulltext/ED365294.pdf (last accessed on October 1, 2020).

Buckingham, David (2015): *Defining Digital Literacy – What do young people need to know about digital media?* In: Nordic Journal of Digital Literacy 10, S. 21–35.

Bulger, Monica / McCormick, Patrick / Pitcan, Mikaela (2017): *The Legacy of inBloom*. Retrieved from: https://datasociety.net/pubs/ecl/InBloom_feb_2017.pdf (October 1, 2020).

Bulger, Monica / Davison, Patrick (2018): *The Promises, Challenges, and Futures of Media Literacy*. Retrieved from: https://datasociety.net/pubs/oh/DataAndSociety_Media_Literacy_2018.pdf (October 1, 2020).

European Audiovisual Observatory (2016): *Mapping of Media Literacy Practices and Actions in EU-28*. Strasbourg: European Audiovisual Observatory. Retrieved from: https://rm.coe.int/0900001680783500 (October 1, 2020).

Frau-Meigs, Divina / Hibbard, Lee (2016): *Education 3.0 and Internet Governance: A new global alliance for children and young people's sustainable digital development*. London: Chatham House. Retrieved from: https://www.cigionline.org/sites/default/files/gcig_no27web_0.pdf (October 1, 2020).

Goffman, Erving (1971): *The Presentation of Self in Everyday Life*. Harmondsworth: Penguin. Retrieved from: https://monoskop.org/images/1/19/Goffman_Erving_The_Presentation_of_Self_in_Everyday_Life.pdf (October 1, 2020).

Hartley, John (2011): *The Uses of Digital Literacy*. New Jersey: Rutgers.

Hasselbalch Lapenta, Gry / Jørgensen, Rikke Frank (2015): *Youth, Privacy and Online Media: Framing the right to privacy in public policy-making*. In: First Monday 20(3). Retrieved from: https://journals.uic.edu/ojs/index.php/fm/article/view/5568/4373 (October 1, 2020).

Kellner, Douglas / Share, Jeff (2007): *Critical Media Literacy Is Not an Option*. In: Learning Inquiry 1(1), S. 59-69.

Lievens, Eva / Livingstone, Sonia / McLaughlin, Sharon / O'Neill, Brian / Verdoodt, Valerie (2018): *Children's Rights and Digital Technologies*. In: U. Kilkelly / T. Liefaard (Hg.): International Human Rights of Children. Singapore: Springer Singapore, S. 1-27.

Livingstone, Sonia (2008): *Engaging with Media – A matter of literacy?* In: Communication, Culture & Critique 1(1), S. 51-62.

Livingstone, Sonia (2018): *Children: a special case for privacy?* In: Intermedia 46(2), S. 18-23. Retrieved from: http://eprints.lse.ac.uk/89706/ (October 1, 2020).

Livingstone, Sonia / Ólafsson, Kjartan (2018): *When do Parents Think Their Child is Ready to Use the Internet Independently?* In: Department of Media and Communications, The London School of Economics and Political Science: Parenting for a Digital Future: Survey Report 2., Retrieved from: http://eprints.lse.ac.uk/87953/ (October 1, 2020).

Lupton, Deborah / Williamson, Ben (2017): *The datafied child: The dataveillance of children and implications for their rights.* In: New Media & Society 19(5), S. 780-794.

Livingstone, Sonia / Blum-Ross, Alicia / Zhang, Dongmiao (2018): *What Do Parents Think, and Do, about Their Children's Online Privacy?* In: Department of Media and Communications, The London School of Economics and Political Science: Parenting for a Digital Future: Survey Report 3. Retrieved from: http://eprints.lse.ac.uk/87954/ (October 1, 2020).

Livingstone, Sonia / Stoilova, Mariya / Nandagiri, Rishita (2019a): *Children's Data and Privacy Online: Growing up in a digital age. An evidence review*. London: London School of Economics and Political Science. Retrieved from: http://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf (October 1, 2020).

Livingstone, Sonia / Stoilova, Mariya / Nandagiri, Rishita (2019b): *Talking to Children about Data and Privacy Online: Research methodology*. London: London School of Economics and Political Science. Retrieved from: http://eprints.lse.ac.uk/101284/ (October 1, 2020).

McDougall, Julian / Livingstone, Sonia / Sefton-Green, Julian / Fraser, Sharon P (2014): *Media and Information Literacy Policies in the UK*. In: Report for the COST (Transforming Audiences, Transforming Societies) initiative, Mapping Media Education Policies. Retrieved from: http://eprints.lse.ac.uk/57103/ (October 1, 2020).

Micheti, Anna / Burkell, Jacquelyn / Steeves, Valerie (2010): *Fixing Broken Doors: Strategies for drafting privacy policies young people can understand*. In: Bulletin of Science, Technology and Society 30(2), S. 130-43.

National Literacy Trust (2018): *Fake news and critical literacy: The final report of the Commission on Fake News and the teaching of critical literacy in schools.* London: National Literacy Trust. Retrieved from: https://literacytrust.org.uk/research-services/research-reports/fake-news-and-critical-literacy-final-report/ (October 1, 2020).

Nissenbaum, Helen (2004): *Privacy as contextual integrity*. In: Washington Law Review 79, S. 119–157.

Norwegian Consumer Council (2018): *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Oslo: Forbrukerrådet. Retrieved from: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (October 1, 2020).

O'Hara, Kieron (2016): *The Seven Veils of Privacy*. In: IEEE Internet Computing 20, S. 86-91.

Shade, Leslie Regan / Singh, Rianka (2016): *'Honestly, We're Not Spying on Kids': School surveillance of young people's social media.* In: Social Media and Society 2, S. 1-12.

Stoilova, Mariya / Livingstone, Sonia / Nandagiri, Rishita (2020): *Digital by default: children's capacity to understand and manage online data and privacy*. Media and Communication, 8(4), DOI: http://dx.doi.org/10.17645/mac.v8i4.3407.

van der Hof, Simone (2016): *I Agree, or Do I? A rights-based analysis of the law on children's consent in the digital world*. In: Wisconsin International Law Journal 34(2), S. 409-45.

Williamson, Ben (2017): *Learning in the 'Platform Society': Disassembling an educational data assemblage*. In: Research in Education 98(1), S. 59-82.

Zuboff, Shoshana (2019): *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.

Wie kann Schule einen Beitrag zur Entwicklung „digitaler Mündigkeit“ bei Kindern und Jugendlichen leisten? Die Herausforderung der Schule als medienpädagogischer Lernort für Datenschutz und Datensparsamkeit

Reinhold Schulze-Tammena

Abstract

Die Entwicklung digitaler Mündigkeit von Kindern und Jugendlichen findet im Spannungsfeld divergierender pädagogischer Überzeugungen, dynamischer technischer Entwicklungen, manifester wirtschaftlicher Interessen und defensiver politischer Regulierungen statt. Die Mediennutzung von Kindern und Jugendlichen stellt alle unmittelbar Beteiligten vor große Herausforderungen. In oft nervenaufreibenden Aushandlungsprozessen stecken Eltern und Lehrkräfte, Kinder und Jugendliche den Grad der Verfügung über digitale Endgeräte und ihre vielfältigen Anwendungen ab. In diesen Aushandlungen geht es auch immer wieder um eine entwicklungspsychologisch angemessene Verabredung sinnvoller Mediennutzung, die einerseits Freiheit ermöglichen soll und andererseits Grenzen setzen muss, ohne das Recht der Kinder und Jugendlichen auf Privatheit und Datenschutz aus dem Blick zu verlieren. Schule kann die digitale Medienkompetenz von Schülerinnen und Schüler maßgeblich stärken und unter bestimmten Bedingungen einen Beitrag zur „digitalen Mündigkeit“ leisten. Der Medienbildung kommt in Bezug auf das Leben und Lernen in und mit digitalen (Um-)Welten sowie beim Kompetenzaufbau im Bereich Datenschutz und Datensicherheit eine bedeutende Rolle zu.

1. Entwicklung digitaler Mündigkeit bei Kindern und Jugendlichen als Ziel

Die Sozialisationsbedingungen von Kindern und Jugendlichen haben sich mit der umfassenden Verbreitung von Smartphones und ihren vielfältigen Anwendungen stark verändert. Die JIM-Studie 2019 macht deutlich, dass Jugendliche selbstständig über eine große Bandbreite an digitalen Technologien verfügen können. „Smartphone, Computer/Laptop und WLAN

sind mit einigen sozial bedingten Einschränkungen in allen Familien vorhanden“ (JIM 2019: 5). Der persönliche Gerätebesitz von Handy oder Smartphone erreicht 98% (JIM 2019: 7). Das hat erhebliche Auswirkungen auf das Spiel-, Kommunikations- und Lernverhalten von Kindern und Jugendlichen.

Von zentraler Bedeutung ist dabei, dass die Kinder und Jugendlichen bei allen Aktivitäten, die über digitale Technologien vermittelt werden, Daten und Metadaten produzieren, die von öffentlichen und privatwirtschaftlichen Akteuren gesammelt, gespeichert und ausgewertet werden.[1] Der Schutz persönlicher Daten von Kindern und Jugendlichen muss unter diesen Bedingungen wachsender digitaler Selbstständigkeit immer wieder aufs Neue definiert und verteidigt werden.

Dabei gibt es keinen gesellschaftlichen Konsens, was „digitale Mündigkeit“ ist, wie sie schrittweise erworben werden kann und welche Rolle Schule, Elternhaus und die Kinder und Jugendlichen selbst dabei spielen sollen. Denn die Entwicklung digitaler Mündigkeit von Kindern und Jugendlichen findet im Spannungsfeld divergierender pädagogischer Überzeugungen, dynamischer technischer Entwicklungen, manifester wirtschaftlicher Interessen und defensiver politischer Regulierungen statt.

Eine enge Definition von „digitaler Mündigkeit“ fokussiert sich hauptsächlich auf die technische Beherrschung digitaler Endgeräte und ihrer Anwendungen durch Individuen.

> „Mit digitaler Mündigkeit wird die Fähigkeit zur Mitnutzung und -gestaltung digitaler Räume bezeichnet, die eine Vielfalt differenzierter Teilfähigkeiten umfasst, welche technische, soziale und politische Komponenten einschließt („Literacies“). So sind digital mündige Bürger in der Lage, selbstbestimmt digitale Plattformen zu nutzen, unerwünschte Risiken zu vermeiden, einen angemessenen Umgang zu pflegen und ihre Interessen auf konstruktive Weise zu verfolgen.“[2]

1 vgl. Kurz/Rieger (2011): Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. Fischer Taschenbuch Verlag: Frankfurt a. M., S. 12-49.

2 Vgl. Basisdefinition eines Forschungsverbundprojekts der Universität Leipzig, Universität Frankfurt a.M., TU München aus dem Jahr 2016 für ein Forschungsprojekt des ISPRAT e.V. durchgeführt, das eine Analyse der digitalen Mündigkeit der deutschen Bevölkerung vorgenommen hat, in: https://www.cmgt.uni-leipzig.de/projekte/digitale_muendigkeit.html (Abfrage am: 14.7.2020).

Eine weite Definition „digitaler Mündigkeit" umfasst auch Ansprüche an eine demokratische Gestaltung digitaler Dienstleistungen und Verfahren auf der Systemebene.

> „Digitale Mündigkeit beinhaltet mehr als nur den bewussten Umgang mit Informationen in sozialen Medien oder den Schutz vor sichtbaren Gefahren wie Cyberbullying, Sexting, Identitätsklau oder Grooming. Politische Jugendbildung sollte verstärkt Wissen über die Hintergründe und Nutzungsmöglichkeiten von Big Data vermitteln und informationelle Selbstbestimmung in den Blick nehmen. Ziel muss es sein, auf diese Weise das Verständnis und das Interesse von Jugendlichen und jungen Erwachsenen an aktuellen Debatten über die politische, rechtliche und kulturelle Gestaltung der Digitalisierung zu befördern."[3]

Über digitale Mündigkeit verfügen Kinder und Jugendliche dann – so die These in diesem Beitrag – wenn sie digitale Endgeräte und Anwendungen selbstständig so nutzen, dass sie sich selbst und anderen weder kurz- noch langfristig schaden. Das schließt aber auch eine weitreichende demokratische Mitgestaltung politischer und wirtschaftlicher Rahmenbedingungen mit ein.

2. Kinder und Jugendliche als Datenproduzenten im Alltag und in der Schule

Schule und Elternhaus, Kinder und Jugendliche müssen in Zukunft einen intensiveren und kompetenteren Dialog über Selbstbestimmung, Datenschutz und Schutz der Privatsphäre in der digitalisierten Welt führen.

Für die versierte Nutzung von digitalem Spielzeug, Computerspielen, Sozialen Netzwerken, Videoplattformen, Suchmaschinen etc. ist es notwendig, dass Kinder und Jugendliche, aber auch Eltern und Lehrkräfte die technischen Verfahren und die dahinterstehenden Geschäftsmodelle besser kennen. Sie müssen umfassender verstehen, dass sie die weitgehend „kostenlose" Nutzung der Angebote mit wertvollen persönlichen Daten „bezahlen".

3 Jantschek 2015, 32-38.

2.1 „Smartes" digitales Spielzeug

Das kann bereits im Kinderzimmer beginnen, wenn Spielzeug über Bluetooth z.B. durch das Handy oder durch WLAN mit dem Internet verbunden ist. Dieses Spielzeug mag bei Kindern und Jugendlichen gut ankommen, aber es ist auch für Erwachsene nicht leicht zu durchschauen, dass Kinder damit unfreiwillig zu Datenlieferanten werden.[4]

Spielzeug, das heimlich Bild- und Tonaufnahmen von Kindern macht[5], das durch Werbung das Spiel unterbricht oder das zu In-App-Verkäufen einlädt, ist problematisch, weil es die Integrität des Spiels und den Schutz der kindlichen Sphäre verletzt.[6]

Bereits vorschulische Einrichtungen und Grundschulen brauchen in diesem Bereich eine größere Expertise, um Eltern und Kinder besser zu informieren und zu beraten sowie um Eltern und Erziehungsberechtigen die Gelegenheit zu geben, sich kritisch fortzubilden. Zur Aufklärung über Gefahren von digitalem Spielzeug im Vorschul- und Grundschulbereich können Verbraucherschutzorganisationen wichtige Partner sein.[7]

2.2 Computerspiele

Die kognitive, soziale, kulturelle und ästhetische Bedeutung von Computerspielen wird von den meisten Pädagogen unterschätzt. Die Diskussion wird von der Gewalt- und Suchtproblematik, die von Computerspielen ausgehen kann, dominiert. Themen wie Kontrolle und Überwachung, Datenschutz und Datamining werden in Zusammenhang mit Computerspielen im schulischen Kontext kaum diskutiert.

Die Thematik „Überwachung und Kontrolle" kann auf der spielerischen Ebene, d.h. innerhalb eines Computerspiels eine zentrale Rolle spielen.

---

4 Bundesamt für Sicherheit in der Informationstechnik (BSI): Smarte Spielzeuge. Lernhilfen oder Spione?, in: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/SmartToys/SmartToys_node.html (Abfrage am: 20.7.2020).

5 Die Puppe "Cayla" des Spielzeugherstellers „Genesis" wurde auf Anraten der Bundesnetzagentur verboten. Vgl. Hubschmid, Maria: Gefährliches Spielzeug. Eltern sollen Puppen zerstören. In: Der Tagesspiegel, 19.2.2017.

6 Heeger, Viola (2019): Spione im Teddyfell. Wenn Spielzeug Daten sammelt. In: Der Tagesspiegel, 23.12.2019.

7 Verbraucherzentrale: Vorsicht bei Smart Toys. Die Risiken von vernetztem Spielzeug (12.9.2018). Online verfügbar unter: https://www.verbraucherzentrale.de/aktuelle-meldungen/umwelt-haushalt/vorsicht-bei-smart-toys-die-risiken-von-vernetztem-spielzeug-29297 (Abgerufen am: 1.8.2020).

Das gilt für populäre Shooterspiele wie z.B. „Call of Duty. Modern Warfare 2019" (trotz USK 18 schon von vielen jüngeren Jugendlichen gespielt) oder elaborierte Rätselspiele wie z.B. „The Turing Test" 2016 (USK 12).[8] Aber nicht nur auf der Spielebene, sondern auch auf der Systemebene, d.h. außerhalb des eigentlichen Computerspiels sind Überwachung und Kontrolle von grundlegender Bedeutung. Fiktive Namen, phantasievolle Avatare, märchenhafte Spielhandlungen in irrealen Fantasiewelten können vergessen machen, dass Computerspielplattformen wie Steam, Nintendo etc. umfassend Daten ihrer Nutzer sammeln und auswerten. Neben Konto- und Adressdaten generieren die Spieleplattformen Informationen über Spielzeit und Spieldauer, Spielverhalten und Erfolgsraten, Kommunikationsverhalten und Normüberschreitungen.[9]

Darüber hinaus ist es wichtig zu wissen, dass Computerspiele hinsichtlich der implizit in sie eingeschriebenen politischen, ästhetischen und moralischen Wertmuster und Spielvarianten nicht neutral sind. Über die Identifikationsangebote, die ihre Spielcharaktere machen, durch die Sanktions- und Gratifikationsmechanismen, mit denen Spielhandlungen versehen werden, durch negative und positive Emblematiken, mit der soziale und natürliche Spielumwelten ausgestattet werden, sind Computerspiele geeignet, ästhetische, moralische und politische Intuitionen entweder zu stärken oder zu schwächen. Gamer geben komplexe Daten im Spielverlauf und im Kommunikationsverhalten über sich preis. Dabei ist es egal, ob sie einer gewalthedonistischen Engführung des Spielverlaufs die Präferenz geben oder Spielenarrative bevorzugen, die komplexe moralische Abwägungen und variantenreiche Spielhandlungen erlauben.[10] Die (spiel-)psychologischen Präferenzen der Spieler werden über die Auswertung von Spielhandlungen auf Dauer erschließbar und verwertbar.

---

8 Görig, Carsten: Rätselspiel "The Turing Test". Ist der Mensch noch schlauer als die Maschine?, in: Der Spiegel 10.9.2016. Online verfügbar unter: https://www.spiegel.de/netzwelt/games/the-turing-test-im-test-clevere-raetsel-und-ein-philosophischer-ueberbau-a-1111332.html (Abfrage am: 1.8.2020).

9 Mader, Illona (2020): Computerspielplattformen als panoptische Systeme. In: paidia. Zeitschrift für Computerspielforschung. Online verfügbar unter: https://www.paidia.de/panoptische-systeme/ (Abfrage am 27.0.2020).

10 Schellong, Marcel (2020): Einleitung. Überwachung und Kontrolle im Computerspiel. Online verfügbar unter: https://www.paidia.de/einleitung-ueberwachung-und-kontrolle/ (Abfrage am: 10.7.2020).

2.3 Soziale Netzwerke

Soziale Netzwerke wie z.B. WhatsApp werden von Kindern und Jugendlichen häufig erstmals im Umfeld der Familie, spätestens aber im Klassenverband und Freundeskreis genutzt. Ab der fünften Jahrgangsstufe (Alter 10-11 Jahre) wächst der soziale Druck zur Teilhabe am Klassenchat. Es geht dabei um Austausch über Hausaufgaben, schulische Termine, persönliche Verabredungen, Klatsch und Tratsch etc. In der EU müssen Jugendliche 16 Jahre alt sein, um WhatsApp zu nutzen. Diese Rechtsnorm wird in der Praxis regelmäßig und systematisch umgangen.

Kinder und Jugendliche, aber auch Erziehungsberechtigte und Pädagogen wissen oft nicht, dass WhatsApp standardmäßig das Telefonbuch des Smartphones ausliest und Kontaktdaten sowie Metadaten an das Mutterunternehmen Facebook weiterleitet. Das ist Teil der AGB von WhatsApp.[11] Die automatisierte Übermittlung dieser Daten geschieht oft aus Bequemlichkeit oder Unwissenheit und in der Regel ohne eine Einverständniserklärung der betroffenen Personen.[12] Tatsächlich müssten Erziehungsberechtigte von minderjährigen Jugendlichen eine Einverständniserklärung zur Nutzung und Weiterleitung dieser personenbezogenen Daten bei jedem einzelnen Kontakt einholen.[13] Erst seit Einführung der Europäischen Datenschutzgrundverordnung haben Nutzer das Recht, bei WhatsApp die gespeicherten Daten einzusehen und die Datenweitergabe an Facebook zu unterbinden.[14]

Krisen in den sogenannten „Klassenchats" fallen häufig ins Niemandsland der Zuständigkeit zwischen Elternhaus und Schule. Sie werden oft

11 Whatsapp: Rechtliche Hinweise. Online abrufbar unter: https://www.whatsapp.com/legal/?eea=0#key-updates (Abfrage am: 15.7.2020).

12 Riese, Dinah (2017): Datenweitergabe durch Whatsapp. Meine Kontakte, deine Kontakte. Online verfügbar unter: https://www.faz.net/aktuell/feuilleton/medien/weitergabe-von-kontakten-durch-whatsapp-vor-gericht-15085153.html (Abfrage am: 15.7.2020).

13 „Damit wir unsere Dienste betreiben und bereitstellen können, gewährst du WhatsApp eine weltweite, nicht-exklusive, gebührenfreie, unter lizenzierbare und übertragbare Lizenz zur Nutzung, Reproduktion, Verbreitung, Erstellung abgeleiteter Werke, Darstellung und Aufführung der Informationen (einschließlich der Inhalte), die du auf bzw. über unsere/n Dienste/n hochlädst, übermittelst, speicherst, sendest oder empfängst." WhatsApp: Datenschutzrichtlinien und Rechtliche Hinweise 2020. Online verfügbar unter: https://www.whatsapp.com/legal (Abfrage am: 15.7.2020).

14 Hery-Moßmann, Nicole: WhatsApp-AGB: Was drin steht und was es bedeutet, in: chip 15.6.2018. Online verfügbar unter: https://praxistipps.chip.de/whatsapp-agb-was-drin-steht-und-was-es-bedeutet_103143 (Abfrage am: 15.7.2020).

erst dann entdeckt, wenn es gravierende Konflikte zwischen den Kindern bzw. Jugendlichen gibt.[15] Ihnen fehlen oft die Kompetenzen, eskalierende Konflikte auf der Nutzer- und Moderatorenebene der sozialen Netzwerke einzudämmen. Für Unternehmen wie z.B. WhatsApp ist es in der Regel irrelevant, welche Kosten den Erziehungs- und Bildungseinrichtungen zur Behebung des sozialen Missbrauchs und der psychologischen Folgeschäden entstehen, obwohl sie durchgängig und umfassend Informationen über das Nutzungsverhalten der Kinder und Jugendlichen generieren. Zum Schutz der Persönlichkeitsrechte und der Integrität der Schülerinnen und Schüler und zur Wiederherstellung des Schulfriedens müssen Schulen erhebliche Ressourcen für externe Information, Beratung und Moderation mobilisieren.[16]

2.4 Videoportale

Videoplattformen wie „Youtube" und seit 2018 „TikTok" sind zum zentralen digitalen Leitmedium und zur kulturellen „Heimat" von Kindern und Jugendlichen geworden.[17] Sie rangieren in der Nutzungsfrequenz weit vor dem klassischen Fernsehen oder den Streamingportalen der öffentlichen Medienanstalten. Genres, die Kinder und Jugendliche z.B. auf YouTube interessieren, sind vor allem Musik- und Konzertvideos, Funny Clips und Filmtrailer. Beliebt bei Jungs sind Gaming-Videos und bei Mädchen überwiegend Fashion-, Mode- und Beauty-Videos.[18]

---

15 Hauptmann, Elke: Nach einer brutalen Auseinandersetzung liegen zwei Achtklässler des „Wiggy" im Krankenhaus Untertürkheim: Streit im Klassenchat eskaliert, in: Cannstatter Zeitung vom 10.12.2019, Online verfügbar unter: https://www.cannstatter-zeitung.de/inhalt.hervorhebung-nach-einer-brutalen-auseinandersetzung-liegen-zwei-achtklaessler-des-wiggy-im-krankenhaus-untertuerkheim-streit-im-klassenchat-eskaliert.21560e06-cb6c-4390-bc03-0e23cecae341.html (Abfrage am: 15.7.2020).

16 Landesanstalt für Kommunikation (LFK) Baden-Württemberg. Handy-Sektor (2017): Zehn goldene Regeln für den Gruppenchat in WhatsApp. Online verfügbar unter: https://www.handysektor.de/artikel/10-goldene-regeln-fuer-den-gruppenchat-in-whatsapp (Abfrage am: 20.7.2020).

17 JIM-Studie 2019, S. 14. Online verfügbar unter: https://www.mpfs.de/fileadmin/files/Studien/JIM/2019/JIM_2019.pdf (Abfrage am: 1.8.2020).

18 Repräsentative Befragung von über 800 Jugendlichen. Studie vom Rat für Kulturelle Bildung e.V. (2020): Jugend, YouTube, Kulturelle Bildung. Horizont 2019, Essen, S. 53. Online verfügbar unter: https://www.rat-kulturelle-bildung.de/fileadmin/user_upload/pdf/Studie_YouTube_Webversion_final.pdf (Abfrage am: 1.8.2020).

Die kritische Auseinandersetzung mit fragwürdigen Inhalten wie z.B. kommerziellen, extremistischen, rassistischen, gewaltverherrlichenden und pornographischen Inhalten findet im Rahmen der „klassischen" Medienerziehung an Schulen in der Regel kontinuierlich, manchmal auch anlassbezogen statt.

Knapp 50 Prozent der befragten Schülerinnen und Schüler betrachten die Plattform „YouTube" darüber hinaus auch als wichtige Informationsquelle und Lernhilfe für die Schule.[19] Auch viele Fachlehrkräften nutzen Videoportale im Unterricht. Ihnen ist aber oft nicht klar, dass sie ihren Schülerinnen und Schülern durch Qualitätsempfehlungen eine wichtige Orientierung bei der Rezeption von Fachinhalten außerhalb der Schule bieten könnten.

Kaum im Fokus der schulischen Medienpädagogik stehen Fragen des Daten- und Persönlichkeitsschutzes bei der Nutzung von Videoportalen. Die aktuelle Diskussion um Datenschutzprobleme bei der Nutzung des chinesischen Videoportals „TikTok" haben hier erstmals Aufmerksamkeit dafür geschaffen, dass u.U.

- kein Datenschutz für Kinder und Jugendlichen gewährleistet wird,[20]
- diskriminierende Moderationsregeln gezielt Minderheiteninteressen verletzen,[21]
- die Applikation in ihrer Programmierung massive Sicherheitslücken aufweist[22] und
- Bild- und Stammdaten für die Gesichtserkennung verwendet werden können.

19 Rat für Kulturelle Bildung 2019: 42f.

20 Koenigsdorff, Simon (2019): Erneute Klage wegen TikTok wegen fehlendem Kinder-Datenschutz. Online abrufbar unter: https://www.heise.de/newsticker/meldung/Erneute-Klage-gegen-TikTok-wegen-fehlendem-Kinder-Datenschutz-4606171.html (Abgerufen am: 1.8.2020).

21 Reuter, Markus; Köver, Chris: TikTok. Gute Laune und Zensur. Online verfügbar unter: https://netzpolitik.org/2019/gute-laune-und-zensur/ (Abgerufen am: 1.8.2020).

22 Westernhaben, Olivia von (2020): TikTok. Serverseitige Schwachstellen ermöglichten Account-Manipulation, Online abrufbar unter: https://www.heise.de/security/meldung/TikTok-Serverseitige-Schwachstellen-ermoeglichten-Account-Manipulationen-4630295.html (Abgerufen am: 1.8.2020).

2.5 Suchmaschinen

Durch die Internetsuchmaschinen „Google“ sei das wachsende Wissen dieser Welt jederzeit, an jedem Ort für jeden Menschen auffindbar; das versprechen die Google-Manager Eric Schmidt und Jared Cohen.[23]

Online-Suchmaschinen wie z.B. der Fast-Monopolist Google sind unerlässliche, zentrale Instrumente zur gezielten Erschließung der immensen Fülle an Informationen und Datentypen im World Wide Web. Die Suchergebnisse werden i.d.R. nutzungsbezogen priorisiert. Wirtschaftliche oder politische Interessen können die Gestaltung der Suchalgorithmen beeinflussen.

Kinder und Jugendliche, aber auch Pädagogen und Bildungsadministratoren, haben in der Regel Schwierigkeiten, das Geschäftsmodell und die Recherchelogik von Internetsuchmaschinen zu erklären. Den meisten Nutzern von Internetsuchmaschinen ist nicht klar,

- dass ihre individuelle Datensuche bereits Daten produziert, die ökonomisch wertvoll und kommerziell verwertbar sind und
- dass viele Suchmaschinen ihren Nutzerinnen und Nutzern personalisierte Resultate anzeigen und deshalb nicht allen dieselben Suchergebnisse präsentieren.

Die vermeintlich kostenlose Suchmaschine basiert auf einem Tauschvorgang zwischen Anfrage und Ergebnis: Bevor das Internet zur Informationsquelle wird, wird der Internetnutzer selbst bereits zum Informationsspender. Er gibt gebunden an seine IP-Adresse Daten über seinen Standort, seine Sprachen, seinen Bildungsgrad, seine Interessen, seine Überzeugungen, seinen Gesundheitszustand etc. preis.[24] Dieser Tausch beruht auf einer massiven Informationsasymmetrie. Denn die Nutzer kennen den Handelswert der von ihnen preisgegeben Informationen und den ihrer Suchhistorie in der Regel nicht. Sie können aber auch nicht den Profit einschätzen, den die Suchmaschinen-Anbieter mit den von ihr priorisierten Ergebnissen generieren. Es bleibt eine wichtige Aufgabe der Schule, Kindern und Jugendlichen das Zusammenspiel von ökonomischen, technischen und informatorischen Funktionen der Internetsuchmaschinen zu verdeutlichen

23 vgl. Schmidt 2014: 4, 13, 15, 21.

24 Weichert, Thilo (2008): Datenschutz bei Suchmaschinen, Unabhängiges Zentrum für Datenschutz Schleswig-Holstein. Online verfügbar unter: https://www.datenschutzzentrum.de/artikel/209-Datenschutz-bei-Suchmaschinen.html (Abfrage am 1.8.2020).

und sie zur Nutzung diskreter, alternativer Suchmaschinen ohne „Datensammelwut“ zu ermuntern.[25]

2.6 *Lernplattformen: Kinder und Jugendliche als Datenproduzenten in der Schule*

Mit der zunehmenden Digitalisierung von Lehr- und Lernprozessen durch digitale Stundenpläne, Klassenbücher, Fehlzeitendokumentationen, Lernsoftware, Lernplattformen, Videokonferenzapplikationen und E-Mail-Verkehr auf ungeschützten Accounts erweitern sich das Spektrum, die Reichweite und die Verfügbarkeit von Daten über Kinder und Jugendliche im schulischen Bereich. Die Erhebung, die Verwendung und der Schutz von Stammdaten, Noten- und Zeugnisdaten, Förderbedarfen, Fehlzeiten, Disziplinardaten sind durch Schulgesetze und Schuldatenverordnungen in den jeweiligen Ländern für den analogen Bereich weitgehend verlässlich geregelt.

Durch die Digitalisierung von Bildungs- und Lernangeboten werden verschiedene Datentypen überhaupt erst systematisch langfristig dokumentierbar und vorhandene Daten neu korrelierbar, wie z.B. Recherchedaten, Lerninhaltsdaten, Lernprozessdaten, Lernergebnisdaten, Kooperationsdaten, Zeitaufwände, Lernzeiträume, Fristeinhaltungen, Fehlzeiten etc. Diese Daten gab es zwar schon immer, sie waren aber nicht in dieser umfassenden Weise zu generieren, langfristig zu dokumentieren und analytisch zu verbinden.

Dies ist der wachsende Objektbereich der datenbasierten Analyse von Lernprozessen (Learning Analytics). Sie dient der Beschreibung und Optimierung von Lehr- und Lernverhalten in digitalen Lernumwelten.

Es ist kein triviales Problem, nachhaltig wirksame, faire Regelungen dafür zu schaffen, wie staatliche Institutionen und kommerzielle Anbieter digitaler Dienstleistungen mit der umfassenden, langfristigen und entgrenzbaren Dokumentation von Fehlversuchen, Fehleinschätzungen, Irrtümern, Versagen, Unvermögen und Normabweichungen von Kindern und Jugendlichen in digitalen Lernprozessen umgehen sollen (Vgl. hierzu Roßnagel in Bezug auf Löschpflichten in diesem Band).

---

25 „Jede Werbung, die nicht schulischen Zwecken dient, ist unzulässig.“ So oder ähnlich formulieren es die meisten Schulgesetze der Länder. Das Werbeverbot in Schulen steht allerdings in einem krassen Widerspruch zur Nutzung der kostenlosen Suchmaschinen, z.B. Google. Vgl. § 99 Abs. 2 SchulG NRW von 2005, i. d. F. v. 2020.

3. Herausforderungen für die Entwicklung digitaler Mündigkeit

Die kooperative Entwicklung von digitaler Mündigkeit bei Kindern und Jugendlichen wird durch eine asymmetrische Verteilung von Informations- und Gestaltungsmöglichkeiten gegenüber der Digitalindustrie auf drei Ebenen zu Ungunsten der Eltern und Pädagogen herausgefordert.

3.1 Wissensasymmetrie bei der Kosten-Nutzen-Kalkulation

Die erste Asymmetrie betrifft die Überforderung der Nutzer in Bezug auf die Verwendung digitaler Endgeräte und die Nutzung digitaler Angebote eine angemessen Kosten-Nutzen-Kalkulation durchführen zu können. Kinder und Jugendliche produzieren – ähnlich wie Erwachsene – oft ohne Absicht und Wissen mit ihren kurzfristigen individuellen Konsum- und Teilhabewünschen in der Digitalsphäre Daten und Metadaten, die langfristig Freiheiten und Spielräume einschränken können. Die Nutzer müssten zwischen den kurzfristigen Vorteilen, die die individuelle Nutzung vermeintlicher „Gratis“-Angebote der Digitalindustrie verspricht, und den langfristigen ideellen und materiellen Freiheitsverlusten, die durch die Enteignung und Verwertung privater Daten durch Digitalunternehmen entstehen, informierter abwägen können (Kurz/Rieger 2011: 246).

3.2 Machtasymmetrie zwischen Konsumenten und Digitalindustrie

Die zweite Asymmetrie besteht darin, dass Digitalunternehmen mit ihren Angeboten einen erheblichen Gruppendruck und machtvollen Konformitätszwang erzeugen können, deren sich die Kinder und Jugendliche, aber auch einzelne Familien oder isoliert handelnde Pädagogen kaum erwehren können.

Eine besondere Herausforderung für Eltern und Pädagogen liegt bei der Nutzung digitaler Medien und Anwendungen durch Minderjährige darin, dass die in der analogen Welt etablierten Erziehungs- und Unterstützungsverfahren zum Schutz von Kindern und Jugendlichen nicht direkt übertragbar sind. Die Erziehung zur Selbstständigkeit erfordert Verantwortungsbereitschaft auf Seiten der Jugendlichen und Vertrauen auf Seiten der Erziehungsberechtigten. Für eine entwicklungspsychologisch verantwortbare Abstufung bei der Nutzung digitaler Endgeräte und Anwendungen fehlen Eltern und Lehrkräften oft die technischen, juristischen und in-

haltlichen Kompetenzen. Der Anspruch auf Durchsetzung rechtlicher Regelungen des Jugendschutzes und die alltägliche Realität einer permissiven Auslegung und laxen Handhabung digitaler Anwendungen treten oft weit auseinander.

3.3 Verantwortungsasymmetrie bei der Nutzung digitaler Angebote

Die dritte Asymmetrie besteht in der ungleichen Verteilung von Verantwortung. Eltern und Pädagogen müssen die volle Verantwortung für die private bzw. schulische Nutzung und auch den Missbrauch digitaler Angebote durch Minderjährige übernehmen[26], verfügen aber oft nicht über ausreichend Wissen bzw. Techniken, diese Aufsicht auszuüben. Die Digitalindustrie, die alle Register der Generierung, Auswertung und Weiterverwertung von Daten zieht, muss dagegen keine pädagogische Verantwortung übernehmen. Mit dem digitalen Endgerät entsteht für Kinder und Jugendliche eine neue virtuelle Privat- und Intimsphäre, die den unmittelbaren Vertrauenspersonen Eltern und Pädagogen, die die volle Erziehungsverantwortung haben, oft nicht zugänglich ist und die für Unternehmen und Dienstleistern der Digitalindustrie weitgehend auslesbar ist, ohne dass sie eine angemessene Form der Verantwortung oder Haftung übernehmen müssen.

4. Schule und ihr Beitrag zum Aufbau digitaler Mündigkeit bei Kindern und Jugendlichen

4.1 Ansätze für ein pädagogisches Konzept digitaler Mündigkeit

Die Kultusministerkonferenz (KMK) definierte im Jahr 2016 „Kompetenzen in der digitalen Welt", über die Jugendliche ab 2018 bis zum Ende ihrer Pflichtschulzeit, d.h. im Alter von 15 bis 16 Jahren verfügen sollen.[27]

---

26 Jackewitz, Iver (2017): Haften Eltern bei Instagram, Snapchat, WhatsApp & Co. für ihre Kinder?. Online verfügbar unter: http://www.jackewitz.de/haften-eltern-bei-instagram-snapchat-whatsapp-co-fuer-ihre-kinder/ (Abfrage am: 1.8.2020).

27 Kultusministerkonferenz (KMK) (2016): Bildung in der digitalen Welt. Online verfügbar unter: https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2018/Strategie_Bildung_in_der_digitalen_Welt_idF._vom_7.12.2017.pdf (Abgerufen am: 1.8.2020).

In allen sechs Kompetenzbereichen verbinden sich mit den geforderten technisch-funktionalen Aspekten der Beherrschung digitaler Geräte und Programme auch der Aufbau von Urteilsvermögen und Entscheidungskompetenz. Damit formuliert die KMK eine Idee „digitaler Mündigkeit", die für die Medienbildung in den jeweiligen Ländern einen ersten verbindlichen Orientierungsrahmen schafft.

Die von der KMK formulierten digitalen Kompetenzen sind fächerübergreifend formuliert. Jedes Fach soll einen spezifischen Beitrag zu deren Entwicklung leisten. Die Jugendlichen sollen am Ende ihrer Pflichtschulzeit

- Informationen und Informationsquellen analysieren und kritisch bewerten können. (**Kompetenzbereich 1 „Suchen, verarbeiten und aufbewahren"**),
- ethische Prinzipien bei der Kommunikation und Partizipation im Internet berücksichtigen (**Kompetenzbereich 2 „Kommunizieren und Kooperieren"**),
- die Persönlichkeitsrechte anderer Menschen beachten (**Kompetenzbereich 3 „Produzieren und Präsentieren"**),
- die potenziellen Risiken und Gefahren, die in digitalen Umgebungen lauern, richtig einschätzen (**Kompetenzbereich 4 „Schützen und sicher agieren"**). Das erfordert auch praktische Kenntnisse, wie sie sich gegen „Datenmissbrauch" wehren und ihre „Privatsphäre" schützen können,
- die grundlegenden Funktionsweisen und Prinzipien der digitalen Welt kennen und verstehen (**Kompetenzbereich 5 „Problemlösen und Handeln"**) sowie
- „die interessengeleitete Setzung, Verbreitung und Dominanz von Themen in digitalen Umgebungen erkennen und beurteilen" sowie „die Bedeutung der digitalen Medien für die politische Meinungsbildung und Entscheidungsfindung kennen und nutzen" (**Kompetenzbereich 6 „Medien in der digitalen Welt verstehen und reflektieren"**).

Bei der Diskussion um digitale Kompetenzen als einem Weg zur digitalen Mündigkeit ist es wichtig, entwicklungspsychologisch den Grad der Reife der Kinder und Jugendlichen zu berücksichtigen. Der Gesetzgeber gibt durch das Jugendschutzgesetz und andere rechtliche Regelungen hierbei eine grobe Orientierung.

4.2 Stärkung der Basiskompetenz im (Selbst-)Datenschutz bei Schülerinnen und Schülern, Pädagogen und Eltern

Schule sollte massiv dabei mitwirken, die Datenschutz-Kompetenzen von Schülerinnen und Schülern sowie die des eigenen Personals und der Eltern zu stärken. Kinder und Jugendliche müssen lernen, wie sie aktiv ihre Privatsphäre schützen und Datensparsamkeit praktizieren, d.h. sie müssen die Kompetenz erwerben,

- sichere Passwörter zu verwenden und geheim zu halten, Virenscanner und Verschlüsselungsanwendungen einzusetzen sowie Einstellungen auf Endgeräten und Betriebssystemen datensparsam zu konfigurieren,
- so wenig persönliche Daten (Stammdaten, Statements, Bilder, Filme, Bewegungsprofile, Gesundheitsdaten etc.) auf Internetseiten, in Chatrooms und sozialen Netzwerken wie möglich preiszugeben,
- beim Umgang mit Daten die Persönlichkeitsrechte anderer Personen zu achten,
- bei Apps zu wissen, welche Daten sie abschöpfen und wo Abo-Fallen lauern sowie
- die Gefahren von Cybermobbing, Cybergrooming und Sexting sicher einzuschätzen und abzuwenden.[28]

4.3 Aufbruch vom passiven Konsum zur aktiven Gestaltung digitaler Technologien und Anwendungen

Schule kann wichtige Impulse setzten, digitale Technologien und Anwendungen kreativ und kritisch zu nutzen. Es ist besser, Erklärfilme selbst zu drehen, als sie zu konsumieren. Es ist sinnvoll, Erfahrungen zu sammeln, wie sich einfache Computerspiele programmieren lassen, als sich stundenlang der suggestiven Kraft der Anreizsysteme etablierter Spielnarrative auszusetzen. Es ist instruktiv eine Internetseite selber zu gestalten und die ihr hinterlegten Zählfunktion selber zu programmieren. Es ist wichtig, gestalterische Erfahrungen mit der Programmierung von Robotikanwendungen und Künstlicher Intelligenz zu machen, um eine Idee davon zu gewinnen, wie Daten erhoben und dargestellt sowie ausgewertet und funktionalisiert werden können. Insgesamt müssen Eltern und Pädagogen die verschiedenen Rollen, die Kinder und Jugendliche in der digitalen Welt übernehmen

28 Wochenschau (2015): Datenschutz. Checkheft – Sek I.: Schwalbach.

können, stärker profilieren und entwickeln, z.B. auf der Ebene des Konsumierens, des Mitmachens, des Sammelns, des Programmierens sowie der Kritik, der Produktion und der technischen, gesellschaftlichen und politischen Gestaltung.

4.4 Entwicklung einer Erziehungspartnerschaft und Lerngemeinschaft in Bezug auf digitale Technologien und Anwendungen zwischen Lehrkräften, Jugendlichen und Eltern

Die Mediennutzung von Kindern und Jugendlichen stellt alle unmittelbar Beteiligten vor große Herausforderungen. In oft nervenaufreibenden Aushandlungsprozessen stecken Eltern und Lehrkräfte, Kinder und Jugendliche den Grad der Verfügung über digitale Endgeräte und ihre vielfältigen Anwendungen ab.

In diesen Aushandlungen geht es auch immer wieder um eine entwicklungspsychologisch angemessene Verabredung sinnvoller Mediennutzung, die einerseits Freiheit ermöglichen soll und andererseits Grenzen setzen muss, ohne das Recht der Kinder und Jugendlichen auf Privatheit und Datenschutz aus dem Blick zu verlieren.

Aushandlungskonflikte zwischen Eltern und Kindern bzw. Jugendlichen um die Mediennutzung sind erst einmal gut, selbst wenn es Streit gibt. Denn in der Auseinandersetzung darüber, welche Medien und Inhalte wie, wie lange, warum und wozu genutzt werden, steckt ein wichtiges Moment zur Entwicklung „digitaler Mündigkeit".

Schule kann wichtige Impulse setzen, z. B.

- im Rahmen von präventiv ansetzenden Informationsveranstaltungen und Fortbildungen für Eltern und Lehrkräfte,
- in Workshops mit externen Referenten zu Themen wie Datenschutz und Datensicherheit sowie Cybermobbing,
- bei pädagogischen Tagen zu einschlägigen medienpädagogischen Themen mit Lehrkräften, Eltern und Schülerinnen und Schülern als Teilnehmende oder Experten.

4.5 Aufbau von Interessenverbänden und Lobbyorganisationen für Eltern, Pädagogen und Jugendlichen zur fairen Gestaltung digitaler Geräte und Anwendungen

Pädagogen, Eltern, Schülerinnen und Schüler müssen ihre digitalpolitischen Interessen für die Sicherheit und den Schutz ihrer Privatsphäre und Gesundheit stärker in die politischen Entscheidungsprozesse und die Produktentwicklung einbringen können. Für die praxisnahe Interessenartikulation und -wahrung brauchen sie unabhängige Foren und starke Organisationen (z.B. digitale Verbraucherschutzeinrichtungen, Beratungsstellen, Lobbyorganisationen etc.).[29]

Die Digitalindustrie muss für die psychischen, aber auch die materiellen Schäden bei Kindern und Jugendlichen, die sie im Zuge ihrer Gewinnabschöpfungen hinterlässt, ungeachtet der vermeintlich kostenlosen Bereitstellung von Dienstleistungen stärker in Haftung genommen werden. Das geht nur durch starke Interessenvertretungen von Nutzern, die auf die digitalen Dienstleistungen nicht verzichten können oder wollen, die aber auch ein Anrecht auf eine präventiv ansetzende, faire und rücksichtsvolle Ausgestaltung digitaler Technologien haben.[30]

5. Selbstdatenschutz reicht nicht

Die Nutzer digitaler Endgeräte und Anwendungen bezahlen Dienstleistungen, die vermeintlich umsonst sind, in der Regel mit ihren eigenen Daten (z.B. Verhaltens-, Befindlichkeits-, Kommunikations-, Bewegungs-, Transaktions-, Konsumdaten etc.).

Der Wert dieser privaten Daten und Metadaten und die dahinterstehende Tauschlogik der Digitalökonomie ist den Kindern und Jugendlichen, ja selbst den erwachsenen Nutzern in ihrer Tiefe und Breite und den damit verbundenen weitreichenden Folgen oft nicht bewusst. Ihre Komplexität und Abstraktheit sind nach wie vor schwer zu vermitteln.

---

29 Es ist fraglich, ob das Bundesamt für Sicherheit in der Informationstechnik (BSI) diesen Auftrag praxisnah wahrnehmen kann. Vgl. https://digitalcharta.eu/neuigkeiten/ (Abfrage am: 20.7.2020); vgl. die Angebote der Stiftung Wahrentest „Digitale Welt für Einsteiger https://www.test.de/presse/pressemitteilungen/Digitale-Welt-fuer-Einsteiger (Abfrage am: 20.7.2020).

30 Vgl. Regelungen der Datenschutzgrundverordnung (DSGVO) und Ansätze für eine Charta digitaler Grundrechte in Europa, in: https://digitalcharta.eu/neuigkeiten/ (Abfrage am: 20.7.2020).

Der Medienbildung in der Schule kommt in Bezug auf das Leben und Lernen in digitalen (Um-)Welten deshalb eine bedeutende Rolle zu. Die Schule kann die digitale Medienkompetenz von Schülerinnen und Schüler maßgeblich stärken und unter bestimmten Bedingungen einen Beitrag zur „digitalen Mündigkeit" leisten. Hierfür braucht Schule gut ausgebildete und substanziell fortgebildete Lehrkräfte.

Es wäre allerdings eine Illusion, zu glauben, dass „digitale Mündigkeit" als Selbstdatenschutz ausschließlich im Sozialraum Familie oder Schule hergestellt werden kann. Hierfür braucht es nach wie vor Organisationen, Initiativen und Foren, die die Schutzinteressen von Kindern und Jugendlichen, von Eltern und Pädagogen massiver als bisher gegenüber staatlichen und wirtschaftlichen Akteuren der Digitalökonomie artikulieren können.

Literatur

Printmedien

Fuchs, Christian (2019): *Soziale Medien und kritische Theorie. Eine Einführung*. UVK Verlag: München.

Friedewald, Michael (Hg.) (2018): *Privatheit und selbstbestimmtes Leben in der digitalen Welt. Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes*. Springer Vieweg: Wiesbaden.

Friedewald, Michael / Lamla, Jörn / Roßnagel, Alexander (Hg.) (2017): *Informationelle Selbstbestimmung im digitalen Wandel*. Springer Vieweg: Wiesbaden.

Hellweg, Martin (2014): *Safe Surfer. Schutz der Privatsphäre im digitalen Zeitalter*. Ullstein Verlag: Berlin.

Jantschek, Ole (2015): *Digitale Mündigkeit – Informationelle Selbstbestimmung als Ziel und Thema politischer Jugendbildung.* In: Journal für Politische Bildung (Wochenschau Verlag), 2/2015, S. 32-38.

Jugendschutz.net (2020): *Jugendschutz im Internet. Bericht 2019 – Risiken und Handlungsbedarf*: Mainz.

Medienpädagogischer Forschungsverbund Südwest c/o Landesanstalt für Kommunikation (LFK) (2019): *JIM-Studie 2019. Basisuntersuchung zum Medienumgang 12-19 Jähriger.* Stuttgart.

Kurz, Konstanze / Rieger, Frank (2011): *Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen*. Fischer Taschenbuch Verlag: Frankfurt a. M.

Schmidt, Eric / Cohen, Jared (2014): *The New Digital Age. Reshaping the Future of People, Nations and Business*. John Murray: London.

Schulze, Thomas (2015): *Was Google wirklich will. Wie der einflussreichste Konzern der Welt unsere Zukunft verändert*. DVA: München.

Wochenschau (2015): *Datenschutz.* Checkheft – Sek I., Schwalbach.

Internetseiten

Bundesamt für Sicherheit der Informationstechnik
https://www.bsi-fuer-buerger.de

Internationales Zentralinstitut für das Jugend- und Bildungsfernsehen (IZI)
https://www.br-online.de/jugend/izi/deutsch/home.htm

Jugendschutz Net. Kinder und Jugendlichen ein gutes Aufwachsen mit Medien ermöglichen
http://www.jugendschutz.net/

Klick safe. Unabhängige Internetseite für mehr Sicherheit im Internet
https://www.klicksafe.de

Medienpädagogischer Forschungsverbund Südwest
https://www.mpfs.de/startseite/

Datenkompetenz durch edukatives Privacy Nudging: Zentrale Prinzipien und Effekte auf Lernprozesse

Andreas Janson, Leonie Kreidel, Sofia Schöbel, Gerrit Hornung, Matthias Söllner und Marco Leimeister

Abstract

Die Digitalisierung verändert nicht nur unser privates, sondern auch unser Arbeitsleben. Immer mehr Daten über Individuen sind online verfügbar und werden für die Nutzung von bestimmten Online Services vorausgesetzt. Hierbei verlieren die Nutzenden oft den Überblick, wie und welche Daten sie von sich preisgeben. Dies birgt nicht nur das Risiko der Preisgabe von privaten Daten, sondern auch unternehmensseitig das Risiko, dass wichtige Daten außerhalb des Unternehmens veröffentlicht werden. Hier kann das Konzept des digitalen Nudgings angewandt werden, welches nunmehr auch als edukatives Privacy Nudging genutzt werden kann. Das Konzept bezweckt, Individuen durch bestimmte Elemente wie beispielsweise Defaults zu Verhaltensänderungen anzuregen. Dieser Beitrag hat zum Ziel, einen Überblick darüber zu geben, welche Privacy Nudges es im edukativen Bereich gibt und wie diese mit verschiedenen Lerntheorien in Einklang gebracht werden können. Der Text soll Forschern und Praktikern eine Orientierung geben, selbst edukative Privacy Nudges zu gestalten und endet mit einem Fallbeispiel, das aufzeigt wie einfache Gestaltungsänderungen Individuen dazu anregen können, sich privatheitsfreundlicher zu verhalten und sorgsamer mit ihren privaten Daten umzugehen.

1. Einleitung und Motivation

Die fortschreitende Digitalisierung und Entwicklungen von Informationstechnologien ermöglichen eine einfache und zunehmende weltweite Vernetzung. Dies hat Auswirkungen auf unsere Gesellschaft und Wirtschaft. Wertschöpfungsprozesse und Arbeitsweisen in Unternehmen verändern sich grundlegend. Zentral für diese Art der Wertschöpfung sind Daten, die

als zentraler ökonomischer Motor agieren, beispielsweise um Angebote von sozialen Netzwerken und anderen Plattformen bestmöglich auf eine bestimmte Gruppe von Nutzenden anzupassen (Krasnova et al. 2010). Mit dieser Entwicklung gehen einerseits enorme Innovationspotenziale einher, beispielsweise die angesprochenen datengetriebenen Geschäftsmodelle. Andererseits entstehen auch große Risiken, welche die Preisgabe und den Umgang mit personenbezogenen Daten in der Plattformökonomie betreffen. Plattformen aller Art sind davon abhängig, dass möglichst viele oder zumindest genug relevante Daten von Nutzenden preisgegeben werden, wodurch beispielsweise das von Zuboff (2019) beschriebene Phänomen des Überwachungskapitalismus entstehen kann.

Entsprechend sind Konzepte notwendig, um mit dem Spannungsverhältnis zwischen Privatheit und den Innovationspotenzialen der Datenökonomie umgehen zu können (Acquisti et al. 2015). Der systematische Aufbau von Datenkompetenz (im Sinne einer spezifischen Form der Medienkompetenz) und die technische Unterstützung entsprechender Lernprozesse zur Sicherstellung eines reflektierten und souveränen Umgangs mit Daten können hierbei als zentrale Instrumente dienen, um diesem Spannungsverhältnis zu begegnen und Individuen ein für sie angemessenes Verhältnis von Privatheit und Datenpreisgabe zu ermöglichen. Gleichzeitig sind Umsetzungsinstrumente notwendig, um diese Kompetenzen zu vermitteln. Dabei gehen wir davon aus, dass klassische Bildungsträger diese nicht allein mit hergebrachten Methoden vermitteln können, sondern proaktive Prozesse wie edukative Nudging-Ansätze im Rahmen der Nutzung von digitalen Plattformen benötigt werden.

Die zentrale Grundannahme basiert auf dem Verständnis, dass Datenkompetenz eine wichtige Voraussetzung ist, damit Nutzende von digitalen Plattformen reflektierte Entscheidungen über die Preisgabe personenbezogener Daten treffen können. Beispielsweise wurde im Rahmen des sogenannten Privacy Paradox festgestellt, dass Menschen zwar abstrakt den Schutz ihrer Privatheit stark fokussieren, sie aber dennoch teilweise entgegengesetzt handeln (Smith et al. 2011). Die Gründe dafür sind vielfältig und können u.a. im fehlenden Verständnis für die Konsequenzen der Verletzung von Privatheit, in der Unkenntnis, wie man seine Privatheit schützen kann, und in der Komplexität der technischen Instrumente zur Wahrung der Privatheit liegen (Coventry et al. 2016). Datenkompetenz betrifft nicht nur die Vorstellung, welche Daten preisgegeben werden, sondern auch das Verständnis davon, was mit komplexen Verfahren, z.B. Machine Learning, mit personenbezogenen Daten möglich ist (Jones 2019) und welche Akteure (Nutzende, Datenempfänger und Dritte) hiervon profitieren können. So kann aus der Preisgabe personenbezogener Daten hoch-

wertiges Wissen geschaffen werden. Bisher fehlen aber ein tiefgreifendes Verständnis und entsprechende Handlungskompetenz bei Nutzenden (und Unternehmen), um die mögliche Wertrealisierung einer Preisgabe von (personenbezogenen) Daten einzuschätzen (Günther et al. 2017). Gleichwohl kann aber Datenkompetenz als Grundlage für souveränes Agieren im digitalen Raum dienen.

Ansatzpunkte zur Förderung von Datenkompetenz im Rahmen der Nutzung digitaler Angebote kann das sogenannte Privacy Nudging bieten, welches das Verhalten in digitalen Umgebungen vorhersehbar dahingehend beeinflussen soll, dass privatheitsfreundliche Entscheidungen getroffen werden (Adjerid et al. 2019, Acquisti 2009). Hier können edukative Nudges (Heidbrink/Klonschinski 2018), nicht nur das Verhalten beeinflussen, sondern durch eine Reflexion auch Lernprozesse befördern. Ziel dieses Beitrags ist es daher, zentrale Prinzipien des Nudgings zu präsentieren und die datenschutzrechtliche Erforderlichkeit und Zulässigkeit im Anschluss an existierende Diskussionen (Sandfuchs 2015, Sandfuchs/Kapsner 2018) zu behandeln. Des Weiteren werden ausgewählte edukative Nudges vor dem Hintergrund zentraler Lerntheorien dargestellt und diskutiert, ob diese zum Aufbau von Datenkompetenz geeignet sind. Dies wird im Rahmen einer Fallstudie am Beispiel der mobilen Applikation Snapchat beleuchtet, welche aus Sicht des Datenschutzes und der jungen Gruppe von Nutzenden einschlägig ist, um das Thema der edukativen Privacy Nudges zu illustrieren.

2. *Theoretischer Hintergrund – Nudges, Digital Nudges und Privacy Nudges*

Der Ansatz des Nudgings kommt aus den Verhaltenswissenschaften und wurde federführend durch Richard Thaler und Cass R. Sunstein geprägt (Thaler/Sunstein 2008). Nudges versuchen durch externe Veränderungen des Handlungsrahmens Personen in Richtung bestimmter Handlungsoptionen zu „stupsen" (englisch: to nudge), während die anderen Handlungsmöglichkeiten weiterhin offenstehen und somit die Entscheidungsfreiheit des Individuums erhalten bleibt. Ein Individuum wird lediglich zu einer Handlungsoption „genudged", deren Folgen – aus Sicht des Nudgenden, d.h. wirklich oder vermeintlich – dem Interesse des Individuums am besten entsprechen.

2.1. Denkmodi im Nudging

Nudges sind daher im Prinzip des libertären Paternalismus verankert (Mirsch et al. 2018). Es gibt viele unterschiedliche Szenarien, in denen Verhaltensänderungen mit Hilfe von Nudges herbeigeführt werden können. Sie können im Online-, sowie auch im Offline-Bereich genutzt werden und umfassen eine Vielzahl an Ansätzen. Im Offline-Bereich beeinflusst beispielsweise in einer Mensa der Ort, an dem ein Essen präsentiert wird, die Anzahl der Personen, die sich für dieses Essen entscheiden: Steht die vegetarische Option am Anfang oder wird die Aufmerksamkeit mit anderen Mitteln auf diese gelenkt, entscheiden sich mehr Menschen für diese Option. Nudges im Online-Bereich übertragen dieses Prinzip auf den digitalen Raum und lenken mit Hilfe von entsprechenden Designelementen in der Benutzeroberfläche die Individuen in die gewünschte Richtung (Weinmann et al. 2016), beispielsweise durch das Setzen von Voreinstellungen bei der erstmaligen Nutzung von Informationssystemen (Schöbel et al. 2020a).

Der Ansatz des libertären Paternalismus geht davon aus, dass Menschen nicht immer nach ihrem besten Interesse wählen und bezieht sich dabei auf die Theorie der zwei Systeme von Kahnemann und Tversky, welche zwei Denkmodi darstellen: die System 1- und die System 2-Denkweise (Kahneman 2011). Diese beiden unterschiedlichen Systeme beschreiben zwei mögliche Wege, die das Gehirn bei der kognitiven Verarbeitung von Reizen und Aufgaben einschlagen kann. Es sind zwei Systeme des Denkens. Die Denkweise von System 1 arbeitet automatisch und schnell, weitgehend mühelos und ohne willentliche Steuerung. Dagegen agiert die Denkweise von System 2 bewusst gesteuert, angestrengt und langsamer, womit das Denken von System 2 in der Lage ist, sich mit komplexen Problemen auseinanderzusetzen. Der Einsatz von System 2 erfordert die Aufmerksamkeit und die Konzentration von Individuen. Beides ist im Alltag schwierig und anstrengend aufrechtzuerhalten. System 1 macht demgegenüber Gebrauch von sogenannten Heuristiken, also verkürzten kognitiven Operationen, mit denen im Alltag ressourcensparend Schlussfolgerungen gezogen werden können, ohne dass komplizierte kognitive Vorgänge verlangt werden. Beide Systeme können, falls notwendig, gleichzeitig aktiv sein und zusammenarbeiten. Die Theorie geht davon aus, dass durch den Einsatz der Heuristiken vor allem in komplexen Situationen zwar rasche, zugleich aber voreilige und systematisch verzerrte Entscheidungen getroffen werden und Individuen per se anfällig für Urteilsfehler (Biases) sind (Kahneman 2011). Zur Verdeutlichung dieser Urteilsfehler wird als Beispiel der Ankereffekt dargestellt. Dieser Effekt tritt auf, wenn einer Schätz-

frage vorrausgehend eine unbestimmte Zahl dargeboten wird. Beispielsweise gaben Englisch und Mussweiler (2001) 16 Richtern, die mindestens 15 Jahre im Amt waren, Material in welchem ein Delikt geschildert wurde. Anschließend bekamen diese die Information, ein Informatikstudent schlüge ein Strafmaß von 12 Monaten (Gruppe 1) oder 32 Monaten (Gruppe 2) vor. Die Richter sollten die Angemessenheit des Vorschlags beurteilen und anschließend selbst ein Strafmaß festsetzen. Die Richter in Gruppe 1 nannten durchschnittlich 28 Monate, die in Gruppe 2 35 Monate als angemessenes Strafmaß. Die genannten Monate blieben im Anschluss also näher bei der Anzahl an Monaten, die den Richtern im Voraus vorgeschlagen wurde (Enough/Mussweiler 2001). Dies bedeutet jedoch nicht, dass Individuen grundsätzlich irrational und unberechenbar sind, sondern dass man vielmehr mit einer systematischen, vorhersehbaren Abweichung vom rationalen Verhalten rechnen kann (Hertwig/Grüne-Yanoff 2017).

Nudges machen sich diese Urteilsfehler zunutze, indem sie die Auswahlmöglichkeiten so designen, dass das System 1 der Individuen die angestrebte Entscheidung auswählt. Manche Nudges erfordern auch die Mitarbeit des System 2. Bei diesen wird davon ausgegangen, dass sie einen langfristigen Lerneffekt hervorrufen (siehe auch zum Konzept des verwandten Boostings: Hertwig/Grüne-Yanoff 2017).

2.2 Privacy Nudging

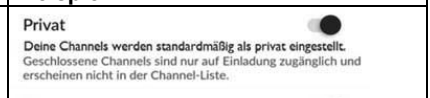
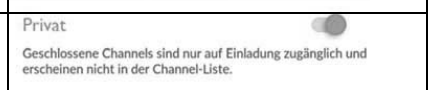
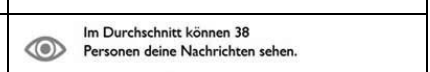
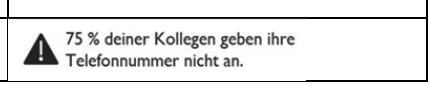
Das Ziel der Privacy Nudges ist es, den Entscheidungsprozess der Individuen in Richtung „besserer" Entscheidungen in Hinblick auf ihre Privatheit zu lenken und sie zu befähigen, ihre informationelle Selbstbestimmung zu berücksichtigen. Aufgrund von Biases werden beispielsweise personenbezogene Daten oftmals unüberlegt offengelegt, da das Risiko einer Verwendung der offengelegten Daten (Überwachung, Profilbildung etc.) mental weniger präsent ist (Verfügbarkeitsheuristik). Privacy Nudges setzen dabei an den beiden Denkmodi an, indem sie Heuristiken ausnutzen, beispielsweise durch privatheitsfreundliche Defaults, oder ihnen entgegenwirken, beispielsweise indem Denkprozesse bewusst nicht abgekürzt, sondern Reflexionsprozesse bei der Datenpreisgabe angestoßen werden (Weinmann et al. 2016).

Die Diskrepanz zwischen der hohen Bedeutung eigener Privatheit und dem dazu gegenläufigen Preisgeben von personenbezogenen Daten kann auf fehlende Handlungskompetenz und automatische, emotionale Entscheidungen zurückgeführt werden (Kühling/Martini 2016). Das Verhalten von Individuen bei der Preisgabe von Daten ist oftmals irrational. Pri-

vacy Nudges können diese Irrationalität im Verhalten nutzen, um Privatheit in unterschiedlichen Szenarien zu fördern.

Privacy Nudging-Konzepte („Anstupser") sollen das Verhalten von Nutzenden dahingehend beeinflussen, dass sie privatheitsfreundlichere Entscheidungen treffen. In diesem Sinne soll ein bewusster Umgang mit personenbezogenen Daten gefördert werden, um informationelle Selbstbestimmung sicherzustellen (Acquisti et al. 2017). Tabelle 1 stellt mögliche Elemente für den Einsatz der Privacy Nudges in digitalen Arbeitssystemen dar, welche durch Konzeptentwickler ausgewählt und gestaltet werden können (siehe hierzu und im Folgenden die Forschungsergebnisse von Schomberg et al. 2019, welche als Grundlage in diesem Beitrag dienen).

Tab.1: Beispiele digitaler Privacy Nudges im Arbeitsumfeld (Schomberg et al. 2019)

Privacy Nudge	**Beispiel**
Default	
Framing	
Information	
Feedback	
Zeitverzögerung	
Soziale Norm	

Default

Als Default Nudge werden Standardeinstellungen im System beschrieben (Acquisti et al. 2017), welche meist als voreingestellte Optionen bevorzugt und nur selten verändert werden (Status-quo Bias). Individuen nutzen Defaults als Informationsquelle und zugleich als Referenzpunkt für das Abwägen von Entscheidungsoptionen. Defaults können tendenziell als die stärksten Nudges bewertet werden (Hummel/Maedche 2019) und gelten auch im Privacy Nudging als sehr effektiv, da Individuen in digitalen Um-

gebungen die Privatheits-Einstellungen oftmals nicht nach ihren eigenen Bedürfnissen modifizieren. Defaults sind effektiv, weil sie nur einen sehr geringen kognitiven Beitrag und gar kein oder ein nur geringes Handeln des Individuums erfordern, zugleich aber dennoch die privaten Daten schützen.

Framing

Farbelemente können als Framing-Nudge verwendet werden, wobei farbliche Hinterlegungen die Aufmerksamkeit auf ausgewählte Elemente lenken, um bestimmte Entscheidungsalternativen hervorzuheben und so attraktiver erscheinen zu lassen (Turland et al. 2015). Die Schaltfläche zur Datenfreigabe kann zum Beispiel gegenüber den anderen Schaltflächen farblich hervorgehoben werden. Im hier gezeigten Beispiel wird der „privat"-Button in grüner Farbe markiert. Dies trägt dazu bei, dass Individuen bevorzugt diese Option wählen. Im Rahmen der digitalen Arbeit wären sensible Daten nun ausschließlich für eine bestimmte Zielgruppe oder nur für das Individuum selbst zugänglich (Almuhimedi et al. 2015). Framing-Nudges haben den großen Vorteil, dass diese ohne großen Aufwand in das Design integriert werden können und das Individuum schnell und effektiv dazu bewegen, wichtige Entscheidungen in Bezug auf seine Privatheit zu überdenken.

Information

Häufig ist die Wahrscheinlichkeit einer Verletzung der Privatheit nicht nachvollziehbar und wird deshalb oft unterschätzt. Dies kann auf die Repräsentationsheuristik zurückgeführt werden, welche die Gefahr beschreibt, dass Individuen die Häufigkeit der Beobachtungen eines Ereignisses fälschlicherweise mit dessen Eintrittswahrscheinlichkeit in Verbindung bringen. Dabei wird aus einem Prozess ein kleiner Ausschnitt als repräsentativ für den ganzen Prozess angesehen und schnell als Muster für alle Ereignisse anerkannt. Einen weiteren Einfluss stellt die Verfügbarkeitsheuristik dar, bei der Entscheidungen auf Informationen gestützt werden, die mental leicht verfügbar sind (Acquisti et al. 2017, Tversky/Kahneman 1974). Das Individuum über Risiken und Konsequenzen seines Handelns aufzuklären, ist deshalb eine effektive Methode, um zu verhindern, dass diese Heuristiken greifen. Diese Informationen kann das Individuum nutzen, um eine fundierte Entscheidung in Bezug auf die eigene Privatheit zu treffen.

Feedback

Die Bereitstellung von Feedback als Privacy Nudge weist ein Individuum auf sein bisheriges Nutzungsverhalten hin. Dadurch entsteht ein Bewusstsein über die bisherigen Entscheidungen und ihre Konsequenzen. Ein Fortschritts-Balken, welcher z.B. beim Registrierungsprozess die Stärke eines Passworts illustriert oder die Menge der eingegebenen Daten im Profil widerspiegelt, ist ein Beispiel für einen Feedback-Nudge. Hier bewegen solche Nudges Individuen spielerisch dazu, ein komplexeres Passwort zu wählen oder weniger Daten im System zu hinterlegen (Khern-am-nuai et al. 2017). Das Design der Nudges, also die Art und Weise ihrer Darstellung, ist bei diesen Nudges ausschlaggebend für eine erfolgreiche Intervention. Besonders effektiv sind hier Textbenachrichtigungen ohne Ton, welche die User-Experience nicht einschränken (Micallef et al. 2017).

Zeitverzögerung

Das „Hyperbolic Discounting" beschreibt die Tendenz eines Individuums, den unmittelbaren Nutzen einer Handlung zu überschätzen und später eintretende Kosten zu unterschätzen. Dies kann dazu führen, dass bei digitalen Entscheidungen über die persönliche Privatheit risikoreiche und wenig durchdachte Entscheidungen getroffen werden, ohne die späteren Konsequenzen der Handlung zu bedenken. Diesem Prozess kann mit Hilfe von Zeitverzögerungen als Privacy Nudges entgegengewirkt werden (Wang et al. 2014). Beispielsweise wird ein Countdown von fünf Sekunden eingesetzt, bevor eine Nachricht mit riskanten Inhalten im Firmennetzwerk veröffentlicht wird. Während dieser Zeit besteht die Möglichkeit das Senden der Nachricht abzubrechen und diese zu bearbeiten oder die Wartezeit zu beenden und die Nachricht direkt zu senden. Ziel des Nudges ist es, das Individuum dazu zu bewegen, weniger impulsiv zu handeln und den Inhalt der Nachricht sowie mögliche negative Konsequenzen zu überdenken. Die hohe Effektivität dieses Nudges sollte mit den potentiellen negativen Effekten wie z.B. einer erhöhten kognitiven Last abgewogen werden (Hu et al. 2017).

Soziale Norm

Individuen orientieren sich oftmals an dem Verhalten ihrer Mitmenschen, wenn sie Entscheidungen treffen müssen. Dies gilt auch für digitale Entscheidungen, welche die Privatheit der Individuen betreffen. Auf diesem Prinzip der sozialen Normen basiert die Wirkung von sogenannten sozialen Nudges (Coventry et al. 2016, Chang et al. 2016). Wenn ein Individu-

um beispielsweise die Information erhält, dass 75% seiner Kollegen die private Telefonnummer nicht im Arbeitsprofil angegeben haben, zieht der individuelle Nutzende diese Information als Referenzpunkt für sein eigenes Handeln heran (Ankerheuristik). Die Wirksamkeit dieses Nudges kann laut einer Studie zu Social Nudges jedoch auch umgekehrt wirken und Individuen dazu veranlassen, mehr persönliche Daten preiszugeben. Falls die Mehrheit den Zugriff einer App auf bestimmte Daten zulässt, könnten Individuen dazu verleitet werden, sich ebenso zu verhalten (Zhang/Xu 2016). Es ist deshalb wichtig, diese Nudges mit Bedacht zu verwenden, um Individuen zu besseren Entscheidungen bezüglich des Schutzes ihrer Daten zu bewegen.

2.3 Rechtliche Perspektive auf das Nudging

Das Grundkonzept des Nudgings wurde in Auseinandersetzung mit imperativen Formen der (rechtlichen) Regulierung entwickelt; nicht umsonst ist einer der Väter der Idee, Cass Sunstein, Rechtswissenschaftler. Schon in seinen Untersuchungen, aber auch in der deutschen Diskussion (zuletzt z.B. Gerg 2019), wird als rechtliches und ethisches Grundproblem des Nudgings die Gefahr der Bevormundung, des Paternalismus, hervorgehoben. Ein solches Vorgehen kann prinzipiell gerechtfertigt werden, wenn es dem Schutz Dritter oder anerkannten Gemeinwohlinteressen (z.B. dem Umweltschutz) dient. Es wird aber problematisch, wenn es zu erzieherischen Zwecken eingesetzt wird. Sunstein begegnet entsprechenden Vorwürfen mit dem Konzept des „libertären", also freiheitswahrenden Paternalismus und hebt hervor, die Entscheidungsfreiheit des Einzelnen werde im Ergebnis nicht behindert, sondern sogar befördert, weil er „gestupst" werde, Entscheidungen zu fällen, die seinen Interessen dienen. Freilich wird das Paternalismus-Problem damit nur auf eine andere Ebene verschoben: Die Entscheidung, was im Interesse des einzelnen Betroffenen ist, wird von Dritten (politische Entscheider, Unternehmen, Programmierer oder andere Akteure) getroffen. Ob und gegebenenfalls unter welchen Voraussetzungen dieses Vorgehen rechtlich akzeptabel ist, ist weiterhin Gegenstand grundsätzlicher Kontroversen.

Bezogen auf das Datenschutzrecht und den Sonderfall der Privacy Nudges bedeutet dies: Gerade mit Blick auf die verfassungsrechtliche Fundierung im Recht auf informationelle Selbstbestimmung ist es prinzipiell problematisch, Nutzenden ein – dann nicht selbst-, sondern eben fremdbestimmtes – Maß an Datenschutz vorzugeben, also eine „Privatheit wider Willen" (Sandfuchs 2015). Einen Ansatz zur Rechtfertigung bildet ein Be-

gründungsstrang des Bundesverfassungsgerichts im Volkszählungsurteil von 1983, in dem es das Recht auf informationelle Selbstbestimmung (auch) als „elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens" bezeichnet hat. Aus dieser Gemeinwohlfundierung lässt sich zumindest ein grundsätzliches Argument für einen Privatheitsschutz auch ohne oder sogar gegen den Willen des Individuums ableiten, das aber noch weiterer Ausarbeitung bedarf. Ähnliches gilt für das Ziel des Schutzes Dritter, das etwa eingreifen könnte, wenn in bestimmten Situationen die reale Gefahr besteht, dass eine unreflektierte massenhafte Datenpreisgabe Dritte unter Druck setzt, ebenfalls auf ihre Privatheit zu verzichten.

Jenseits solcher übergeordneten Interessen und Schutzaufgaben ist es dem liberalen Rechtsstaat grundsätzlich verwehrt, seine Bürgerinnen und Bürger vor sich selbst zu schützen oder sogar zu erziehen (Hillgruber 1992, Schwabe 1998, Krönke 2016). Informationelle „Selbst"-Bestimmung impliziert zumindest grundsätzlich auch das Recht, sorglos mit seinen Daten umzugehen, solange die erwähnten Grenzen des Gemeinwohls und der Rechte Dritter nicht überschritten werden. Dies gilt allerdings nur mit einer wichtigen Ausnahme: Das Recht kennt in vielen Bereichen Instrumente zum Schutz von Minderjährigen und einwilligungsunfähigen Personen vor sich selbst, hier also derjenigen, die ihre Privatheit zwar selbstbestimmt preisgeben, bei denen es aber in dieser Frage aus rechtlicher Sicht an der Entscheidungskompetenz fehlt (Sandfuchs 2015).

Der letzte Punkt ist für die DSGVO von besonderer Bedeutung, weil diese an vielen Stellen explizit die besondere Vulnerabilität von Minderjährigen und den daraus resultierenden hohen Schutzbedarf hervorhebt (Art. 6 Abs. 1 UAbs. 1 lit. f, Art. 8, Art. 12 Abs. 1, Art. 17 Abs. 1 lit. f, Erwägungsgründe 38, 58, 65, 71 und 75). Insofern eröffnet sich im Bereich von Online-Angeboten, die sich spezifisch an Minderjährige richten (sowie bei der schulischen Bildung) ein nicht nur sinnvolles, sondern auch rechtlich abgesichertes Einsatzfeld für Privacy Nudges.

Mit Blick auf die erwähnten Schutzziele wird man auch im Übrigen davon ausgehen müssen, dass Privacy Nudges, die keine übermäßige Willenseinschränkung beinhalten (bei denen der Betroffene also zwar gegebenenfalls mit etwas Aufwand, aber grundsätzlich problemlos alternative Handlungsoptionen wählen kann), nicht in unzulässiger Weise in die Autonomie der Grundrechtsträger eingreifen. Wenn also die DSGVO in den Art. 12 ff. die Informationspflichten der Verantwortlichen erheblich ausgeweitet und damit – wenn man so will – Informations-Nudges vorgibt, so ist dies unproblematisch, solange der Nutzende nicht gezwungen wird,

sich im Detail und ungebührlich lange mit den Informationen zu befassen. Es dient sogar umgekehrt dem anerkennenswerten Ziel, eine uninformierte, und damit nicht selbstbestimmte Preisgabe der Privatheit zu verhindern, und damit dem Schutz der Selbstbestimmung (Sandfuchs 2015).

Es ist aus demselben Grund nicht grundrechtlich problematisch, wenn der europäische Gesetzgeber in Art. 25 Abs. 2 DSGVO eine Pflicht zu privatheitsfreundlichen Voreinstellungen vorgibt und damit verbindlich die Verwendung von Default Nudges anordnet (Schomberg et al. 2019). Dies gilt zumindest, solange es dem Nutzenden nicht durch die Gestaltung der Oberfläche unverhältnismäßig erschwert wird, die Voreinstellungen nach seinen eigenen Präferenzen zu verändern.

Im Ergebnis ist der Einsatz von Privacy Nudges damit im Falle von Art. 25 Abs. 2 DSGVO verpflichtend und in vielen anderen Szenarien der technischen Gestaltung von IT-Systemen ein sinnvolles Instrument zum Schutz der Privatheit der Nutzenden, wenn es in geeigneter Weise ihre Selbstbestimmung fördert und z.B. das Problem des Privacy Paradoxes adressiert (Sandfuchs/Kapsner 2018). Nudges können auch ein Instrument sein, um die Datenschutzgrundsätze des Art. 5 DSGVO umzusetzen und im Sinne der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) diese Umsetzung nachzuweisen. Es handelt sich also – je nach Ausgestaltung – um technische und/oder organisatorische Maßnahmen, die der Verantwortliche nach dem Grundsatz des Datenschutzes durch Technikgestaltung (Art. 25 Abs. 1 DSGVO) ergreifen muss. Hierbei besteht zwar keine Pflicht zum Einsatz von Nudges, weil es insoweit einen Einschätzungs- und Auswahlspielraum des Verantwortlichen gibt. Edukative Nudges könnten in Zukunft hierbei aber eine relevante Rolle spielen.

3. Lernen durch edukatives Nudging

Eine lernförderliche Gestaltung von Privacy Nudges kann einen Lernprozess und das Verhalten von Lernenden kurz-, mittel- und langfristig anregen und Datenkompetenz aufbauen. Um eine langanhaltende Verhaltensänderung in Richtung auf Privatheit förderndes Verhalten zu erzielen, ist es notwendig, Lernende zum Lernen anzuregen und sie in ihrem Lernprozess aktiv zu unterstützen. Im Folgenden werden verschiedene Theorien dafür diskutiert, welche Prozesse für langanhaltendes Lernen verantwortlich sind. Die bedeutendsten werden kurz vorgestellt, in Beziehung zu den Privacy-Nudges gestellt und hinterfragt, ob nicht auch Nudges in der Lage sind, langanhaltende Verhaltensänderungen herbei zu führen.

3.1 Behavioristische Lerntheorie

Die behavioristische Lerntheorie geht davon aus, dass ein Individuum durch einen Reiz oder eine Stimulation zu einer Reaktion veranlasst wird. Durch externes positives oder negatives Feedback wird diese Reaktion entweder verstärkt oder aber abgeschwächt und die Wahrscheinlichkeit derselben Reaktion bei erneuter Präsentation des Reizes oder Stimulus steigt oder sinkt (Skinner 1954). In Bezug auf Nudges kann hier bei dem externen Feedback angesetzt werden und beispielsweise durch Smileys ein positives oder negatives Feedback die Reaktion verstärken oder abschwächen. Dementsprechend müsste der Nudge wiederholt eingesetzt werden, um einen langfristigen Lerneffekt hervorzurufen. Auf Basis der behavioristischen Lerntheorie kann argumentiert werden, dass auch Nudges durch Wiederholung zu einem Lerneffekt und anhaltender Verhaltensänderung beitragen. Gleichzeitig sollte aber Erwähnung finden, dass insbesondere behavioristisches Lernen dem libertären Gedanken und der eigenen Entscheidungsfreiheit entgegensteht.

3.2 Kognitivistische Lerntheorie

Anders als die behavioristische Lerntheorie richtet die kognitivistische Lerntheorie den Fokus weniger auf das sichtbare Verhalten, sondern auf kognitive Informationsverarbeitungsprozesse. Diese Theorie postuliert, dass ein Individuum Informationen aktiv aufnimmt, diese verarbeitet, zu innerlich repräsentierten Wissenseinheiten abspeichert und dann an bereits vorhandenes Wissen anknüpft (Rösler 1983). Bei direkter Rückmeldung dienen die dabei übermittelten Informationen weniger als Verstärker, sondern eher als Informationsquelle für das Individuum (Krapp/Weidenmann 2001). Als Nudge könnten dem Individuum genauere Informationen über die Bedeutung von Privatheit mitgeteilt werden, sodass das Individuum die Informationen auf den Umgang mit seinen eigenen Daten beziehen kann. Durch die kognitive Verarbeitung der Nudge-Informationen sind Informationen im Langzeitgedächtnis gespeichert. Eine Wiederholung der Informationen würde den Lerneffekt dennoch verstärken und festigen. Diese Art der Nudges könnte man den edukativen Nudges zuordnen, da hier eine Veränderung der Kognitionen oder des Wissenstandes zu einer Verhaltensänderung führt.

3.3 Sozial-kognitive Lerntheorie

Die sozial-kognitive Lerntheorie Albert Banduras, auch Modelllernen genannt, kann in vier Phasen unterteilt werden und beginnt mit der Aufmerksamkeitsphase, in welcher das Individuum seine Aufmerksamkeit auf ein Modell lenkt und dessen Handlungen beobachtet (Janson et al. 2017). In der zweiten Phase speichert das Individuum die zuvor beobachteten Handlungen im Gedächtnis ab und ahmt diese in der dritten Phase nach, indem die Handlungen aus dem Gedächtnis reproduziert werden. In der vierten Verstärkungs- und Motivationsphase werden die nachgeahmten Handlungen des Individuums verstärkt, sobald ein Erfolg wahrgenommen wird (Bandura 1977). Nudges, welche Privatheit förderndes Verhalten modellieren und entsprechende soziale Normen aufnehmen, eignen sich im Rahmen dieser Lerntheorie besonders. Hier ist beispielsweise das Vorleben (Gupta/Bostrom 2013) von privatheitsfreundlichen Einstellungen durch Freunde und andere soziale Bezugsgruppen zu nennen, wonach sich Individuen richten können. Auch hier ist eine Wiederholung zur besseren Einprägung förderlich und die wiederholte Durchführung des Verhaltens kann dazu beitragen, dass das gewünschte Verhalten eine Gewohnheit für das Individuum wird (Bandura 1997). System 1 (s. 2.1 Denkmodi im Nudging) übernimmt die gewünschte Verhaltensoption und speichert diese als Standardverhalten ab.

3.4 Konstruktivistische Lerntheorie

Der konstruktivistische Ansatz definiert Lernen als individuellen und aktiven Prozess des Individuums. Der Fokus liegt auf individuellen, konstruktiven Prozessen in sozialen Interaktionen. Das bedeutet, dass das Wissen nicht von einer Person auf eine andere übertragen werden kann, sondern von jedem Individuum neu konstruiert wird. Anhand von Informationen schafft jedes Individuum sich eine subjektive Realität, welche stark von der individuellen Prägung abhängig ist. Die Informationen erhalten Bedeutung durch den Bezug zu relevanten Kontexten (Janson et al. 2019). Wichtig sind hierbei die intrinsische Motivation des Individuums, die Inhalte lernen zu wollen, das Vorwissen (Thiel de Gafenco et al. 2018), sein kultureller Hintergrund (Ernst et al. 2018) und seine Erfahrungen. Nudges, welche kognitive Prozesse anstoßen, sind in Bezug auf diese Theorie von Bedeutung. Ähnlich wie bei dem kognitivistischen Ansatz ist auch hier der Nudge repräsentativ im Gedächtnis gespeichert und eine Wiederholung würde den bestehenden Lerneffekt festigen und verstärken. Nudges, welche in diesem Kontext von Bedeutung sind, sind ebenfalls die edukativen Nudges.

4. Edukative Privacy Nudges im digitalen Umfeld

Im Folgenden soll nun ergänzend dargestellt werden, wie die oben vorgestellten Lernprozesse in Zusammenhang mit den Privacy Nudges zu langanhaltenden Verhaltensänderungen führen können. Zur Übersicht wurden die Nudges nach den zugrundeliegenden Lerntheorien geordnet.

Default und Framing

Die Default- und Framing-Nudges können durch behavioristische Prozesse anhaltende Verhaltensänderung herbeiführen. Der Reiz, auf den eine Reaktion des Individuums folgt, wird im Vorhinein so modifiziert, dass bei diesen Nudges bereits die gewünschte Reaktion durch den Reiz angestoßen wird. Bei Default-Nudges ist dies die Standardeinstellung, welche oftmals ohne Änderung angenommen wird und jedenfalls dann als Reiz wirkt, wenn sie zuvor wahrgenommen (also nicht nur „weggeklickt") wird. Die Framing-Nudges lenken mit Hilfe von Farbelementen die Aufmerksamkeit des Individuums auf die gewünschte Reaktion (Schomberg et al. 2019). Durch die daraus entstehenden privatheitsfreundlichen Auswirkungen seines Handelns erfährt das Individuum ein positives Feedback seines Verhaltens, und dieses wird verstärkt. Die Wahrscheinlichkeit, dass das Individuum das gewünschte Verhalten in Zukunft erneut ausführt, steigt (Skinner 1954).

Information und Feedback

Informations- und Feedback-Nudges können als unterstützende Elemente im Lernprozess für den Behaviorismus und den Kognitivismus eingeordnet werden. Das Individuum erhält eine direkte Reaktion auf seine Handlung, welche in Form von positivem Feedback verstärkend oder in Form von negativem Feedback abschwächend sein kann (Skinner 1954). So könnte ein Informationssystem beispielsweise am Ende jedes Tages ein klares Feedback darüber bereitstellen, wie viele Daten das Individuum geteilt hat und was dies bedeutet (Almuhimedi et al. 2015). Aus kognitivistischer Perspektive besitzen beide Ansätze ebenfalls das Potenzial, eine anhaltende Verhaltensänderung herbeizuführen. Das Individuum hat die Möglichkeit, die durch das Feedback erhaltenen Informationen zu verarbeiten, in bestehende Wissensstrukturen einzuordnen und abzuspeichern. Es ist so in der Lage, das erworbene Wissen zu abstrahieren und auf andere Kontexte anzuwenden (Krapp/Weidenmann 2001).

Soziale Norm

Zu den Nudges, welche sich das Konzept der sozialen Norm zu Nutze machen, gehören jene, die dem Individuum soziale Normen spiegeln und solche, die das gewünschte Verhalten modellieren. Beide Arten gehören sowohl zum Kognitivismus als auch zum sozial-kognitiven Lernen. Wird das gewünschte Verhalten modelliert, hat das Individuum die Chance, das beobachtete privatheitsfreundliche Verhalten des Modells zu übernehmen und so eigene negative Erfahrungen zu umgehen (Bandura 1977). Die Informationen über die Auswirkungen des Verhaltens des Modells kann es so abspeichern und in Zukunft auf sein eigenes Verhalten übertragen. Werden soziale Normen zum Gegenstand des Nudgings, kann das Individuum das privatheitsfreundliche Verhalten, welches für einen Großteil der Personen leitend ist, als Referenzpunkt für seine eigenen Handlungen nutzen und hat so ebenfalls ein Modell zur Verfügung.

Tabelle 2: Nudges und Lerntheorien

Nudge	**Lerntheorie**	**Mögliche Effekte für privatheitsfreundliches Verhalten**
Default	Behavioristische Lerntheorie	Keine Änderungen des Default Settings
Framing (Präsentation)	Behavioristische Lerntheorie	Die Auswahl nehmen, die farblich als privatheitsfreundlich hervorgehoben ist
Feedback	Behavioristische Lerntheorie, kognitivistische Lerntheorie	Rückmeldung über das Verhalten so lange bis das System meldet, dass privatheitsfreundliche Einstellungen vorliegen
Information	Behavioristische Lerntheorie, kognitivistische Lerntheorie	Die Option wählen, die entsprechend positive privatheitsfreundliche Konsequenzen aufzeigt
Soziale Einflüsse	Kognitivistische Lerntheorie, sozial-kognitive Lerntheorie	Die privatheitsfreundliche Einstellung nehmen, die die Mehrheit anderer Leute genutzt hat
Nudging, das kognitive Prozesse anregt	Konstruktivistische Ansatz	Langzeiteffekte, die mit Emotionen, Erfahrungen und der Entwicklung einer Meinung verbunden sind

Nudges, die kognitive Prozesse auslösen

Wenn Nudges in Form von Hinweisen verwendet werden, lösen diese kognitive Prozesse aus und können der konstruktivistischen Lerntheorie zu geordnet werden (siehe Tabelle 2 für den Vergleich der Theorien). Derartige Nudges induzieren Emotionen und Erfahrungen und generieren Bedeutung. Es wird davon ausgegangen, dass hierbei stabile Langzeiteffekte nachweisbar sind (Krapp/Weidenmann 2001).

Aufbauend auf der Beschreibung der einzelnen Nudges und der Lerntheorien, bietet die nachfolgende Tabelle einen Einblick in die Zusammenhänge zwischen den verschiedenen Nudges, den Lerntheorien und möglichen Verhaltenseffekten.

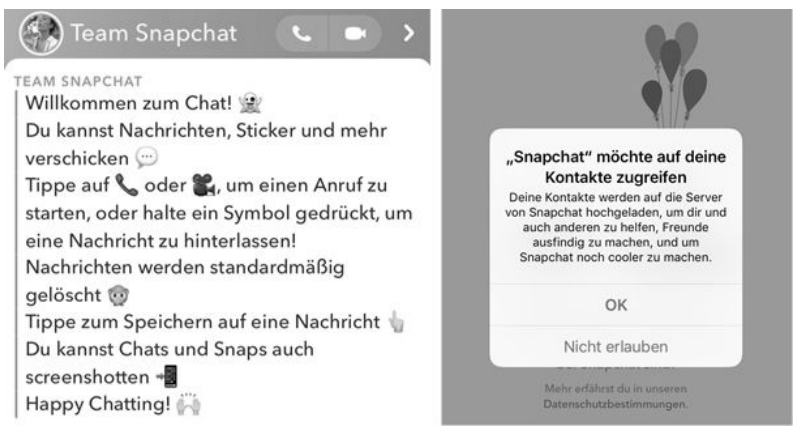
Um den Einsatz der Nudges besser verstehen zu können, dient das nachfolgende Beispiel als Grundlage.

5. Ansatzmöglichkeiten zu edukativen Nudges am Beispiel von Snapchat

Snapchat ist ein sogenannter Instant-Messaging Dienst, der auf mobilen Endgeräten genutzt werden kann und es Nutzenden ermöglicht, Fotos und andere Medien für eine bestimmte Anzahl von Sekunden an andere Nutzende zu senden, bis die gesendeten Medien verschwinden.

Innerhalb von Snapchat gibt es zahlreiche Ansätze des Einsatzes von Nudges, mit denen Nutzende auf eine edukative Weise angeregt werden, ihr Verhalten zu verändern. Gleichzeitig zeigt die aktuelle Applikation aber, dass von diesen Möglichkeiten kaum Gebrauch macht wird. Abbildung 1 zeigt zwar Informationen zur Nutzung an, nudged aber zum bewussten Freigeben der Kontakte durch ein Framing, wobei der „Ok"-Button im Gegensatz zu dem „Nicht Erlauben"-Button hervorgehoben wird (bedingt durch das Betriebssystem Apple IOS).

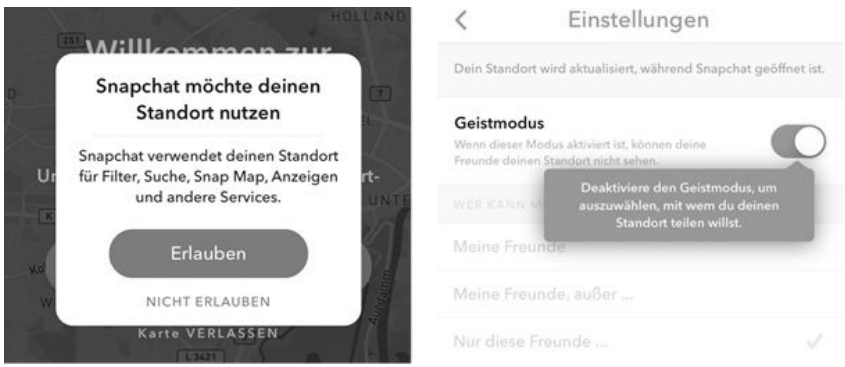
Abbildung 1. Informationsnudge



Quelle: Eigene Screenshots aus Snapchat App, Snap, Inc., https://apps.apple.com/de/app/snapchat/id447188370

Innerhalb der Einstellungen verwendet Snapchat zwei weitere Nudges zum Standort teilen (siehe Abbildung 2). So wird bewusst die Entscheidung der Standortnutzung zum „Erlauben" angestupst, gleichzeitig wird aber auch ein privatheitsfreundlicher Default implementiert, indem das Teilen des öffentlichen Standorts durch den sogenannten „Geistmodus" abgeschaltet wird. Beiden Nudges gemein ist, dass die edukativen Aspekte im Hintergrund sind.

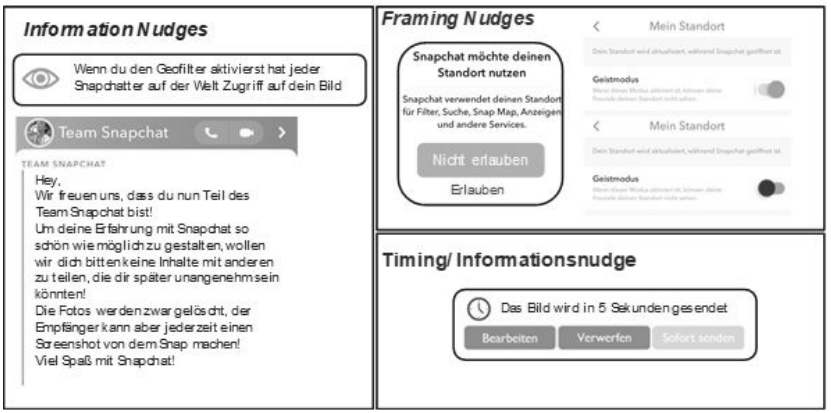
Abbildung 2: Information und Default Nudge



Quelle: Eigene Screenshots aus Snapchat App, Snap, Inc., https://apps.apple.com/de/app/snapchat/id447188370

Bis auf die Default Option sind die Einstellungen und der Umgang mit den Daten von Snap Chat Nutzenden durchaus als fragwürdig zu beurteilen, was den Schutz von Nutzerdaten angeht. Durch einfache Änderungen und Integration von Nudges können Nutzende jedoch edukativ so geschult werden, dass diese sensibler mit ihren Daten umgehen. Mögliche Beispiele, wie Snapchat seine Benutzeroberfläche privatheitsfreundlicher gestalten könnte, werden in Abbildung 3 vorgestellt.

Abbildung 3: Mögliche privatheitsfreundliche Anpassungen von Snapchat (eigenes Beispiel für mögliche Erweiterungen)



Basierend auf: Eigene Screenshots ais Snapchat App, Snap, Inc., https://apps.apple.com/de/app/snapchat/id447188370

Wie bereits zuvor vorgestellt, wäre die einfachste Option der Einsatz eines Informationsnudges in Kombination mit Framing. Anstelle der aus Sicht der Privatheit bedenklichen Option, sollte dann die privatheitsfreundliche hervorgehoben werden. Durch das Framing kann auch die sogenannte Geisterfunktion in Bezug auf die Privatheit verbessert werden, also die Nutzung des Systems ohne permanentes Teilen des eigenen Standorts. Hier kann die rote Farbe ein nicht privatheitsfreundliches Verhalten indizieren, die grüne hingegen ein privatheitsfreundliches Verhalten. Um das Grundprinzip des Versendens von Bildern besser zu steuern, könnte eine Zeitverzögerung an einen Informationsnudge gekoppelt werden, sodass dem Nutzenden noch einmal bewusst gemacht wird, was für ein Bild er dort teilt.

6. Zusammenfassung und Würdigung

Edukatives Privacy Nudging gewinnt immer mehr an Bedeutung. Besonders die vermehrte Preisgabe von Daten in Online Umgebungen erfordert, Individuen für einen anhaltenden achtsamen Umgang mit privaten Daten zu sensibilisieren. Hier kann das Konzept des digital Nudgings angewandt werden, welches als edukatives Nudging einen klaren Bezug zum Lernen herstellen kann. Nudges wie Defaults basieren beispielsweise auf der beha-

vioristischen Lerntheorie und können durch ihren Einsatz Individuen dazu anregen, vorsorglicher zu agieren. Soziale Einflüsse hingegen können durch die Demonstration von Handlungsweisen anderer Individuen, basierend auf der sozial kognitiven und der kognitivistischen Lerntheorie, dazu beitragen, dass Individuen durch das Verhalten anderer Nutzender lernen, sich selbst privatheitsfreundlicher zu verhalten. Dieser Beitrag zeigte daher verschiedene edukative Privacy Nudges auf und bietet somit einen Ansatzpunkt für Forscher und Praktiker edukative Privacy Nudges zu gestalten. Limitiert ist dieser Beitrag durch die fehlende empirische Demonstration der Effektivität von edukativen Privacy Nudges, was jedoch einen Raum für künftige Forschungsstudien bieten kann, beispielsweise hinsichtlich der zielgruppenspezifischen Gestaltung durch spielerische Nudges (Schöbel et al. 2020b).

Danksagung

Dieser Beitrag wurde im Rahmen des Projekts „Nudger“ (www. nudger.de; Förderkennzeichen: 16KIS0890K; 16KIS0891) unter der Projektträgerschaft des VDI/VDE-IT erarbeitet und mit den Mitteln des Bundesministeriums für Bildung und Forschung gefördert. Zudem danken wir Melanie Schwede für die initiale Mitarbeit an der Beitragsidee. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Literatur

Acquisti, Alessandro (2009): *Nudging privacy: The behavioral economics of personal information*. In: IEEE security & privacy 7 (6), S. 82–85.

Acquisti, Alessandro / Brandimarte, Laura / Loewenstein, George (2015): *Privacy and human behavior in the age of information*. In: Science (New York, N.Y.) 347 (6221), S. 509–514. doi:10.1126/science.aaa1465.

Acquisti, Alessandro / Adjerid, Idris / Balebako, Rebecca / Brandimarte, Laura / Cranor, Lorrie F. / Komanduri, Saranga / Leon, Pedro G. / Sadeh, Norman / Schaub, Florian / Sleeper, Manya / Wang, Yang / Wilson, Shomir (2017): *Nudges for privacy and security*. In: ACM Comput. Surv. 50 (3), S. 1–41. doi:10.1145/3054926.

Adjerid, Idris / Acquisti, Alessandro / Loewenstein, George (2019): *Choice architecture, framing, and cascaded privacy choices.* In: Management Science 65 (5), S. 2267–2290. doi:10.1287/mnsc.2018.3028.

Almuhimedi, Hazim / Schaub, Florian / Sadeh, Norman / Adjerid, Idris / Acquisti, Alessandro / Gluck, Joshua / Cranor, Lorrie F. / Agarwal, Yuvraj (2015): *Your location has been shared 5,398 times!: A field study on mobile app privacy nudging*. In: Proceedings of the 33rd annual ACM conference on human factors in computing systems, S. 787–796.

Bandura, Albert (1977): *Social learning theory*. Englewood Cliffs: Prentice-Hall.

Bandura, Albert (1997): *Self-efficacy. The exercise of control*. New York: W.H. Freeman.

Chang, Daphne / Krupka, Erin L. / Adar, Eytan / Acquisti, Alessandro (2016): *Engineering information disclosure. Norm shaping designs*. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: Association for Computing Machinery (CHI '16), S. 587–597. doi:10.1145/2858036.2858346.

Coventry, Lynne. M. / Jeske, Debora / Blythe, John M. / Turland, James / Briggs, Pam (2016): *Personality and social framing in privacy decision-making: A study on cookie acceptance.* In: Frontiers in Psychology 7, S. 1–12.

Enough, Birte / Mussweiler, Thomas (2001): *Sentencing under uncertainty. Anchoring effects in the courtroom*. In: J Appl Soc Psychol 31 (7), S. 1535–1551. doi:10.1111/j.1559-1816.2001.tb02687.x.

Ernst, Sissy-Josefina / Janson, Andreas / Söllner, Matthias / Leimeister, Jan Marco (2018): *Mobiles Lernen in praktischen Trainings. Lernzielerreichung vor dem Hintergrund von Motivation und Akzeptanz der Zielgruppe.* In: de Witt, Claudia / Gloerfeld, Christina (Hg.): Handbuch Mobile Learning. Wiesbaden: Springer VS, S. 409–431.

Gerg, Stephan (2019): *Nudging. Verfassungsrechtliche Maßstäbe für das hoheitliche Einwirken auf die innere Autonomie des Bürgers*. Tübingen: Mohr Siebeck (5).

Günther, Wendy Arianne / Rezazade Mehrizi, Mohammad H./ Huysman, Marleen / Feldberg, Frans (2017): *Debating big data. A literature review on realizing value from big data.* In: The Journal of Strategic Information Systems 26 (3), S. 191–209. doi:10.1016/j.jsis.2017.07.003.

Gupta, Saurabh / Bostrom, Robert (2013): *An investigation of the appropriation of technology-mediated training methods incorporating enactive and collaborative learning*. In: Information Systems Research 24 (2), S. 454–469. doi:10.1287/isre.1120.0433.

Heidbrink, Ludger / Klonschinski, Andrea (2018): *Nudges, Transparenz und Autonomie – Eine normativ gehaltvolle Kategorisierung von Maßnahmen des Nudgings*. In: Vierteljahrshefte zur Wirtschaftsforschung 87 (1), S. 15–27. doi:10.3790/vjh.87.1.15.

Hertwig, Ralph / Grüne-Yanoff, Till (2017): *Nudging and boosting. Steering or empowering good decisions.* In: Perspectives on Psychological Science: A Journal of the Association for Psychological Science 12 (6), S. 973–986. doi:10.1177/1745691617702496.

Hillgruber, Christian (1992): *Der Schutz des Menschen vor sich selbst*. München: Vahlen.

Hu, Paul Jen-Hwa / Hu, Han-fen / Fang, Xiao (2017): *Examining the mediating roles of cognitive load and performance outcomes in user satisfaction with a website: A field quasi-experiment*. In: MIS Quarterly 41 (3), S. 975–987.

Hummel, Dennis / Maedche, Alexander (2019): *How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies*. In: Journal of Behavioral and Experimental Economics 80, S. 47-58. doi:10.1016/j.socec.2019.03.005.

Janson, Andreas / Söllner, Matthias / Leimeister, Jan Marco (2017): *Individual appropriation of learning management systems — Antecedents and consequences*. In: *A*IS Transactions on Human-Computer Interaction 9 (3), S. 173–201.

Janson, Andreas / Söllner, Matthias / Leimeister, Jan Marco (2020): *Ladders for learning. Is scaffolding the key to teaching problem solving in technology-mediated learning contexts?* In: Academy of Management Learning & Education 19 (4), S. 439–468. doi:10.5465/amle.2018.0078.

Jones, Matthew (2019): *What we talk about when we talk about (big) data.* In: The Journal of Strategic Information Systems 28 (1), S. 3–16. doi:10.1016/j.jsis.2018.10.005.

Kahneman, Daniel (2011): *Thinking, fast and slow.* New York: Farrar, Straus and Giroux.

Khern-am-nuai, Warut / Yang, Weining / Li, Ninghui (2017): *Using context-based password strength meter to nudge users' password generating behavior: A randomized experiment*. In: Hawaii International Conference on System Sciences 2017 (HICSS-50). Online verfügbar unter: https://www.researchgate.net/publication/317120932_Using_Context-Based_Password_Strength_Meter_to_Nudge_Users%27_Password_Generating_Behavior_A_Randomized_Experiment (Abfrage am: 6.10.2020).

Krapp, Andreas / Weidenmann, Bernd (Hg.) (2001): *Pädagogische Psychologie*: Weinheim: Beltz.

Krasnova, Hanna / Spiekermann, Sarah / Koroleva, Ksenia / Hildebrand, Thomas (2010): *Online social networks. Why we disclose.* In: Journal of Information Technology 25 (2), S. 109–125. doi:10.1057/jit.2010.6.

Krönke, Christoph (2016): *Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung*. In: Der Staat 55 (3), S. 319–351.

Kühling, Jürgen / Martini, Mario (2016): *Die Datenschutz-Grundverordnung. Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?* In: Europäische Zeitschrift für Wirtschaftsrecht (EuZW), S. 448–453.

Micallef, Nicholas / Just, Mike / Baillie, Lynne / Alharby, Maher (2017): *Stop annoying me!* In: Alessandro Soro (Hg.): OzCHI 2017 - Human Nature. Proceedings of the 29th Australian Computer-Human Interaction Conference (OzCHI 2017): Brisbane 28th November -1st December, 2017, the 29th Australian Conference. Brisbane, Queensland, Australia. New York City: The Association for Computing Machinery (ICPS), S. 371–375.

Mirsch, Tobias / Lehrer, Christiane / Jung, Reinhard (2018): *Making digital nudging applicable: The digital nudge design method*. In: ICIS 2018 Proceedings.

Rösler, Winfried (1983): *Alltagsstrukturen—kognitive Strukturen—Lehrstoffstrukturen. Zur phänomenologischen Kritik an der kognitivistischen Lerntheorie*. In: Zeitschrift für Pädagogik 29 (6), S. 947–960.

Sandfuchs, Barbara (2015): *Privatheit wider Willen? Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht*. Dissertation. Tübingen: Mohr Siebeck.

Sandfuchs, Barbara / Kapsner, Andreas (2018): *Privacy nudges: Conceptual and constitutional problems.* In: Burk, Steffen / Hennig, Martin / Heurich, Benjamin / Klepikova, Tatiana / Piesga, Miriam / Sixt, Manuela / Trost, Kai Erik (Hg.): Privatheit in der digitalen Gesellschaft. Berlin: Duncker & Humblot (Internetrecht und Digitale Gesellschaft, Band 10), S. 320–339.

Schöbel, Sofia / Barev, Torben / Janson, Andreas / Hupfeld, Felix / Leimeister, Jan Marco (2020a): *Understanding user preferences of digital privacy nudges – A best-worst scaling approach*. In: HICSS 2020 Proceedings, S. 3918–3927.

Schöbel, Sofia / Janson, Andreas / Jahn, Katharina / Kordyaka, Bastian / Turetken, Ozgur / Djafarova, Naza et al. (2020b): *A research agenda for the why, what, and how of gamification designs results on an ECIS 2019 panel.* In: CAIS 46. doi:10.17705/1CAIS. 04630.

Schomberg, Sabrina / Barev, Torben Jan / Janson, Andreas / Hupfeld, Felix (2019): *Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld. Datenschutz durch Nudging*. In: Datenschutz und Datensicherheit 43 (12), S. 774–780. doi:10.1007/s11623-019-1204-5.

Schwabe, Jürgen (1998): *Der Schutz des Menschen vor sich selbst*. In: JuristenZeitung, S. 66–75.

Skinner, Burrhus Frederic (1954): *The science of learning and the art of teaching*. In: Harvard Educational Review 24, S. 86–9.

Smith, H. Jeff / Dinev, Tamara / Xu, Heng (2011): *Information privacy research. An interdisciplinary review*. In: MIS Quarterly 35 (4), S. 989–1015.

Thaler, Richard H. / Sunstein, Cass R. (2008): *Nudge. Improving decisions about health, wealth, and happiness*. New Haven, Conn.: Yale Univ. Press. Online verfügbar unter http://www.loc.gov/catdir/enhancements/fy0833/2007047528-b.html (Abfrage am: 6.10.2020).

Thiel de Gafenco, Marian / Janson, Andreas / Schneider, Tim (2018): *KoLeArn – Smarte und kontextsensitive Aus- und Weiterbildung für die chinesische Industrie*. In: DeLFI 2018 Proceedings.

Turland, James / Coventry, Lynne / Jeske, Debora / Briggs, Pam / van Moorsel, Aad (2015): *Nudging towards security. Developing an application for wireless network selection for android phones.* In: Proceedings of the 2015 British HCI Conference. New York, NY, USA: Association for Computing Machinery (British HCI '15), S. 193-201. doi:10.1145/2783446.2783588.

Tversky, Amos / Kahneman, Daniel (1974): *Judgment under uncertainty. Heuristics and biases*. In: Science (New York, N.Y.) 185 (4157), S. 1124–1131.

Wang, Yang / Leon, Pedro Giovanni / Acquisti, Alessandro / Cranor, Lorrie Faith / Forget, Alain / Sadeh, Norman (2014): *A field trial of privacy nudges for facebook*. In: Jones, Matt / Palanque, Philippe / Schmidt, Albrecht / Grossman, Tovi (Hg.): CHI 2014, one of a CHInd. Conference proceedings : Toronto, Canada, April 26 - May 1, 2014 ; the 32nd Annual ACM Conference on Human Factors in Computing Systems. Association for Computing Machinery. New York, NY: Assoc. for Computing Machinery, S. 2367–2376.

Weinmann, Markus / Schneider, Christoph / vom Brocke, Jan (2016): *Digital nudging*. In: Business & Information Systems Engineering 58 (6), S. 433–436. doi:10.1007/s12599-016-0453-1.

Zhang, Bo / Xu, Heng (2016): *Privacy nudges for mobile applications. Effects on the creepiness emotion and privacy attitudes.* In: Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing, S. 1676–1690.

Zuboff, Shoshana (2019): *The age of surveillance capitalism. The fight for the future at the new frontier of power*. London: Profile Books.

Datenschutz und Medienbildung – Chancen und Barrieren in der schulischen Praxis

Andreas D. Schulz

Abstract

Die Digitalisierung im Bildungswesen und die zunehmende Relevanz von digitalen Bildungsmedien wirft verstärkt Fragen des Datenschutzes auf. Schülerinnen und Schüler, Eltern und Lehrkräfte waren mit dem Inkrafttreten der Europäischen Datenschutz-Grundverordnung 2019 verunsichert, welche Informationen erhoben, verarbeitet und gespeichert werden können. In den Klassenräumen entfernten die Lehrer die Geburtstagskalender und auf Schulfesten vermied man Fotos. Mit den Datenschutzerklärungen und den Verzeichnissen von Verarbeitungstätigkeiten betreten die Lehrkräfte Neuland. Die Digitalisierung der Bildung verändert nicht nur die Art des Unterrichts und die Kompetenzvermittlung, sondern auch die Strukturen und Prozesse innerhalb der Schule. Welchen Einfluss hat die Datenschutz-Grundverordnung in der Schule und wie beeinflusst sie die Digitalisierung der Lehr- und Lernprozesse? Wie wirken die rechtlichen Anforderungen, die sich entwickelnde Daten-Ökonomie bzw. Internetwirtschaft sowie die Mediatisierung der Schulgemeinschaft auf die Organisation des Unterrichts und der Schule?

Einleitung

Die Schließung der Schulen im Frühjahr 2020 verliehen digitalen Lehr- und Lernformaten eine unvorhersehbare Aktualität und Bedeutung. Diese Entwicklung setzte sich mit dem digitalen Distanzunterricht im Winter 2021 fort und wird nachhaltig wirken. So wichtig der Start in das digitale Lernen auch war: Der Datenschutz spielte in dieser Zeit kaum eine Rolle (vgl. HKM 2020). Lehrerinnen und Lehrer erhielten in dieser Zeit kaum Hinweise, welche digitalen Lehr- und Lernangebote datenschutzkonform sind und wie die Datenschutzrechte der Schülerinnen und Schüler gewahrt werden können. Der Umgang der Schulen mit digitalen und datenschutzkonformen Lehr- und Lernangeboten variierte daher stark zwischen den Bundesländern.

So wurden die Schulen während der Schulschließungen scheinbar in die Zeit des digitalen Lernens katapultiert. Die „Verwaltungsvereinbarung DigitalPakt Schule 2019 bis 2024“ unterstützt mit 5,5 Mrd. Euro die Schulen nahezu zum richtigen Zeitpunkt. Tatsächlich ist es bis zur Umsetzung des DigitalPaktes aber noch ein weiter Weg. In vielen Schulen sind weder Vereinbarungen über anstehende Maßnahmen (z.B. Zielvereinbarungen zur Nutzung der digitalen Ausstattung im Rahmen didaktischer Medienkonzepte) noch Gelder zur Finanzierung einer (ausreichenden) Breitbandanbindung an das Internet angekommen. Der DigitalPakt scheint den Schulen eine Option für eine „didaktische Wende“ mit Hilfe digitaler Lehr- und Lernformate zu bieten. Die Umsetzung wird allerdings noch einige Zeit benötigen. Dennoch werfen die Erfahrungen aus den Schulschließungen im Frühjahr 2020 und im Winter 2021 Fragen in Hinblick auf die Notwendigkeit einer aktuellen und für alle nutzbaren digitalen Infrastruktur, didaktischen Medienkonzepten, Medienkompetenzen, Medienbildung sowie den Datenschutz auf. Die Digitalisierung der Schulen beeinflusst direkt die Realisierung des Grundrechtschutzes auf informationelle Selbstbestimmung von LehrerInnen und SchülerInnen. Die Art und Weise der Nutzung digitaler Lehr- und Lernformate tangiert somit auch den Datenschutz. Das Chatformat ZOOM hat beispielsweise gezeigt, wie unsicher und anfällig digitale Anwendungen für Störungen von außen, wie z.B. die Teilnahme unbekannter Dritter, sind. Das Verhältnis von Medienbildung und Datenschutz in den Schulen ist mehr als prekär. Dieser Beitrag wird daher der Frage nachgehen, vor welchen Herausforderungen die Schulen im Rahmen der Realisierung einer datenschutzkonformen Medienbildung stehen. Welche Anforderungen seitens der Medienbildung und des Datenschutzes werden an die Schulen[1] gestellt?

1. Datenschutzrechtliche Relevanz und Anforderungen an die Medienbildung

Welche Relevanz hat der Datenschutz in Schulen und welche Anforderungen müssen Schulen erfüllen? Die Frage nach der Relevanz des Datenschutzes in Schulen müsste eigentlich obsolet sein, denn die Mitglieder einer Schulgemeinschaft – Lehrkräfte, Eltern und Lernende – sind Bürger und Bürgerinnen, und sie haben daher natürlich alle Grundrechte wie auch das Recht auf informationelle Selbstbestimmung. Dennoch ergeben

1 Schule umfasst in diesem Beitrag alle Schulformen in Deutschland: z.B. Grundschulen, Haupt- und Realschulen, Gymnasien, berufliche Schulen etc.

sich aus der pädagogischen Tätigkeit, der Bildungsinstitution und dem Erziehungs- und Schutzauftrag der Schule bezüglich der Kinder und Jugendlichen besondere Anforderungen. Schaumburg (2015) nennt in ihrer Studie sechs Einflussgrößen der digitalen Medien auf den Unterricht und den Schulalltag, die den Datenschutz direkt tangieren:

Die Schule wird erstens zunehmend beeinflusst durch die individuellen medialen Erfahrungen und Praxen der Kinder und Jugendlichen. Die regelmäßig veröffentlichten KIM und JIM Studien (vgl. Südwest, M. F. 2018, 2019) zeigen den Medienwandel und Medienkonsum der nachwachsenden Generation. Mobile Geräte wie Smartphones und Tablets werden in der Nutzung immer wichtiger. Die Kommunikation mit Freunden über Messengerdienste, die Informationssuche, Video- und Musikdienste sowie Online-Spiele nehmen einen wichtigen Platz im Medienverhalten ein. Die Alltagswirklichkeit von Kindern und Jugendlichen ist demnach nicht nur medialer, sondern auch digitaler geworden.

Schulen und Bildungsverlage versuchen sich auf diese Entwicklung einzustellen und den Kindern und Jugendlichen digitale Lernmöglichkeiten bereitzustellen. Schon vor der Corona-Pandemie standen eine Reihe von digitalen Werkzeugen zur Diagnose des Lernstandes, Leseprogramme (z.B. Antolin), Lernprogramme und Lernapps zur Verfügung. Mit den Schulschließungen haben sich diese Werkzeuge und Lernoptionen relativ stark verbreitet. Bildungsverlage und Anbieter von Apps stellen einerseits mehr Materialien auch kostenlos online. Andererseits werden von den Lehrkräften, die für die Lernenden Online-Materialien suchen, auch mehr Materialien nachgefragt. Eine zunehmende Verbreitung finden auch Online-Tests zur Diagnose von Lernfortschritten, die ebenfalls personenbezogene Daten beinhalten. Daher ist die Entwicklung eines Medienbildungskonzeptes für die weitere Digitalisierung der Schulen ebenso wichtig wie ein angemessenes Datenschutzkonzept. Denn durch die Nutzung externer digitaler Angebote sind immer auch Dritte eingebunden, die personenbezogene Daten erheben. Die Lehrkräfte müssen sich daher überlegen, welche externen digitalen Angebote genutzt werden, ob diese datenschutzkonform hinsichtlich der DSGVO sind, wie viele Einverständniserklärungen sie den Erziehungsberechtigten zumuten wollen und wie sie diese organisatorisch bewältigen können.

Die Digitalisierung wirkt sich drittens auch auf die technische und organisatorische Entwicklung der Schule als Institution aus. Die Ausstattung mit mobilen Geräten, digitaler Präsentationstechnik und WLAN sind zurzeit die größten technischen Herausforderungen für die Schulträger. Damit verbunden sind erhebliche Anstrengungen hinsichtlich der institutionellen Strukturen und Abläufe, z.B. die Organisation der Zugänge in das

Internet, zu Lernplattformen und Schulportalen, die Umstellung der Administration und die Verteilung der digitalen Ressourcen und Geräte. Gleichzeitig mit dieser digitalen Vernetzung wächst auch hier der Bedarf an Datenschutzkonzepten.

Das oben beschriebene Medienverhalten von Kindern und Jugendlichen hat spezifische Ursachen. Neben der Kommunikation, Information und Entspannung nutzen die Heranwachsenden digitale Anwendungen auch zur Entwicklung ihrer eigenen Persönlichkeit. Entwicklungsaufgaben werden durch Kinder und Jugendliche zunehmend im Internet bearbeitet, wie z.B. die eigene Geschlechterrolle zu finden, ein eigenes Wertesystem aufzubauen, intellektuelle und soziale Kompetenzen auszubilden und einen eigenen Lebensstil zu entwickeln (vgl. Hurrelmann/Rosewitz/Wolf 1985). Der Erziehungsauftrag der Schule diffundiert in die digitale Welt hinein und wird um digitale Kompetenzen erweitert, nicht nur um Kindern und Jugendlichen vor den Risiken im Internet zu schützen, sondern um sie bei der Suche nach eigenen Werten und Normen, dem Erlernen sozialer Kompetenzen, der Entwicklung eines eigenen Lebensstils und letztlich einer eigenen Persönlichkeit zu unterstützen. Das eigene Verhalten im Internet zu überprüfen, sich vor Gefährdungen zu schützen, personenbezogene Daten sparsam im Internet zu verbreiten und in Grundzügen auch die Internet- und Datenökonomie zu verstehen, sind Anknüpfungspunkte für eine Datenschutzbildung, die Bestandteil der Medienbildung in den Schulen sein sollte.

Hiermit sind auch die Gefahren und Risiken angesprochen, die mit der Nutzung digitaler Medien einhergehen können. Kinder und Jugendliche müssen sich mit den kommerziellen Interessen der Internetunternehmen, mit Aggression und Gewalt, sexuellen Übergriffen, rassistischen und verzerrten Informationen und Ratschlägen im Internet auseinandersetzen. Spitzer (2018) stellt eine ganze Reihe von gesundheitlichen, psychischen und gesellschaftlichen Risiken für Kinder und Jugendliche vor, die mit der Nutzung von Smartphones und dem Internet einhergehen sollen. Auch wenn seine Darstellungen sehr einseitig und plakativ sind, Bildungsinstitutionen müssen sich zunehmend mit dem Nutzen und den Gefährdungspotenzialen digitaler Medien auseinandersetzen und hierfür Bildungsinhalte für Kinder und Jugendliche entwickeln.

Die geschilderte Verbreitung digitaler Medien in den Bildungsinstitutionen zeigt den Bedarf an Medienbildung, der mit höheren Anforderungen hinsichtlich des Datenschutzes und einer Datenschutzbildung korrespondiert. Neben diesen pädagogischen Herausforderungen müssen sich Schulleitungen und Lehrkräfte mit den bestehenden gesetzlichen Anforde-

rungen der Datenschutz-Grundverordnung auseinandersetzen und diese in den Schulen umsetzen.

Die Mitglieder einer Schulgemeinschaft besitzen dabei zunächst die gleichen Datenschutzrechte wie alle anderen Bürgerinnen und Bürger. Schulen haben möglichst datensparsam zu arbeiten und Informationen nur zweckgebunden zu erheben und zu speichern. Eltern haben im Auftrag ihrer noch nicht volljährigen Kinder das Auskunftsrecht, das Recht auf Korrektur und Löschung der Daten und sie können sich an den Datenschutzbeauftragten wenden. Die Schulen ernennen hierfür einen Datenschutzbeauftragten und eine Stellvertretung.

Darüber hinaus gelten die Bestimmungen des Sozial- und Gesundheitsdatenschutzes, z.B. für die Erhebung und Archivierung der Ergebnisse der Einschulungsuntersuchung oder anderen gesundheitlichen und psychologischen Untersuchungen. Zusätzlich gelten landestypische Verordnungen über die Verarbeitung personenbezogener Daten in Schulen. Diese beinhalten Vorschriften zum Umgang mit personenbezogenen Daten auf den privaten Endgeräten der Lehrkräfte, Vorgaben zum Führen der Klassenbücher und Kurshefte, Regelungen zum Führen der Schülerakten und Einsichtnahme der Eltern, Aufbewahrungspflichten, Art der zu sammelnden Daten (Schülerdaten, Daten der Lehrkräfte, Daten zum Unterricht und zu Schulveranstaltungen), Bestimmungen für die Übermittlung von Daten z.B. zwischen Kitas und Schule, bei Schulwechsel, zum Gesundheits- oder Jugendamt, aber auch Vorgaben zur Organisation des Datenschutzes (vgl. Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4.2.2009 in Hessen[2]).

Medienbildung als Datenschutzbildung

Der Bildungs- und Erziehungsauftrag der Schulen, die Strukturen und Prozesse innerhalb der Schulen und der Datenschutz sind eng verknüpft. Eltern erhalten durch die Schülerinnen und Schüler die Einwilligungserklärungen über die Erhebung und Nutzung von personenbezogenen Daten und sie sind zunehmend sensibilisiert, wenn es um Aushänge und um Foto- und Videoaufnahmen geht. Aber auch im Unterricht müssen Lehrkräfte auf der Basis der Fachcurricula auf die Entwicklung von Medienkompetenzen achten. Im Folgenden sind die Anforderungen für die Primarstufe und die Sekundarstufe in Hessen beispielhaft aufgeführt:

2 Online verfügbar unter: https://www.rv.hessenrecht.hessen.de/bshe/document/hevr-SchulStatErhVHEpAnlage1 (Abfrage am: 8.10.2020).

- „Die Lernenden nutzen anforderungsbezogen unterschiedliche Medien gestalterisch und technisch. (...) Sie nutzen Neue Medien verantwortungsvoll und kritisch." (HKM 2011: 10)
- Die Lernenden sollen „einen selbstbestimmten Umgang mit sozialen Netzwerken im Spannungsfeld zwischen Wahrung der Privatsphäre und Teilhabe an einer globalisierten Öffentlichkeit praktizieren" (HKM 2016: S. 9)

Die Grundlage für diese curricularen Anforderungen liefern Ansätze zur Medienbildung und Medienkompetenz, wie sie seit Baacke (1997) und Tulodziecki, Herzig und Grafe (2019) entwickelt wurden. In neueren Ansätzen wird vor allem auf eine höhere Medienbildung für Kinder und Jugendliche gesetzt. Medienbildung ist geeignet,

> „sich diese *(durch die digitalen Medien – A.S.)* entfremdete Welt wieder anzueignen – und zu erkennen, dass sie von den Menschen selbst gemacht und verantwortet ist. Sie hat die Aufgabe, Bildungsprozesse zu unterstützen, die deutlich machen, wie Medien Werkzeuge der Menschen sind, um die Welt zu verstehen und über sie zu kommunizieren." (Moser 2019: 211)

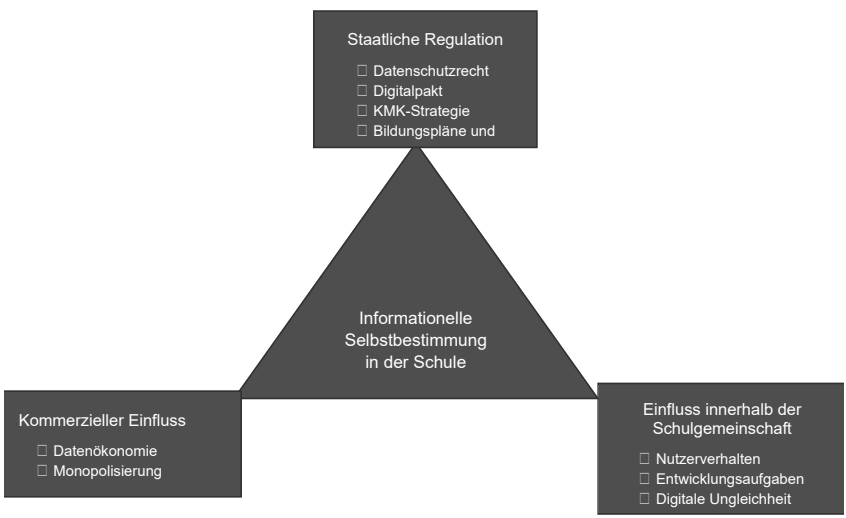
Schülerinnen und Schüler sollen demnach wissen, welche Daten in welchem Kontext zu schützen sind und wie sie sich verhalten sollen, wenn Dritte auf diese Daten zugreifen und unbefugt verwenden. Neben den Grundzügen des Datenschutzes als Grundrechtsschutz sollen Schülerinnen und Schüler neben den allgemeinen Grundlagen (Passwortschutz, Schutzeinstellungen in Anwendungen und im Internet) auch lernen, was personenbezogene Daten sind, Verhaltensweisen zum Schutz ihrer personenbezogenen Daten kennen und sich vor Dritten schützen. Moser (2019) bewertet diese Ansprüche jedoch als Überforderung von Kindern und Jugendlichen:

> „(...) im schlimmsten Fall wird sogar die Illusion vermittelt, man habe es selbst in der Hand zu vermeiden, dass die eigenen Daten abgegriffen werden" (Moser 2019, S. 213).

Daher sollte Medienbildung auch die Bedeutung systemrelevanter Akteure aufzeigen, wie z.B. die Rolle von Internetunternehmen, die Interessen und Möglichkeiten der Zivilgesellschaft sowie die Chancen durch staatliche und betriebliche Datenschutzbeauftragte.

Wirkungen der Triade aus Staat, Markt und Schulgemeinschaft

Bislang wurden neben dem Medienverhalten von Kindern und Jugendlichen vorwiegend staatliche und medienpädagogische Perspektiven rezipiert und in Hinblick auf deren Wirkung für die Medienbildung und den Datenschutz bewertet. Im Folgenden soll die in der Literatur vorherrschende Perspektive erweitert werden. Eine am Datenschutz orientierte Medienbildung zeichnet sich durch die Berücksichtigung staatlichen Rechts und pädagogischer Leitlinien, durch das Antizipieren datenökonomischer und wirtschaftlicher Einflüsse auf das Handeln der Schulgemeinschaft und schließlich durch das soziale Handeln der Kinder, Jugendlichen, Eltern und Lehrkräften als Schulgemeinschaft aus. Die Umsetzung des Rechts auf informationelle Selbstbestimmung zeigt sich – nicht nur in der Schule – als Handlungsfolge aus einer Triade zwischen Hierarchie, Markt und informellem Handeln. Diese Hybridität (vgl. Evers/Rauch/Stitz 2002) kann einerseits positive Synergien für den Datenschutz ergeben, andererseits aber auch zu Spannungen (vgl. Schulz 2010) führen.



Dezentralisierung und Flexibilität seitens des Staates

Neben der DSGVO bestehen einige, schon zitierte Vorgaben der Kultusministerkonferenz und der Kultusministerien für den Datenschutz an den Schulen (z.B. Strategiepapier der KMK „Bildung in der digitalen Welt", Kerncurricula, Digitalpakt). Deren Realisierung erfolgt allerdings weitge-

hend dezentral. Das bedeutet, dass die Planung der technischen Ausstattung und die Medienbildungskonzepte in den Händen der Schulen liegen und die Umsetzung weitgehend selbstständig von den schulischen IT-Beauftragten mit Unterstützung der Schulämter und den städtischen Schulträgern getragen werden. Aufgrund der noch mangelhaften IT-Ausstattung konzentrieren sich die Bemühungen der Schulen vor allem auf eine Breitbandanbindung, WLAN-Ausstattung, Anschaffung von Präsentationshardware und eine Grundausstattung mit modernen Personalcomputern oder iPads. Ob für die Anschaffung mobiler Endgeräte im Sinne einer modernen Medienbildung noch genügend Ressourcen zur Verfügung stehen, ist fraglich. Hier wäre eine Balance zwischen der Entwicklung von Hardwarekonzepten und Medienbildungskonzepten sinnvoller. Auch die Integration der digitalen Medien in den Fachunterricht bleibt den einzelnen Schulen überlassen. Bestehende Apps und Angebote für Mathematik, Deutsch, Sprachen, Natur- und Gesellschaftswissenschaften müssen mit den fachlichen Kompetenzen verzahnt werden. Eine parallel stattfindende IT-Bildung kann Grundlagen für die Herausbildung von Medienkompetenzen bieten, aber führt kaum zu einer Selbstreflexion des eigenen Medienhandelns. Hinzu kommt eine Medienbildung, die den Datenschutz immer noch als individuelles Abwehrrecht vermittelt, andere Einflüsse wie traditionelle pädagogische Standards, die Datenökonomie und soziale Faktoren aber außen vorlässt. Der morgendliche Erzählkreis in den Grundschulen, Plakate mit Bildern vom Urlaub, Geburtstagskalender, Aushänge von Klassenfotos, Aufzeichnung von Schulfesten und Abbildungen errungener Siege bei Meisterschaften in der Schülerzeitung werden hinsichtlich des Datenschutzes zunehmend hinterfragt und bergen für die Verantwortlichen Unsicherheiten. Einfache Leitlinien für die in den meisten Fällen rechtlichen Laien, einheitliche Verzeichnisse der Verarbeitungstätigkeiten und eine reduzierte Form von Einverständniserklärungen für die zunehmende Anzahl von digitalen Anwendungen in der Schule fehlen aufgrund einer zunehmenden Autonomie und Flexibilität für die einzelnen Schulen.

Der Datenmarkt und Einflüsse digitaler Monopole

Der Markt wirkt mehrfach auf das Handeln der Schulen und die Umsetzung der Medienbildung. Zum einen tragen die Schülerinnen und Schüler regelmäßig neue technische Entwicklungen und Anwendungen in die Schule. Abgesehen von den Tablets und Smartphones treten bestimmte Anwendungen als Moden auf, mit denen sich die Schule auseinandersetzen muss. WhatsApp, Instagram, Tik Tok, Pokemon oder Fortnite. begeistern viele Kinder und Jugendliche, bergen aber auch Gefahren. Die Aufga-

be der Schulen ist es daher, den Schülerinnen und Schülern zu vermitteln, dass diese Angebote mit den persönlichen Daten bezahlt werden und das problematisch werden kann. Wikipedia ist neben YouTube und Google eine der beliebtesten Wissensquellen. Doch die Zuverlässigkeit der Informationsangebote ist in vielerlei Hinsicht sehr unterschiedlich und sollte den Schülerinnen und Schülern bekannt sein. Hinzu kommen altersspezifische Unterschiede bei der Nutzung des Internets. Für Grundschüler und -schülerinnen existieren als Alternative zu Google und Wikipedia eine Vielzahl an altersgerechten Suchseiten und Kinderlexika im Internet (z.B. helles-köpfchen, frag-finn). Auf diese Informationsangebote muss besonders hingewiesen werden. Eine größere Herausforderung stellen digitale Anwendungen dar, die erst noch eine höhere Verbreitung finden werden. Die Smart Watch oder die Fitness Tracker, Smart Home, smarte Kleidung oder das Smart Car sind Beispiele für das Internet der Dinge, die besondere Anforderungen an den Datenschutz und die Medienbildung stellen (vgl. Husemann/Pittroff/Schulz 2018). Eine empirische Erhebung an der Universität Kassel 2017 zeigte, dass Schülerinnen und Schülern zu diesem Zeitpunkt kaum bewusst war, dass der Schlafzyklus, der Stromverbrauch, die Anzahl der Schritte am Tag, die gefahrenen Kilometer o.ä. ebenfalls personenbezogene Daten sein können und damit schützenswert sind.[3] Digitale Anwendungen und Geräte können durch das Aufzeichnen, das Verarbeiten und die kommerzielle Nutzung personenbezogener Daten unser Verhalten im Alltag beeinflussen. Die Aufgabe der Schule wird daher auch hier darin bestehen, über die Funktionsweise des Internet der Dinge aufzuklären.

Hinzu kommen Markteinflüsse auf die Schule selbst. In den meisten Fällen legen die Schulträger fest, welche digitalen Medien Einzug in die Schulen finden. Doch häufig sind Betriebssystem und Anwendungen vorbestimmt – und das ist meist das Betriebssystem von Microsoft. Bei den Office-Lösungen gibt es eine breitere Varianz, allerdings scheint sich auch hier der Trend zu Microsoft durchzusetzen. In Hessen wurde der Einsatz von Office 365 zwar zunächst gestoppt. Der Anreiz, das Produkt vom Marktführer kostenlos einzusetzen, ist aber groß. Ähnliche Tendenzen bestehen bei bestimmten Lernprogrammen, die sich – sicherlich auch aus gutem Grund – in vielen Schulen durchzusetzen scheinen. Antolin, Anton,

3 Die Daten wurden erhoben im Rahmen des von Jörn Lamla und Alexander Roßnagel geleiteten interdisziplinären Projektes „Smart Environment, Smart Information?“ (SEnSI) an der Universität Kassel (gefördert vom BMJV 01/2017 bis 12/2017).

die Lernwerkstatt oder PADLET sind nur einige Beispiele. Auch die Schulbuchverlage setzen verstärkt auf Lernapps. Während der Schulschließungen im Corona Lockdown stellten die Verlage Megabyte an PDFs zur Verfügung, die Lernapps blieben aber teilweise kostenpflichtig. Kostenlose Versionen hatten nur eine eingeschränkte Funktionalität oder einen begrenzten Umfang. Der Datenschutz spielte zu Beginn der Pandemie kaum eine Rolle. Die Prämisse lag auf der Ermöglichung des Lernens zu Hause. Wie häufig personenbezogene Daten ungeschützt und ohne Aufklärung versandt und verarbeitet wurden, ist allerdings unklar. Digitales Lernen benötigt einen Zugang zu datenschutzkonformen Lernmaterialien. Den Schulen bleibt es dagegen selbst überlassen, welche digitalen Medien und Anwendungen sie erwerben und wie sie den Datenschutz gewährleisten. Das ist allerdings häufig jedoch eine Frage der Kompetenzen der schulischen Datenschutzbeauftragten, IT-Beauftragten oder interessierten Lehrerinnen und Lehrern.

Die Schulgemeinschaft

Aufgrund der hohen formalen Einbindung der Schule in die Hierarchie aus Kultusministerium und Schulämtern bzw. Bezirksstellen besteht die Gefahr, die Schule auch als demokratische und gemeinschaftliche Institution zu unterschätzen. Doch den Eltern steht eine Reihe von Mitsprachemöglichkeiten z.B. über die Elternbeiräte oder Fördervereine zu. Kinder lernen als Schulsprecher, in Klassenräten und Kinderkonferenzen demokratische Grundlagen kennen. Die Eltern gestalten zusammen mit den Lehrerinnen und Lehrern in Schulkonferenzen wesentliche Entwicklungen mit. In den Gesamtkonferenzen, Klassenkonferenzen und durch die Personalvertretung haben auch die Lehrerinnen und Lehrer einen gewissen Einfluss auf die Schul- und Unterrichtsorganisation.

Wesentliche strukturelle Veränderungen des Lehrens und Lernens sind in diesen Institutionen der Schulgemeinschaft zu besprechen und demokratisch zu legitimieren. Das gilt auch für den Datenschutz und die Medienbildung. Die Anschaffung digitaler Geräte und die Medienbildungskonzepte müssen in den demokratischen Gremien besprochen und abgestimmt werden. Die Datenschutzerklärungen und die Bedingungen für die Nutzung der Privatgeräte für dienstliche Zwecke (Passwortschutz, Virenscanner, Datensicherheit) sind vorzustellen und zu unterschreiben. Allerdings treten schon hier Probleme auf. Den Lehrkräften stehen keine dienstlichen Endgeräte wie Laptops oder iPads und nur selten dienstliche E-Mails zur Verfügung, d.h. die Unterrichtsvorbereitungen und die Zeugniserstellung werden meist am heimischen, privaten PC erstellt, was daten-

schutzrechtliche Fragen aufwirft. In Zeiten von Corona werden die privaten Geräte zudem für das Online-Lernen mit Lernplattformen und für Videokonferenzen und E-Mails genutzt. Eine Vermischung von privaten und dienstlichen Daten, ein unzureichender Datenschutz und Datensicherheit sowie begründete oder unbegründete Ängste in Bezug auf Schäden bei privaten Geräten führen zu fehlender Akzeptanz für die Nutzung digitaler Möglichkeiten für die digitale Lehre und letztlich die Ablehnung der Medienbildung. Die verbreitete Annahme, dass nur jüngere Lehrkräfte den Zugang zu den digitalen Medien finden und diese im Unterricht einsetzen, kann nicht bestätigt werden. Den „digital native" gibt es nicht (vgl. z.B. Schaumburg 2015). Individuelle Präferenzen und Interessen, aber auch eine unzureichende Medienbildung während der Ausbildung führen auch bei Jüngeren zu einem angespannten Verhältnis zu digitalen Lehr- und Lernmitteln.

Neben der Schul- und Unterrichtsorganisation bestehen Anforderungen für den Datenschutz in Bezug auf die soziale Interaktion zwischen den Kindern und Jugendlichen. Zum ersten ist es für die Einzelnen zunehmend schwerer, sich digitalen Moden zu entziehen. Das betrifft die Anschaffung neuer Geräte, für deren Kosten ältere Schülerinnen und Schüler vermehrt Nebentätigkeiten aufnehmen, aber auch welche Apps en vogue sind. Kostenlose Spiele werden schnell zu Kostenfallen, wenn die darin versteckten App-In-Käufe ein höheres Prestige und ein schnelleres Weiterkommen im Spiel ermöglichen. Können Kinder und Jugendliche zwischen Online-Spielen und Lernapps auswählen, werden die Spiele und das „Zocken" präferiert, so dass sich letztlich alle Kinder im Jump-and-Run Modus befinden. Angebote wie z.B. Antonin, Anton, die Lernwerkstatt oder das „Internet-ABC", eine Plattform zum Erlernen grundlegender Kompetenzen am Computer und im Datenschutz, nutzen freiwillig nur wenige Kinder und Jugendliche. Diese Angebote können daher nur in unterrichtsadäquater Form vermittelt werden. Die Nutzung des Internets als Informationsquelle hängt zudem stark mit dem Bildungsniveau des Elternhauses zusammen (vgl. Schaumburg 2015). Zweitens führt die Ausbreitung der digitalen Geräte zunehmend zu Problemen wie Cyber-Mobbing, Sexting und anderen Gefahren (vgl. Südwest 2019). Während Ausgrenzungen in vordigitalen Zeiten auf dem Schulhof blieben, besteht nun die Gefahr, dass die Betroffenen auch durch Schulwechsel oder bis ins Erwachsenenalter von den Angriffen begleitet werden. Eine früh ansetzende Medienbildung zum Schutz der Grundrechte, aber auch geeignete Konzepte an den Schulen gegen Cyber-Mobbing, Sexting und andere Gefahren müssen Teil der Medienbildung werden. Ein aus fürsorglicher Perspektive verständliches Han-

dyverbot an Schulen (vgl. Spitzer 2012, 2018) verhindert die Risiken und Gefahren nur symptomatisch.

Fazit: Anforderungen an die schulische Medienbildung aus der Perspektive des Datenschutzes

Abschließend lassen sich einige Anforderungen für das Bildungswesen formulieren, die den Datenschutz für Kinder und Jugendliche, Eltern, Fürsorgetragende und die Lehrkräfte verbessern könnten. Diese Liste ist aber weder vollständig noch garantiert sie einen allumfänglichen Datenschutz:

1. Die Schulen können das Grundrecht auf informationelle Selbstbestimmung nicht alleine mit ihren begrenzten Ressourcen garantieren. Sie unterliegen zu vielen staatlichen, ökonomischen und informellen Einflüssen. Die Lehrkräfte sind Experten für Pädagogik und Erziehung, für zusätzliche Aufgaben braucht es Ausbildung oder schulübergreifende Beauftragte.
2. Schulträger und Schulaufsichtsbehörden könnten den Schulen konkrete Handlungsleitlinien und Hinweise für gute digitale Lehr- und Lernanwendungen bieten, die datenschutzkonform und pädagogisch wertvoll sind.
3. Digitales Lernen kann Bildungsungleichheiten aufgrund unzureichender technischer Ausstattung, geringer digital literacy oder bestehender Bildungsungleichheiten zwischen den Elternhäusern verstärken. Hier braucht es Unterstützung zum Beispiel durch die Bereitstellung von mobilen Endgeräten und WLAN, Kurse für Kinder und Eltern, die Einbindung der digitalen Lernformen in den Unterricht und in die Ganztagsbetreuung.
4. Um die Bedeutung des Datenschutzes zu erhöhen, muss das Verständnis über den Datenschutz, Handlungsmöglichkeiten und kritische Entwicklungen im Mediensystem in die Medienbildung einfließen. Im Rahmen der Schulcurricula können digitale Lehr- und Lernformen in den Fachunterricht integriert werden.
5. Die Schulaufsichtsbehörden sollten Datenschutzbeauftragte für mehrere Schulen installieren, die angesprochen werden können. Zwar sind die bisherigen schulischen Datenschutzbeauftragten formal unabhängig, doch eine Lehrkraft kann gegenüber der Schulleitung nicht zugleich weisungsgebunden und unabhängig sein.
6. Das Bildungswesen benötigt eine „digitale Wende“, die die Bedeutung für den Datenschutz und die Medienbildung im Sinne digitaler Lern-

und Lehrformen stärkt. Bislang stehen vor allem die digitale Schuladministration, Breitbandanbindung und Präsentationstechniken im Vordergrund. Datenschutz ist im Interesse der Schülerschaft und Elternschaft und damit der Schüler- und Elternbeiräte. Aber auch andere bürger- und zivilgesellschaftliche Interessensgemeinschaften, die sich für die demokratische Digitalisierung der Gesellschaft einsetzen, sind hier gefordert.

Digitale Lehr- und Lernmittel wie auch die Digitalisierung der Schulprozesse müssen datenschutzkonform entwickelt werden. Das bedeutet einerseits, Lehrkräfte und die Kinder und Jugendlichen mit Fragen des Datenschutzes vertraut zu machen und dafür zu sensibilisieren, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ihre Grundrechte tangiert. Andererseits muss auch ein pragmatischer Umgang mit den rechtlichen Anforderungen, des Einflusses der Datenökonomie und der Mediatisierung der Schulgemeinschaft gefunden werden, der Lehrkräfte, Eltern, Kinder und Jugendliche nicht überfordert, gleichzeitig aber den Datenschutz gewährleistet. Hierfür braucht es die Entwicklung von Bildungsangeboten zum Thema Datenschutz und Medienbildung. Die Zivilgesellschaft ist zunehmend gefordert, den Prozess der Digitalisierung im Bildungswesen zu begleiten.

Literatur

Baacke, Dieter (1997): *Medienpädagogik*. Tübingen: Niemeyer.

Evers, Adalbert / Rauch, Ulrike / Stitz, Uta (2002): *Von öffentlichen Einrichtungen zu sozialen Unternehmen: Hybride Organisationsformen im Bereich der Dienstleistungen.* Berlin: Ed. Sigma.

Hessisches Kultusministerium (HKM) (2011): *Bildungsstandards und Inhaltsfelder - Das neue Kerncurriculum für Hesse, Primarstufe: Deutsch.*

Hessisches Kultusministerium (HKM) (2016): *Kerncurriculum gymnasiale Oberstufe, Deutsch.*

Hessisches Kultusministerium (HKM) (2020). *Digitale Kommunikation von Lehrkräften öffentlicher Schulen in Hessen während der Zeit der Covid-19-Pandemie*. Hinweise des Hessischen Beauftragten für Datenschutz und Informationsfreiheit vom 23. März 2020.

Hurrelmann, Klaus / Rosewitz, Bernd / Wolf, Hartmut K. (1985): *Lebensphase Jugend: eine Einführung in die sozialwissenschaftliche Jugendforschung.* Weinheim u.a.: Juventa-Verlag.

Husemann, Charlotte / Pittroff, Fabian / Schulz, Andreas D. (2018): *Fitness-Tracking als Informationsproblem. Zu den Potenzialen und Herausforderungen rechtlicher Regulierung und pädagogischer Vermittlung.* In: Datenschutz und Datensicherheit – Dud 11, S. 694-700.

Moser, Heinz (2019): *Einführung in die Medienpädagogik: Aufwachsen im digitalen Zeitalter, Wiesbaden.* Wiesbaden: Springer VS.

Schaumburg, Heike (2015): *Chancen und Risiken digitaler Medien in der Schule. Medienpädagogische und -didaktische Perspektiven.* In: Bertelsmann-Stiftung (Hg.): Individuell fördern mit digitalen Medien – Chancen, Risiken, Erfolgsfaktoren. Gütersloh: Bertelsmann-Stiftung, S. 20-94.

Schulz, Andreas D. (2010): *Organisationen zwischen Markt, Staat und Zivilgesellschaft: Arbeitsmarktförderung von Langzeitarbeitslosen im Deutschen Caritasverband.* Wiesbaden: VS Verlag für Sozialwissenschaften.

Schulz, Andreas D. (2019): *Informationelle Selbstbestimmung. Grundrecht oder Mythos?* In: Praxis Politik 5, S. 42-48.

Spitzer, Manfred (2012): *Digitale Demenz: Wie wir uns und unsere Kinder um den Verstand bringen.* München: Droemer.

Spitzer, Manfred (2018): *Die Smartphone-Epidemie: Gefahren für Gesundheit, Bildung und Gesellschaft.* Stuttgart: Klett-Cotta.

Südwest, Medienpädagogischer Forschungsverbund (2018): *KIM-Studie: Kinder und Medien, Computer und Internet.* Stuttgart: MPFS.

Südwest, Medienpädagogischer Forschungsverbund (2019): *JIM-Studie: Jugend, Information, (Multi-)Media.* Stuttgart: MPFS.

Tulodziecki, Gerhard / Herzig, Bardo / Grafe, Silke (2019): *Medienbildung in Schule und Unterricht: Grundlagen und Beispiele.* Bad Heilbrunn: Verlag Julius Klinkhardt.

Zillien, Nicole (2009): *Digitale Ungleichheit: Neue Technologien und alte Ungleichheiten in der Informations- und Wissensgesellschaft.* Wiesbaden: VS Verlag für Sozialwissenschaften.

Teil V – Praktische Umsetzung(en) – Erfahrungsberichte und Handlungsempfehlungen

A day-in-the-life of a datafied child – observations and theses

Jen Persson

Abstract

"*Children do not lose their human rights by virtue of passing through the school gates.*" The UN Committee on the Rights of the Child set out a clear message in 2001. As the use of electronic school records has expanded rapidly in the twenty years since, however, children's rights have not only been left at the school gates but have become lost in the digital environment in which companies follow online activity from school into the home, 24/7, and every day of the year. I describe some of the practices in the state education system in England, where children attend compulsory education from their fifth birthday, and immediately lose control of their digital footprint. At the time of writing, there has been little enforcement of GDPR in education, and there is a lack of attention paid to laws in edTech thinking. I propose actions needed to build a rights' respecting environment in education, and areas for further research in emerging harms, with the aim of preventing known interferences with rights today; reducing personal, institutional and state security risks; and horizon scanning, to protect the future of children's autonomy, human rights, state education, and society.

1. Children do not lose their human rights by virtue of passing through the school gates, but they are not well realised:

1.1 In 2017 the Children's Commissioner in England concluded in a report called 'Growing Up Digital', that we are failing in our basic responsibility as adults to give children the tools to be agents of their own lives. If the issue of managing our digital footprint is difficult for adults, it is even harder for children in compulsory education where they are disempowered by default.

1.2 In addition to personal data collected directly from families for the administration of a child's education and care; invisible or inferred information are collected about pupils; through RFID (Taylor 2019), beacons,

virtual assistants in the classroom and by Internet Connected Things. A child's permanent digital record may include standardised test scores but also opinion and inferences, such as behavioural records recorded by a teacher in a school core information management system, an app, or created by artificial intelligence (AI).

1.3 Children care about their privacy and want to be able to decide what information is shared with whom. That is difficult when "*teachers are unclear what happens to children's data and there is common misunderstanding of how much data leaves a school.*" (Stoilova et al. 2019).

1.4 If children do not know where their digital footprint goes, they cannot understand how others may use it to make decisions about them. This is amplified when school records are linked with other personal data about them held by the state, by companies, or linked to data purchased from third-party data brokers (WhatDoTheyKnow 2018).

1.5 Rights may not be realised if there is no way to understand them or the choices that the individual has as a result, or there is no clear route for redress when they are infringed upon. Emerging harms and infringements to children's privacy rights under the *General Data Protection Regulation (GDPR)* and Convention 108[1], to their dignity, free expression (Kaye 2019), and their rights enshrined in the UN Convention on the Rights of the Child (UNCRC) to full development and human flourishing, can result from various areas of commercial and state practice that stem from mining the 'datafied child' (Lupton/Williamson 2017). These may be obvious institutional (BBC 2019), personal privacy, or security breaches, but hidden harms may remain to be exposed, such as discrimination and racism or bias in automated decision-making.

1.6 A child's best interests are not consistently defined or considered as part of one-size-fits-all risk assessments in digital procurement processes today, that may not assess special educational needs, ethnicity, or lack of access to technology at home, as part of equality duties.

1.7 There need be no conflict between privacy and innovation (Denham 2017), yet some products in emerging fields infringe on rights when pupils are compelled to use a product, and their interactions are used as the source of training data. The effects of personalisation or of AI on children's wellbeing are largely opaque to families.

1.8 The changing landscape of what is permissible, what is possible, and what is acceptable in education, is being trialled on our children. But

1 Convention 108. Online verfügbar unter: https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108 [Abfrage am 4.10.2020].

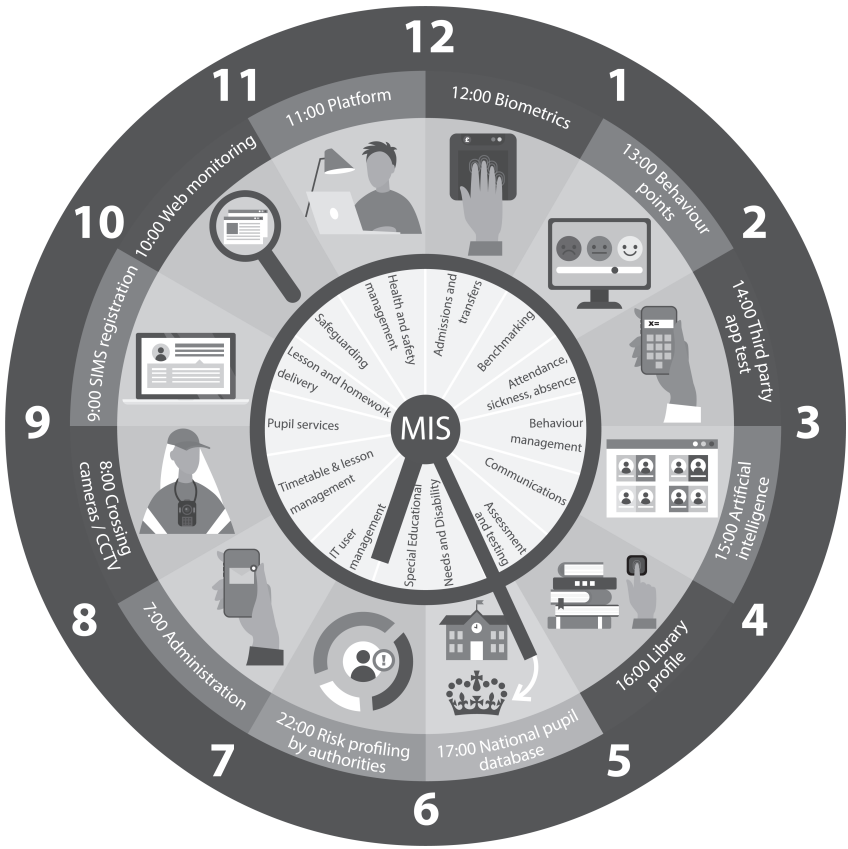
should children be used as continuous research subjects? For a company, a year could be a short time to bring a product onto the market, or to discover the efficacy of an edTech tool is poor, but it could be a defining year of a child's education.

1.9 To be able to give children the tools to be the agents of their own lives, and enable them to realise their rights as fully fledged right holders, we need a sector-wide new approach.

2. What does a day-in-the-life of a datafied child look like?

2.1 To demonstrate the variety of data processing across the range of activities in a child's day, this illustration gives an example of an imagined eleven-year-old's day in a state school. The Data Wheel captures the administrative areas for which a school processes a child's data using a core Management Information System (MIS) at its centre. A variety of private companies offer these to the education sector in England, and also work in collaboration with the national Department for Education to ensure interoperability with the national government data collection every school term, in the school census. In addition, illustrated in the outer ring, children have daily interactions with a wide variety of external third party tools.

Fig 1. An illustrative summary of an eleven-year-old's day in the English school system. Designed by and created from research by the author. Artwork created by Nadia Snopek.



2.2

- 07:30 An event reminder arrives on a child's mobile phone.
- 08:30 She walks to school via the street crossing and is filmed on the patrol officer's bodycam and on closed circuit television (CCTV) at the school entrance, as she enters the playground and the corridors.
- 09:00 Attendance is registered on the school management information system (MIS).
- 09:15 She has logged onto Google classroom, and silently the school web monitoring software starts up, comparing every Internet search

term against a set of thousands of keywords that will trigger a system alert if found. Artificial Intelligence supported software looks for risk indicators of self-harm, mental health, bullying, stranger-danger, terrorism and extremism. Her quick search for information about the cliffs from the family walk she enjoyed that weekend, triggers a flag as potential suicide risk. That notification is sent from the company support staff to a school teacher's inbox.

- 10:00 She is asked by the maths teacher to use an app on her personal mobile phone, to do a quick quiz. She enters her username, school email address and data of birth as verification. The teacher sees all scores and progress on their own screen.
- 11:00 In chemistry she logs into the AI-led platform, and watches a short film. She wasn't paying attention and only gets six out of ten on the multiple choice quiz: Watch it again, suggests the machine learning app, having recorded her mouse movements every two seconds, otherwise she cannot proceed to the next chapter.
- 12:00 Reaching the front of the line to pay for her lunch without cash, she pushes her finger into the unclean machine (Leaton Gray/Phippen 2017) to read her biometrics for the tenth time that week. Every child must use the systems to not only buy lunch, but also to borrow a library book.
- Before they leave that day, the children will have logged into three more apps, including a foreign language app matching vocabulary to pictures, and a reading app to measure the number of words of fiction they read a week. Any child whose profile shows a slowdown in reading speed over a month, will be required to see the librarian.
- At the after-school football club pupil attendance is checked against their names from the school information management system provided details. Their sports changing space is recorded on CCTV. Their team photo was taken for the school website, social media pages, and local newspaper for the tournament that weekend. She feels left out as the only one whose parents have refused photographs for marketing.
- 18:00 At six pm, she logs back into Google classroom, accessing her homework tasks and contents at home. She watches a YouTube video, and all the time the web monitoring is scanning her Internet screen content for signs of suicide. She's on a watch list now since this morning's system error. But she doesn't know it.
- 22:00 At the end of each day, the school information management system sends changes and new data to the Regional Authority database to match with welfare, health, and policing records and build predictive profiles for interventions.

- Once a term, three times a year, her details from the Management Information System are sent in the school census to the National Pupil Database, now holding the named records of over 21 million people in England. (defenddigitalme 2018)
- Years later, her school records will be joined to data from her university application records, and her first employment earnings and / or state welfare payments, will suggest to civil servants how much each education costs the state and be used by politicians to tell the public which courses have the greatest economic return.

2.3 She has no idea to how many companies in which countries her personal data has been sent in the course of this day, or knowledge of the national databases. The implications for the future of society are staggering if we can no longer rely on privacy as an enabling right to participation, to protect full and free development of personhood and character free from excessive or opaque influence of behaviour, to protect the right to access confidential information without surveillance, or to move into adulthood without being held back by predictive profiling used to deny opportunities to pupils less likely to succeed, used in secret to deny eligibility for student loans (Adams 2018) or passed on from school to Higher Education.

3. The sensitivity of children's data in the school system must not be underestimated

3.1 The International Working Group on Data Protection in Telecommunications recognised in its working paper on e-learning platforms (2017) that *"the sensitivity of digitized pupil and student data should not be underestimated"*.

3.2 "*Education happens to be today, the world's most data-mineable industry by far,*" said the then CEO of Knewton, José Ferreira, in 2012 at the White House Datapalooza. Technology investment is laden with values and the politics of what education means, how and where it is delivered, and who controls it (UNICEF 2018). Estimations of global market value and investments from incubators and angel investors (Metaari 2020) suggest: *"The US accounted for just over 58% ($5.5 billion) of all investments made to learning technology companies in 2017. This changed dramatically in 2018, with companies in China garnering 44.1% of all funding, followed by the US at 32%. This reverted in 2019 with the US retaking their status as the top edtech investment destination. In 2019, China accounted for 'only' 21.4% of all funding on the*

planet while the US accounted for 42.9% of all global funding, double the investments made in China."

3.3 At the same time, under the pressures of keeping costs down and marketisation, the infrastructure to deliver UK state education is exposed to risk via commercial 'freeware' that locks schools into closed, proprietary systems that are run based on platforms that were first developed for business, not children. They often extract children's data and teaching material content with little transparency over processing after transfer from the school, or about their own practices in data analytics (Hessen Data Protection Authority 2019).

3.4 There are regular reports of security problems in apps that process children's sensitive data, such as children's mental health assessments (The Register 2019) yet neither the efficacy nor credentials of apps are required to meet the high bar of necessary due diligence that medical apps might be (NHS 2020). Risks to personal, institutional (BBC 2019), and national security, of both data and technology infrastructures are underestimated in a single school risk assessment, that does not look for national or collective risk.

3.5 The State further creates and controls a child's national digital footprint by their fifth birthday. This creates risks for the child when identifying data from the National Pupil Database are given to thousands of non-state actors (Department for Education, 2020) without a child's or their family's knowledge (Survation poll 2018). Government departments further link and repurpose individuals' education data with their records across government, which adds further levels of sensitivity through its joined-up additional knowledge and impact from use, including use for immigration enforcement (defenddigitalme 2016).

4. Children's rights are failed in practice

4.1 When it comes to a legal basis for data processing as the first protection for children, schools are the gatekeepers not only for the State, but for thousands of third-parties to gain access to millions of children's lives. If the school assumes an absolute right to make choices on the child's behalf, which technology must be used in the classroom or for homework, the most fundamental principles of data protection are easily ignored. Schools routinely assume all data processing is permissible under the public task. But features designed for easy school administration can risk abuse, such as compulsory open directories (The Register 2018). Even where companies' terms and conditions state consent is required, children's personal details,

often together with parents' emails, are routinely extracted in bulk from the core MIS to third-parties, and without parental permission.

4.2 This lack of accountability fails children. Third-parties generally assume that they are data processors not controllers, but may be incorrect where they routinely determine the nature and purposes of processing (defenddigitalme case studies 2020).

4.3 Fundamental principles in data rights include a right to know who collects which personal data about you, for what purposes, who it is shared with, how long it is kept, and rights to correct inaccuracies or object to marketing re-use. All these rights are ignored where the companies pass on the responsibility to the schools that rarely have the understanding or capacity to manage the 'new governmental arrangements' of big data they process (Williamson 2017a).

4.4 Even for special category data such as religion, consent as a legal basis for processing personal data can fail children. A recent national project extracted the personal data including religion and behavioural data from 65,000 children, claiming legitimate interests (Ruda 2019). UCAS, the UK university applicant system asks young people (who may be under 18 routinely in Scotland, or at the time of applying) for consent to share their religion, sexual orientation and disabilities with their future university, as part of the higher education application equality monitoring process. But application forms do not explain that this will be linked with their named, individual national pupil record, and be kept indefinitely at the Department for Education (Shearing 2019).

4.5 Increasingly invasive technology has become normalised in schools, as tools have become routine without challenge. Not only can apps be used to document whole class behaviour, but body worn cameras too. In 2018, a school in Birmingham installed cameras the size of a fifty pence coin in classrooms to monitor voice and movement (Schools Week 2018) for teacher training purposes. How can schools respect individual rights in class-wide policies?

4.6 Commercial exploitation may not be explicit. Apps that monitor children's behaviour scores may have terms and conditions on not reselling data. But they might also require that the school accepts click-wrap agreements - pre-packaged terms and conditions designed by the company that cannot be changed by the school and must be accepted to continue to use the product even if they change over time. Indefinite pseudonymous data retention is routine in such terms. It is also common for companies to re-use personal data for their own commercial purposes; whether for in-app adverts, or to send parents emails for premium products. Families are a captive audience.

4.7 The increasing scale, speed and simplicity of data transfer has been rapid, while data storage cost has fallen. The technological barriers to data access, copying and distribution have been diminished while the complexity of emerging products has grown.

4.8 It is impossible for a school to really understand how lots of these tools work. Researchers at the Oxford University Department of Computer Science, revealed the extent of hidden trackers, in an assessment of nearly one million apps (Binns et al. 2018). And if developers might not even understand the full extent of what their code does (Ekambaranathan et al. 2020), how can schools meet the obligations of data privacy and protection by design and default (ICO 2020a) or teachers be expected to understand all this and explain it to families? All these circumstances create an increase in the need for expert due diligence in order to realise children's rights in practice, that cannot be adequately met in today's school systems.

5. Can regulatory enforcement save us?

5.1 The Data Protection Authority in Sweden was the first decision under GDPR, to recognise the power imbalance in schools, and rule that consent was invalid, in the case of facial recognition used for registering attendance (Swedish Data Protection Authority 2019). In Norway insufficient technical and organisational measures to ensure information security were found in a home school communications app. And in the UK the ICO made an interim statement during its investigation of the Department for Education that the Department breached data protection rules over its controversial pupil nationality data collection and by sharing pupils' details with the Home Office since 2015 (Schools Week 2019). In 2020 its audit made 139 recommendations, of which over 60% were urgent or high priority (ICO 2020b). However, if enforcement is only on a case-by-case basis, will that bring about the systemic change needed to respect children's rights?

5.2 Natasha Singer writing in the New York Times in May 2017, described in her words, how Google took over the US classroom.

> "In the space of just five years, Google has helped upend the sales methods companies use to place their products in classrooms. It has enlisted teachers and administrators to promote Google's products to other schools. It has directly reached out to educators to test its products — effectively bypassing senior district officials. And it has outmaneuvered Apple and Microsoft with a powerful combination of low-cost laptops, called Chromebooks, and free classroom apps.

> Today, more than half the nation's primary- and secondary-school students — more than 30 million children — use Google education apps like Gmail and Docs, the company said. And Chromebooks, Google-powered laptops that initially struggled to find a purpose, are now a powerhouse in America's schools."

5.3 Large companies that capture large amounts of personal data about large numbers of children - millions in multiple countries - are growing a power base that other companies simply do not have. It is power that goes beyond data processing but starts to reach into how and what teachers teach. By shaping staff training, you capture elements of the shape of the curriculum and the structure of how it is delivered, at country level, then worldwide. Research is needed to ask whether this shapes a change in not only state delivered education but its purpose — why focus on teacher knowledge after all, if your company has turned its search term to look for knowledge online, into a common verb?

5.4 How transparent are their objectives and with what oversight are their outcomes measured? The potential global implications for the future cost and stability of the state sector education infrastructure, and the individual and collective costs to children in terms of privacy and normalisation may be shaping students and society in ways we are yet to see.

6. Taking stock of system led decision-making

6.1 Artificial intelligence can be used from low-level decision making, such as assigning class seating plans based on children's behavioural scoring through to shaping a personalised curriculum. But although commonly referred to in marketing materials, what AI actually is and does in some tools is vague, *"often indistinguishable from the application of computing, statistics, or even evidence"* (Veale 2019).

6.2 Developers shape what is done to children through their design. There are no statutory boundaries of how far they are permitted to nudge a child's behaviour, how they affect a child's mental health, how they judge a child's performance, how they judge the intent behind a child's Internet search, and what data analytics they process - all these decisions are dependent on companies that are subject to change of control at no notice, through sales, mergers, private equity and takeovers. These decisions are shaping children's lives.

6.3 The GDPR term 'significant effect' is not yet well enough understood, particularly in terms of future effects on children and predictive us-

es of data and while such effects may not yet be transparent to public sector staff or families. The predictive utility and accuracy of risk factors are largely assumed rather than established via independent evaluation of the tool (Van Brakel 2019). Others have also proposed children must be better protected from such technology using historical data: "*Children should be ensured a free, unmonitored space of development, and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data*" (HLEG-AI 2019).

7. What is next?

7.1 The next generation of technologies is already intervening in the lives of the next generation of society in ways that we do not yet understand. We are failing to ask the right questions of policy makers and companies. We are allowing the available tools to shape education unquestioningly when the hype of edTech achievement so far outweighs the evidence of delivery. Writing in the Impact magazine of the Chartered College in January 2019 Neil Selwyn summed up:

> *"the impacts of technology use on teaching and learning remain uncertain. Andreas Schleicher – the OECD's director of education – caused some upset in 2015 when suggesting that ICT has negligible impact on classrooms. Yet he was simply voicing what many teachers have long known: good technology use in education is very tricky to pin down*."

7.2 Behavioural science, neuroscience (Standaert 2019), psycho-policies (Williamson 2017b), personalisation through genetics (Education Select Committee 2013), facial recognition and gait analysis, affective tech (Nemorin 2017), and questions over the use of other emerging technologies including using AI in school surveillance software for countering-violence and extremism (defenddigitalme 2019) abound. In the face of these advances, and in the volume and velocity of data processing, there is an urgent need to support moratorium (Kaye 2020) while the exercise of rights is enabled in practical and meaningful ways.

8. Conclusion: How do we build a rights-respecting environment for life not just one day?

8.1 Data protection alone is insufficient to protect children's full range of rights in the digital environment. Only by reshaping the whole process,

will we have a chance to restore the power balance to schools and to families. Schools must return to a strong position of data controllers and delegate companies to data processors with consistent standards on what they are permitted to do. That infrastructure may not exist, but we need to build it.

8.2 Procurement processes must require assessment of what is pedagogically sound and what is developmentally appropriate, as part of risk assessment including data protection, privacy and ethical impact. Assessment of risk is not a one-time state at the start of data collection, but across the data life-cycle. While teacher training must include a core requirement on data and digital rights, and continuing professional development should be offered regularly, a shared-skill model could reduce the burden of due diligence across every school.

8.3 Legislation, Codes of Practice, and enforcement need to prioritise the full range of human rights of the child in education, in accordance with COE Recommendation CM/Rec (2018) of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, and the Council of Europe (2020) Committee on Convention 108 Guidelines on Children's Data Protection in an Education Setting. Policy at all levels must respect the UNCRC Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector:

> *"A State should not engage in, support or condone abuses of children's rights when it has a business role itself or conducts business with private enterprises. For example, States must take steps to ensure that public procurement contracts are awarded to bidders that are committed to respecting children's rights. State agencies and institutions, including security forces, should not collaborate with or condone the infringement of the rights of the child by third parties. States should not invest public finances and other resources in business activities that violate children's rights."*

8.4 Consent and contract terms must be rethought in the context of education. As set out by the European Data Protection Board in 2020 *Guidelines on consent*, children [and their guardians] cannot freely consent to data processing, where the nature of the institutional-personal power imbalance means that consent cannot be refused, or easily withdrawn without detriment, and they recognise that the GDPR does not specify practical ways to gather the parent's consent or to establish that someone is entitled to perform this action.

8.5 Defining standards and expectations could begin in data security, set out in statutory Codes of Practice (Art. 40 GDPR) and Freedom of Infor-

mation laws should be applied to all non-state actors, companies and arms´ length government bodies, providing education and children's services to the publicly funded state sector.

8.6 Public Authorities should document and publish

- commercial processors /subprocessors engaged in children's data processing
- a register of any commercially obtained sources of personal data collected for processing, or linkage with data provided by individuals in the course of their public sector interactions (Dencik et al 2019), and update it on a regular basis (i.e., Data brokers, third-party companies, social media).
- Data Protection Impact Assessments, Retention schedules, and GDPR s36(4) Assessments with periodic reviews to address change.

8.7 Sector-wide changes are needed on

- Children's agency
- The role of families
- The role of school staff
- A model framework of management of permitted processing not based on consent
- Reducing the investigative burden
- Procurement
- Automated decisions, profiling, and AI
- Horizon scanning on new technology
- The permanent single record
- Representation and remedy
- And lifetime accountability for the data cycle.

8.8 An alternative model of data rights' management in education is that of the U.S., governed by FERPA with state variations. It is imperfect but offers a regional model of law and expertise for schools to rely on, with trusted contractual agreements. Schools are data controllers. Processors cannot change terms and conditions midway through the year, without agreed notifications, and reasonable terms of change. Families get a list each year (or at each school move) to explain the products their child will be using - and crucially, legal guardians retain a right to object. Schools are obliged to offer an equal level of provision via an alternative method, so that objection is not to the detriment of the child (Student Privacy Compass).

8.9 A strong foundation must be built to ensure children do not lose their human rights by virtue of passing through the school gates. While the UK government is driving an edTech strategy for post-Brexit export, it fails to address fundamental principles of data laws, and the child rights framework needed for the safe use of educational products, not only in the life of a child on one day, but forever.

References

Adams, Richard (2018): *Student Loans Firm Accused of 'KGB Tactics' for Assessing Eligibility.* In: The Guardian. Online verfügbar unter: https://www.theguardian.com/education/2018/oct/30/student-loans-firm-accused-of-kgb-tactics-for-assessing-eligibility [Abfrage am: 6.10.2020].

Allen-Kinross, Pippa (2019): *DfE Facing Action Iver 'Wide Ranging and Serious' Data Protection Breaches*. In: Schools Week. Online verfügbar unter: https://schoolsweek.co.uk/dfe-facing-action-over-wide-ranging-and-serious-data-protection-breaches/ [Abfrage am: 4.10.2020].

Binns, Reuben / Lyngs, Ulrik / Van Kleek, Max / Zhao, Jun (2018): *Third Party Tracking in the Mobile Ecosystem*. Online verfügbar unter: https://www.researchgate.net/publication/326138940_Third_Party_Tracking_in_the_Mobile_Ecosystem [Abfrage am: 6.10.2020].

Chirgwin, Richard (2018): *Victoria's Educational Apps-For-Students Let Creeps Contact Kids*. In: The Register. Online verfügbar unter: https://www.theregister.co.uk/2018/05/22/has_google_built_a_haven_for_creeps_in_victorias_education_apps/ [Abfrage am: 4.10.2020].

Committee on the Rights of the Child General comment No. 16 (2013): *On State Obligations Regarding the Impact of the Business Sector on Children's Rights*. Online verfügbar unter: https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf.

Corfield, Gareth (2019): *Pupil Mental Health Monitor Promises App Rewrite After Hardcoded Login Creds Discovered*. In: The Register. Online verfügbar unter: https://www.theregister.co.uk/2019/09/27/pupil_mental_health_tracking_app_security_fears/ [Abfrage am: 4.10.2020].

Coughlan, Sean (2019): *Hackers Beat University Cyber-Defences in Two Hours*. In: BBC. Online verfügbar unter: https://www.bbc.co.uk/news/education-47805451 [Abfrage am: 4.10.2020].

Council of Europe (2020): Committee on Convention 108 *Guidelines on Children's Data Protection in an Education Setting* https://www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting- [Abfrage am: 27.11.2020]

Defenddigitalme (2016): *Timeline of Home Office Access to Pupil Data in England for Immigration Enforcement*. Online verfügbar unter: https://defenddigitalme.org/timeline-school-census/ [Abfrage am: 6.10.2020].

Defenddigitalme (2018): *A Comparison of National Pupil Databases in the UK*. Online verfügbar unter: http://defenddigitalme.com/wp-content/uploads/2018/03/UK_pupil_data_comparison-1.pdf [Abfrage am: 6.10.2020].

Defenddigitalme and Survation (2018): *The State of Data 2018. A Poll of 1,004 of Children Aged Five to Eighteen, in the State Education System*. Online verfügbar unter: https://defenddigitalme.com/stateofdata2018-gdpr/ [Abfrage am: 6.10.2020].

Defenddigitalme (2020) Case studies: *The State of Data 2020: mapping a child's digital footprint across state education* (Report section 3.8.4) https://defenddigitalme.org/state-of-data/ (Abfrage am 07.10.2020)

Dencik, Lina / Hintz, Arne / Redden, Joanna / Warne, Harry (2018): *Data Scores as Governance: Investigating Uses of Citizen Scoring in Public Services.* Data Justice Lab, Cardiff University, UK. Online verfügbar unter: https://datajusticе.files.wordpress.com/2018/12/data-scores-as-governance-project-report2.pdf [Abfrage am: 6.10.2020].

Denham, Elisabeth (2017): *The Information Commissioner Findings on Google DeepMind and Royal Free*. Online verfügbar unter: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/ [Abfrage am: 6.10.2020].

Department for Education (DfE) (2020): *External Data Shares*. Online verfügbar unter: https://www.gov.uk/government/publications/dfe-external-data-shares [Abfrage am: 6.10.2020].

European Commission (2019): *High-Level Expert Group on AI (AI HLEG) Policy and Investment Recommendations for Trustworthy Artificial Intelligence*. Online verfügbar unter: https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence [Abfrage am: 6.10.2020].

European Data Protection Board (2020): *Guidelines on Consent Under Regulation 2016/679*. Online verfügbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [Abfrage am: 6.10.2020].

Education Select Committee (2013): *Underachievement in Education by White Working Class Childr*en - para 77. Online verfügbar unter: https://publications.parliament.uk/pa/cm201415/cmselect/cmeduc/142/14206.htm#a38 [Abfrage am: 6.10.2020].

Ekambaranathan, Anirudh / Zhao, Jun / Van Kleek, Max (2020): *Understanding Value and Design Choices Made by Android Family App Developers*. In: CHI'2020. Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA, S. 1-10.

Ferreira, Jose (2012): *CEO of Knewton, Speaking at the DataPalooza on the U.S. Department of Education YouTube Channel of the Office of Educational Technology*. Online verfügbar unter: https://youtu.be/Lr7Z7ysDluQ [Abfrage am: 6.10.2020].

Hessen Data Protection Authority (2019): *Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen.* Opinion on the Use of Cloud Storage like Amazon, Google, Microsoft 365 in State Schools under GDPR. Online verfügbar unter: https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und [Abfrage am: 6.10.2020].

ICO (2020a): *On Article 25 Data Protection by Design and Default*. Online verfügbar unter: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ [Abfrage am: 6.10.2020].

ICO (2020b): *Statement on the outcome of the ICO's compulsory audit of the Department for Education.* Online verfügbar unter: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/statement-on-the-outcome-of-the-ico-s-compulsory-audit-of-the-department-for-education/ (Abfrage am 07.10.2020)

Kaye, David (2019): *Moratorium Call on Surveillance Technology to End 'Free-for-All' Abuses: UN Expert, Recommendations*. In: UN News. Online verfügbar unter: https://news.un.org/en/story/2019/06/1041231 [Abfrage am: 6.10.2020].

Leaton Gray, Sandra / Phippen, Andy (2017) *Invisibly Blighted: The Digital Erosion of Childhood.* London: IOE Press.

Lupton, Deborah / Williamson, Ben (2017)*: The Datafied Child: The Dataveillance of Children and Implications for Their Rights*. In: New Media & Society 19(5), S. 780-794. Online verfügbar unter: https://doi.org/10.1177/1461444816686328 [Abfrage am: 6.10.2020].

Metaari (2020): *Global Edtech Investments Reach a Staggering $18.66 Billion via PRweb*. Online verfügbar unter: https://www.prweb.com/pdfdownload/16814926.pdf [Abfrage am: 6.10.2020].

Murray, Cath (2018): *A Camera in Every Classroom: Would You Do It?* In: Schools Week. Online verfügbar unter: https://schoolsweek.co.uk/a-camera-in-every-classroom-would-you-do-it/ [Abfrage am: 4.10.2020].

Nemorin, Selena (2017): *Affective Capture in Digital School Spaces and the Modulation of Student Subjectivities*. In: Emotion, Space and Society 2, S. 11-18.

NHS (2020): *Apps Library 'How the Assessment Works'*. Online verfügbar unter: https://digital.nhs.uk/services/nhs-apps-library/guidance-for-health-app-developers-commissioners-and-assessors/how-we-assess-health-apps-and-digital-tools#how-the-assessment-works.

Ruda, Simon (2019): *BIT Director of Home Affairs and International Programmes* (at 1:36) "Imminently we will be launching a trial with 75 schools and 65,000 children...". Online verfügbar unter: https://www.youtube.com/watch?v=z2Vvt8wKgYU [Abfrage am: 6.10.2020].

Selwyn, Neil (2019): *Teachers and Technology: Time to Get Serious.* In: Journal of the Chartered College. Online verfügbar unter: https://impact.chartered.college/article/editorial-education-technology/ [Abfrage am: 6.10.2020].

Shearing, Hazel (2019): *Millions Of Students' Sexual Orientations And Religious Beliefs Are Being Held On A Government Database.* In: Buzzfeed UK. Online verfügbar unter: https://www.buzzfeed.com/hazelshearing/the-government-has-a-database-of-millions-of-students [Abfrage am: 6.10.2020].

Singer, Natasha (2017): *How Google Took Over the Classroom*. In: The New York Times. Online verfügbar unter: https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html [Abfrage am: 6.10.2020].

Standaert, Michael (2019): *Chinese Primary School Halts Trial of Device that Monitors Pupils' Brainwaves*. In: The Guardian. Online verfügbar unter: https://www.theguardian.com/world/2019/nov/01/chinese-primary-school-halts-trial-of-device-that-monitors-pupils-brainwaves [Abfrage am: 4.10.2020].

Stoilova, Mariya / Livingstone, Sonia / Nandagiri, Rishita (2019): *Children's Data and Privacy Online*. Online verfügbar unter: https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf [Abfrage am: 6.10.2020].

Student Privacy Compass (2020): *Named After the Core Federal Law that Governs Education Privacy, FERPA, This is a U.S. Education Law and Privacy Resource Site*. Online verfügbar unter: https://studentprivacycompass.org/state-laws/ [Abfrage am: 6.10.2020].

Swedish Data Protection Authority (2019): *Supervision Pursuant to the GDPR (EU) 2016/679 –[DI-2019-2221] Skellefteå Municipality*. Online verfügbar unter: https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf [Abfrage am: 6.10.2020].

Taylor, Emmeline (2019): T*eaching Us to Be 'Smart'? The Use of RFID in Schools and the Habituation of Young People to Everyday Surveillance*. In: Taylor, Emmeline / Rooney, Tonya (Hg.): Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People. Emerging Technologies, Ethics and International Affairs. Oxon / New York: Routledge, S. 67-78.

UNICEF (Child Rights and Business Unit) (2018): *Discussion Paper Series: Children's Rights and Business in a Digital World. Privacy, Protection of Personal Information, and Reputational Rights*. Online verfügbar unter: https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf [Abfrage am: 6.10.2020].

Van Brakel, Rosamunde (2019): *Rise of Pre-Emptive Surveillance: Unintended Social and Ethical Consequences*. In: Taylor, Emmeline / Rooney, Tonya (Hg.): Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People. Emerging Technologies, Ethics and International Affairs. Oxon / New York: Routledge, S. 187-199.

WhatDoTheyKnow (2018): *FOI Reference: 4368666 A Freedom of Information Request from Jen Persson to Kent County Council Integrated Dataset: Children and Young People*. Online verfügbar unter: https://www.whatdotheyknow.com/request/integrated_dataset_children_and_4 [Abfrage am: 6.10.2020].

Williamson, Ben. (2017a): *Big Data in Education: The Digital Future of Learning, Policy and Practice*. London: Sage.

Williamson, Ben (2017b) *Decoding ClassDojo: Psycho-Policy, Social-Emotional Learning and Persuasive Educational Technologies, Learning, Media and Technology*, 42 (4), S. 440-453. Online verfügbar unter: https://doi.org/10.1080/17439884.2017.1278020.

Digitalisierung in der Schule – Datenschutz mitdenken

Marit Hansen

Abstract

An Schulen werden hohe Erwartungen gestellt, auch im Bereich der Digitalisierung. Schon von Kindesbeinen an sollen die Kinder und Jugendlichen mit Technik und digitalen Informationsangeboten umgehen lernen. Jedoch stehen noch nicht überall datenschutzkonforme Lösungen zur Verfügung, sodass Schülerinnen und Schüler ebenso wie Lehrkräfte Risiken in Bezug auf ihre personenbezogenen Daten und Privatsphäre ausgesetzt werden. Hier besteht Nachholbedarf. Wichtig dafür ist es, Datenschutz mitzudenken und in neue Anwendungen von Anfang an einzubauen. Dies betrifft sowohl die Basis-Arbeitsmittel für Unterricht und Schulverwaltung als auch pädagogische Lehrmaterialien. Hilfestellungen und Austausch untereinander können dazu führen, dass nicht jede Schule selbst das Rad neu erfinden muss, sondern dass Best Practices standardisiert zur Verfügung gestellt werden.

1. Startpunkt der Schulen[1]

Schule und Digitalisierung. Und Datenschutz. Passt dies alles zusammen? Noch nicht so wirklich: Der Schulalltag sieht anders aus. Während für Schülerinnen und Schüler zumindest auf den weiterführenden Schulen der Einsatz von Smartphones, das Abrufen von Fotos, Videos und Musik aus dem Internet sowie die Benutzung von Sozialen Medien in ihrem Privatleben eine Selbstverständlichkeit ist, läuft der Unterricht zumeist weit weniger digital(isiert) ab. Dabei wird von den Schulen erwartet, dass sie die Kinder und Jugendlichen auf das Leben vorbereiten, auch auf das Leben in der zunehmend digitalisierten Informationsgesellschaft. Dass sie Medienkompetenz – sowohl für das Nutzen von Angeboten als auch für das Bereitstellen von Inhalten – lehren. Dass Informatik-Sachverhalte und

1 Anmerkung: Dieser Text entstand auf Basis des Workshops „Digitalisierung in der Schule – Datenschutz mitdenken“ auf der Jahrestagung 2019 des Forum Privatheit.

technisch geprägte Themen vermittelt werden, und zwar an alle (Lautebach 2018).

Die besondere Wichtigkeit von Digitalisierung in Schulen zeigt sich in Situationen, in denen der Schulunterricht nicht physisch stattfinden kann. So zeigten sich im März 2020, als die Schulen in Deutschland aufgrund der Corona-Pandemie weitgehend geschlossen wurden und auf Fernunterricht ausweichen mussten, erhebliche Probleme im Homeschooling. Laut der internationalen Vergleichsstudie „*International Computer and Information Literacy Study*" (ICILS) hat Deutschland Nachholbedarf, beispielsweise beim schulischen WLAN für die Internet-Nutzung, wie dies in Deutschland 2018 erst 25 % der Schulen ermöglichten, während dies in Dänemark an nahezu jeder Schule Standard ist (Fraillon et al. 2020). In einer repräsentativen telefonischen Befragung von 1.003 Personen in Deutschland ab 16 Jahren, darunter 269 Eltern schulpflichtiger Kinder, im August 2020 hat der deutsche Digitalverband „Bitkom" ermitteln lassen, wie die Bevölkerung und insbesondere Eltern den Stand der digitalen Bildung einschätzt (Bitkom Research 2020). Fast alle Eltern wollten digitalen Unterricht, ist eines der Ergebnisse. Demnach stünde die Notwendigkeit der Ausstattung mit digitalen Technologien wie Computer, Smartboards oder Tablets im Vordergrund (Zustimmung von 93 % der befragten Eltern; die Werte für die Gesamtbevölkerung liegen jeweils einige Prozentpunkte darunter); dadurch sollten die Schüler auf das Leben und Arbeiten in der digitalen Welt vorbereitet werden (Zustimmung von 79 % der Eltern). Dass digitale Technologien es den Lehrkräften ermöglichten, individueller auf einzelne Schülerinnen und Schüler einzugehen, wurde in der Umfrage nicht im selben Maße bestätigt (Zustimmung von 43 % der Eltern (Bitkom Research 2020: 7)). Maßnahmen, um die Digitalisierung der Schulen voranzubringen, wurden sowohl im Bereich der Verbesserung der technischen Ausstattung der Schulen (Zustimmung von 96 % der Eltern (Bitkom Research 2020: 9)) als auch im Bereich der Lehrerfortbildungen und Anpassung der Lehrpläne an die Möglichkeiten der Digitalisierung (Zustimmung jeweils 93 % der Eltern (Bitkom Research 2020: 10)) gesehen.

Markig heißt es vom Bitkom-Präsidenten Achim Berg, dass die „Corona-Krise [...] unser Bildungssystem vor eine Zerreißprobe gestellt" hat. „Die massiven Verunsicherungen durch Behörden und Datenschutzbeauftragte haben dann auch noch die digitalen Vorreiter unter den Schulen und Lehrkräften ausgebremst." (Bitkom 2020)

Zwar enthält der online verfügbare Foliensatz zur Umfrage von Bitkom Research gar keine Aussagen zu Datenschutz, auch nicht zu weiteren öfter genannten Problemen wie beispielsweise zur notwendigen Priorisierung in den Schulen vor Ort, wenn bauliche oder Hygienemängel behoben wer-

den müssen. Aber die Verunsicherung scheint groß zu sein. Nicht erst seit der Corona-Pandemie: Schon im April 2018 äußerte sich der Lehrer Matthias Förtsch in einer Kolumne zu einer angeblichen „Diktatur des Datenschutzes“: „Was ist wichtiger? Die zeitgemäße Bildung aller Schülerinnen und Schüler oder das möglichst geringe Risiko eines potenziellen Datenmissbrauchs? Beides zusammen geht (bislang) nicht: Die Europäische Datenschutz-Grundverordnung (DSGVO) gewährleistet Datensicherheit, Datenschutzvorschriften insgesamt können aber einem modernen, digitalen und vernetzten Schulalltag auch im Weg stehen“ (Förtsch 2020).

Hier mögen Aspekte von Datensicherheit und Datenschutz etwas durcheinander geraten zu sein, denn die Datenschutz-Grundverordnung enthält Regeln zum Schutz personenbezogener Daten, wobei die Sicherheit – also Vertraulichkeit, Integrität und Vertraulichkeit – nur eine der zahlreichen Anforderungen ist, die bei einer fairen Verarbeitung zu berücksichtigen sind. Schön wäre natürlich, wenn bereits – wie bei ihrer Einführung versprochen – die DSGVO tatsächlich ihre Wirkung dahingehend entfaltet hätte, dass sämtlich Angebote und Dienstleistungen im europäischen Markt, die mit personenbezogenen Daten zu tun haben, rechtskonform gestaltet wären und damit einem Datenmissbrauch der Riegel vorgeschoben wäre. Wäre dies so, würde es die Auswahl von Systemen für Schulverwaltung oder Homeschooling und ihren rechtskonformen Einsatz stark vereinfachen. Die Realität sieht anders aus. Dass aber dennoch Datenschutz und Schulalltag keine Gegensätze sein müssen, wird im Folgenden beleuchtet.

Abschnitt 2 gibt einen Überblick über generelle Datenschutzanforderungen. Dass für „Schule“ kein „One-size-fits-all“-Ansatz funktioniert, rückt Abschnitt 3 ins Bewusstsein, der verschiedene Charakteristika je nach Einsatzszenario und die Abgrenzungsnotwendigkeiten der Akteure je nach ihrer individuellen Rolle beleuchtet. Wesentliche Herausforderungen und Trends für Digitalisierung aus Datenschutzsicht werden in Abschnitt 4 dargestellt. Schließlich gibt Abschnitt 5 Empfehlungen für Digitalisierung in der Schule, bei dem Datenschutz von Anfang an mitgedacht wird.

2. *Datenschutzanforderungen – ganz kurz*

Beim Datenschutz geht es um den Schutz der Menschen und ihrer Persönlichkeitsrechte. In der Datenschutz-Grundverordnung steht in Artikel 1 in den Absätzen 1 und 2:

> „(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
> (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten."

Mit der Digitalisierung werden immer mehr Daten verarbeitet, darunter viele mit Personenbezug. Deswegen spielen Datenschutzanforderungen häufig eine Rolle, wenn Prozesse digitalisiert werden oder wenn die Akteure sich digitaler Dienstleistungen bedienen, z. B. über Angebote im Internet. Zu den Datenschutzrisiken gehören nicht nur unberechtigte Zugriffe auf die Daten, sondern auch unfaire Arten der Datensammlung oder -auswertung, z. B. bei Überwachung oder Beobachtung des Verhaltens der Menschen. Anhand von personenbezogenen Daten lassen sich viele Schlüsse über die Personen ziehen, auf Basis derer Entscheidungen getroffen werden können. Dies ist nicht in jedem Fall illegal oder illegitim, aber stets ist Aufmerksamkeit geboten, um Fairness der Verarbeitung zu gewährleisten und beispielsweise Manipulation auszuschließen.

Schulen müssen selbstverständlich Datenschutzanforderungen in ihren eigenen papierenen oder digitalen Verarbeitungen einhalten. Zusätzlich gehört Datenschutz in den Unterricht, um einerseits die Grundsätze, die sich aus den Grundrechten und Menschenrechten ableiten, und andererseits heutige oder kommende Datenverarbeitungen mit ihren Risiken und Gestaltungsmöglichkeiten verständlich zu machen.

Kernstück der DSGVO ist Artikel 5 mit den Grundsätzen für die Verarbeitung personenbezogener Daten. In Absatz 1 werden die folgenden Grundsätze aufgelistet:

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
b) Zweckbindung
c) Datenminimierung
d) Richtigkeit
e) Speicherbegrenzung
f) Integrität und Vertraulichkeit

„Rechtmäßigkeit" bedeutet: Für die Verarbeitung personenbezogener Daten benötigt man eine Rechtsgrundlage, beispielsweise ein Gesetz, eine Einwilligung oder einen Vertrag.

Die Verarbeitung muss fair erfolgen („Treu und Glauben"). Wichtig ist auch die Transparenz der Verarbeitung, also eine verständliche Information für die betroffenen Personen. Vor der Erhebung von Daten muss man

sich bewusst machen, welchen Zwecken die Verarbeitung dienen soll, denn davon hängt ab, für welche Zwecke die personenbezogenen Daten verwendet werden dürfen („Zweckbindung"), welche Daten für die Zwecke erforderlich sind, sodass keine weiteren Daten verarbeitet werden („Datenminimierung"), für wie lange die Daten in identifizierender Form benötigt werden, sodass sie danach zu löschen sind („Speicherbegrenzung"). Außerdem muss der Verantwortliche Sorge für die „Richtigkeit" der Daten und für die Datensicherheit (insbesondere „Integrität und Vertraulichkeit") tragen, damit sie nicht unbefugt zugänglich werden.

Jede Verarbeitung personenbezogener Daten bedeutet ein Risiko; deswegen muss der Verantwortliche – das ist derjenige, der über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet – sich dessen bewusst sein und geeignete Maßnahmen treffen, um das Risiko ausreichend einzudämmen.

Da der Schulbereich in Deutschland föderal geregelt ist, gilt für die Verarbeitung von Schülerdaten das Schulgesetz des jeweiligen Bundeslandes, ergänzend das Landesdatenschutzgesetz und stets auch die DSGVO. In Schleswig-Holstein wird das Schulgesetz von einer Schul-Datenschutzverordnung flankiert, die ebenfalls Regeln zum Umgang mit personenbezogenen Daten enthält und damit konkretisierende Anforderungen und Hilfestellungen enthält. Schulverwaltungen und Lehrkräfte sind zumeist gewohnt, mit ihren Schulgesetzen zu arbeiten, da sich auf dieser Basis vielerlei Prozesse – beispielsweise das Führen von Verwaltungsakten in der Schule – etabliert haben. Es empfiehlt sich, auch bei der zunehmenden Digitalisierung zu standardisierten Lösungen zu kommen, damit nicht jede Lehrkraft oder jede Schule das Rad von Neuem erfinden muss.

3. Abgrenzungsnotwendigkeiten in der Schule

Schule ist nicht Privatvergnügen, Schule ist aber auch nicht typische Behörde. An Schule und Lehrkräfte stellen sich hohe Erwartungen. Umso wichtiger ist es, sich bewusst zu machen, welche Regeln gerade gelten, welche Rolle einzuhalten ist und wo Grenzziehungen nötig sind.

3.1 Schule: Verwaltung oder pädagogischer Auftrag

Einerseits weist die Schule einen Verwaltungscharakter auf: Die Dokumentation über die Schülerin oder den Schüler muss korrekt geführt werden

und nachvollziehbar sein, beispielsweise zu Leistungsnachweisen oder Abwesenheiten, die beispielsweise zeugnisrelevant sind. Dasselbe gilt für die Aktenführung in besonderen Situationen, die einen Schulverweis nach sich ziehen können und daher einer gerichtlichen Überprüfung standhalten können sollen.

Andererseits besteht ein pädagogischer Auftrag der Schulen, der nicht per bürokratischem Absolvieren der Unterrichtseinheiten gut zu erfüllen ist. Hier ist mehr individuelles Eingehen der Lehrkraft mit ihrer Persönlichkeit auf die Schülerinnen und Schüler vonnöten. Kreativität ist gefragt, Lehrinhalte können und sollen gerne mit aktuellen Geschehnissen in Verbindung gebracht werden.

3.2 Schulische und außerschulische Veranstaltungen: Schutzraum oder reale Welt

Generell sind die Sorgeberechtigten für ihre Kinder verantwortlich. In der Schule halten sich die Kinder aber ohne die Sorgeberechtigten auf. Das bedeutet zum einen, dass sie in der Schule vor schädigenden Einflüssen zu schützen sind, beispielsweise gemäß den Vorgaben des Jugendschutzes. Eine Lehrkraft darf daher im Unterricht keinen Film mit ungeeigneter Altersfreigabe zeigen.

Zum anderen sollen die Kinder ihre Persönlichkeit und die Befähigung zum Umgang mit der echten Welt auch im Schulbereich entwickeln können. Dies wäre aber kaum möglich, wenn die Schule ihren Schutzauftrag als vollständige Abschottung verstünde.

Während für schulische Veranstaltungen in der Regel eine Teilnahmepflicht der schulpflichtigen Kinder und Jugendlichen besteht, ist dies anders bei außerschulischen Veranstaltungen. Solche außerschulischen Aktivitäten können von der Schulleitung, Lehrkräften oder Klassengemeinschaften initiiert sein; manche ergeben sich auch beispielsweise in Zusammenarbeit mit Veranstaltern von Wettbewerben oder auf Anregung von Vereinen, Krankenkassen, Banken und Sparkassen sowie gemeinnützigen Einrichtungen. Selbstverständlich betrifft dies auch den Bereich der Digitalisierung, z. B. wenn Hardware oder Software gesponsort wird oder wenn besondere Digitalevents wie Wettbewerbe mit Bezug zur Online-Welt anstehen, bei denen die Schülerinnen und Schüler mit ihren Namen und ggf. weiteren Daten angemeldet werden. Da je nach Bundesland unterschiedliche Regularien gelten, muss man sich über den schulischen oder außerschulischen Charakter im Klaren sein. Dies betrifft auch die Frage, ob eine Einwilligung der Eltern für die Teilnahme und die oft damit ver-

bundene Weitergabe personenbezogener Daten notwendig ist und wem gegenüber sie abgegeben werden muss. Es ist ein Unterschied, ob es dabei nur um den Zweck des Teilnehmens geht oder ob zusätzlich Fotos oder Videos für den individuellen Gebrauch, für die Schul-Webseite oder für öffentliche Darstellungen in sozialen Medien gefertigt werden.

In den Schulgesetzen finden sich häufig Regelungen zum Umfang erlaubter Werbung – denn vollständig ausgeschlossen ist Werbung in den Klassenzimmern oder bei von der Schule initiierten oder unterstützten Veranstaltungen zumeist nicht. Es haben sich sogar Werbetreibende auf das Schulmarketing spezialisiert, denn schließlich handelt es sich um eine „konsumfreudige junge Zielgruppe", die „über viele Milliarden an Kaufkraft"[2] verfügt. Die damit verbunden Gefahren sehen auch Verbraucherschützer, die ein vollständiges Werbeverbot fordern (Verbraucherzentrale Bundesverband 2020). Oft übersehen werden die typischen Werbeeinblendungen beim Zeigen von Filmen aus Videoportalen oder beim Surfen im Internet, die möglicherweise sogar an die Zielgruppe oder an den jeweils verwendeten Nutzeraccount der Lehrkraft oder der einzelnen Schülerinnen und Schüler angepasst werden. Aus Datenschutzsicht sind hier die vorhandenen Datenspuren und ausgewerteten Nutzerprofile bedenkenswert; zusätzlich können Jugendschutzfragen relevant werden.

3.3 Lehrkraft: Beruf oder Privatmensch

Engagierte Mitarbeitende bringen stets ein Stück ihrer Persönlichkeit mit ein und verstehen ihren Job nicht als ungeliebte Arbeit im vorgegebenen Zeitkorsett. Dies gilt auch für Lehrkräfte. Allerdings dürfen die Grenzen nicht verschwimmen, beispielsweise wenn Jugendliche für eine Lehrkraft schwärmen und auch privat den Kontakt zu ihrem Schwarm suchen. Hier empfiehlt sich das Einhalten der nötigen Distanz und eine unmissverständliche Ausdrucksweise. Das gilt auch für die digitale Welt mit zahlreichen privaten und öffentlichen Kommunikationswegen. Statt dass Lehrkräfte über private Nutzerkonten per E-Mail, Messenger oder in anderen sozialen Medien kommunizieren, bieten sich standardisierte Schul-E-Mail-Adressen oder andere Schul-Nutzerkonten an, bei denen stets der Kontext „Schule" deutlich wird. Dies ist auch im Sinne der Fairness für das Privatleben der Lehrkräfte, denen damit eine Trennung zwischen Beruf und Freizeit ermöglicht wird und die beispielsweise generell „Freundschaftsanfragen" in

2 https://www.grundschulmarketing.de/ (Abfrage am: 21.09.2020).

sozialen Medien, in denen sie als Privatperson vertreten sind, von Schülerinnen und Schülern ablehnen sollten. Auch sollten Lehrkräfte überlegen, wann Gruppen-Nachrichten z. B. an die ganze Klasse sinnvoll sind und wann auch einmal eine individuelle (schulische) Kommunikation mit einzelnen Schülerinnen oder Schülern zu bevorzugen ist.

4. Digitalisierungsschub: brave new school world?

Wie die Bitkom-Umfrage herausarbeitet, ist der Zustand der Digitalisierung im Schulbereich noch verbesserungsbedürftig (Bitkom 2020). Mit der Corona-Pandemiesituation hat sich gezeigt, dass ein schnelles Umstellen des Unterrichts auf Online-Formate und eine Lehrer-Schüler-Kommunikation per elektronischen Medien nicht reibungslos funktioniert hat. Weder die Schulen noch die Haushalte der Schülerinnen und Schüler waren darauf vorbereitet. Es war Zufall, ob bei den Lehrkräften und Schülerinnen und Schülern geeignete Hard- und Software sowie eine ausreichende Internet-Anbindung zur Verfügung stand, die z. B. für Videokonferenzen und Kollaborationstools geeignet ist. Auch wenn ein Notebook im Haushalt dafür nutzbar war, konnte es bei mehreren schulpflichtigen Kindern schwierig sein, den Online-Schulunterricht zu organisieren. Vorteilhaft wäre es gewesen, wenn jedes Schulkind mit der (standardisierten) Hard- und Software ausgestattet gewesen wäre, wie es seit Jahren in skandinavischen Schulen gehandhabt wird und nun auch in Deutschland zunehmend geschieht.

Ein weiteres Problem jedoch bestand und besteht in dem Angebot der Dienste, die häufig Mängel bezüglich des Datenschutzes und der Datensicherheit aufweisen. In der plötzlichen, durch Corona bedingten Schulschließsituation im März 2020 waren viele Schulen nicht handlungsfähig, selbst wenn landesweit über die Kultusministerien einige Hilfestellungen zu Auswahlkriterien und geeigneten Angeboten für das Homeschooling gegeben wurden.[3] Zwar war man sich in vielen Fällen der abstrakten Kriterien bewusst, z. B. dass die Angebote datenschutzkonform sein sollten. Es war aber nicht jedem von Anfang an klar, dass dies auch bedeutete, sich mit Verschlüsselung beispielsweise bei Videokonferenzen, mit Server-Standorten innerhalb des Europäischen Wirtschaftsraums oder an anderen

3 Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQ.SH): *Einsatz von digitalen Angeboten während der Corona-Krise.* 2020. Online verfügbar unter: https://medienberatung.iqsh.de/corona2.html (Abfrage am: 21.09.2020).

Orten mit angemessenem Datenschutzniveau, mit der Einbindung von Unterauftragnehmern, die keine zusätzlichen Risiken verursachen dürfen, und natürlich mit Geschäftsmodellen zu beschäftigen, die teilweise auf Analyse der Nutzerdaten (hier: Schülerinnen und Schüler) zielten. Einfacher schien es einigen Akteuren, die Kommunikation über (vermeintlich) bei allen Schülerinnen und Schülern verfügbaren Tools wie WhatsApp auf den Smartphones der Jugendlichen zu führen, was jedoch aus Datenschutzsicht alles andere als empfehlenswert war. Die Kritik der Datenschützer betrifft beispielsweise die nicht zu deaktivierende Synchronisation der (gehashten) Telefonnummern in den Adressbüchern der Smartphones mit den WhatsApp-Servern, sodass auch personenbezogene Daten von unbeteiligten Personen erfasst sind. Auch dass WhatsApp eine Tochter von Facebook und damit ein Datenaustausch unter beiden möglich ist, spricht gegen den Einsatz dieses Messengers.

Auf keinen Fall sollten Personen, die aus Datenschutzgründen kritische Angebote ablehnen, im schulischen Kontext dazu gezwungen werden – hier dürfen keine Abstriche gemacht werden. Wenn verbreitete Lösungen, die aus Privatinteresse von einigen oder sogar vielen Schülerinnen und Schülern verwendet werden, nicht datenschutzkonform sind, dürfen sie nicht als Blaupause für den schulischen Einsatz dienen, zumal es vielfach bessere Angebote gibt oder man Veränderungen bei den Anbietern einfordern kann. In der Tat zeigte sich im Jahr 2020 während der Corona-Pandemie, dass auf Nachfrage mehr Datenschutz und Datensicherheit in Homeoffice- oder Homeschooling-Lösungen realisiert wurde.[4]

Standardisierte Lösungen für schulische E-Mail-Adressen für Lehrkräfte und für Schülerinnen und Schüler oder die Nutzung einer Schul-Cloud gab es zumindest nicht flächendeckend in Deutschland. Das Problem ist jedoch komplexer. Schnellschüsse oder ein unkritisches Implementieren jeder technischen Lösung sind nicht angeraten – aber man kann aus den

4 Jedoch sind auch Ende des Jahres 2020 Datenschutzanforderungen zum internationalen Datentransfer, wie sie der Europäische Gerichtshof (EuGH) in seinem Urteil vom 16.07.2020, C-311/18, formuliert hat, bei Servern im außereuropäischen Ausland noch nicht überall umgesetzt. In dieser Entscheidung erklärte der EuGH das Abkommen „Privacy Shield", das für viele Dienste als Rechtsgrundlage zum Austausch personenbezogener Daten mit den USA diente, für unwirksam und machte am Beispiel der Zugriffsmöglichkeiten für US-Nachrichtendienste deutlich, dass die Daten der europäischen Bürgerinnen und Bürgern nicht ohne bessere Garantien, z. B. einen ausreichenden Rechtsschutz, ins Ausland transferiert werden dürfen.

folgenden Beispielen lernen, die heute schon in Deutschland oder anderswo Wirklichkeit sind oder es zumindest bald sein könnten.

4.1 Dienstleister mit eigenen Interessen

Im Bereich der Digitalisierung geht es nicht nur um das Schalten von Werbung, sondern um das Gewinnen von jahrelangen – vielleicht sogar lebenslangen – Kundinnen und Kunden: Schülerinnen und Schüler, die standardmäßig mit Hardware, Software und Nutzerkonten eines Anbieters ausgestattet werden, können durch Gewöhnung an das „Look & Feel" der User Interfaces auch nach ihrer Schulzeit die Dienste nutzen wollen. Das gilt umso mehr dann, wenn der Haushalt ebenfalls solche oder ähnliche Angebote nutzt, was vorteilhaft sein kann, wenn ansonsten die Geräte in der Schule verbleiben, aber man von zu Hause aus an seinen Projekten weiterarbeiten möchte. Außerdem kann es unbequem sein, wenn man den Anbieter wechseln möchte, nachdem man sich alles so konfiguriert hat, wie es einem am besten gefällt, und dort auch vielleicht weitere Daten gespeichert hat, die erst mühsam zusammengesammelt werden müssten. Deswegen läuft ein Kampf um die Kundenakquise im Klassenzimmer, bei dem große Anbieter sich auch über attraktive Angebote für Großaufträge oder andere Arten eines Sponsorings in Stellung bringen (siehe auch Harris 2016).

Wie auch in anderen Bereichen der Digitalisierung gewohnt, dominieren wenige globale Anbieter den Markt. Es fehlt in Deutschland und Europa an digitaler Souveränität. Problematisch ist eine wachsende Abhängigkeit von diesen wenigen Anbietern. Für öffentliche Stellen hat insbesondere Microsoft mit seiner Office-Umgebung eine Quasi-Monopol-Funktion, sodass es Alternativen schwer haben – auch in der Schule (Kuketz 2020). Apple wiederum stellt „Apple Education Specialists" zur Verfügung, die umfassend beraten, wie Digitalisierung im Schulbereich funktioniert – natürlich mit Angeboten von Apple.[5]

Auch wenn es nicht um die Grundausstattung der Schülerinnen und Schüler geht, kommt man für die Anwendungen und Online-Angebote in eine ähnliche Situation, denn Anbieter für Videos (wie YouTube) oder für Suchmaschinen (wie Google oder Bing) verfolgen mit den Nutzungsdaten eigene Zwecke. Auch sind viele Webseiten mit Tracking-Tools ausgestattet,

5 https://www.apple.com/de/education/how-to-buy/education-specialist/ (Abfrage am: 21.09.2020).

die wiederum bestimmte Daten der Schülerinnen und Schüler erfassen und auswerten können. Zudem sind die Kinder und Jugendlichen der Internet-Werbung ausgesetzt, wenn dies nicht aktiv – z. B. durch den Einsatz von Werbeblockern – unterbunden wird.

4.2 Überwachungsaufrüstung

Überwachungsfreie Räume werden immer seltener – das gilt auch für Schulen. Während in Deutschland vielfach genau abgewogen wird, unter welchen Bedingungen in welchen Zeiten welche Bereiche des öffentlichen Raums von einer Videoüberwachung umfasst sein dürfen und im Schulbereich auch Schulträger, Lehrkräfte, Eltern oder die Schülervertretung mitdiskutieren, wird dies in anderen Ländern häufig nicht infrage gestellt. Mittlerweile beschäftigen sich einige Untersuchungen mit dem Effekt, den eine Überwachung auf Schülerinnen und Schüler oder auch auf Studierende haben (Lindstrom et al. 2018, Birnhack/Perry-Hazan 2020): teilweise werden Videoüberwachungen aus Sicherheitssicht begrüßt, aber aus Datenschutzgesichtspunkten sehen viele Personen darin einen Eingriff in ihre Privatsphäre.

Fälle von heimlicher Überwachung, beispielsweise über ausgegebene Schul-Notebooks per Webcam ins Kinderzimmer, werden nicht nur in Deutschland besonders kritisch gesehen (Zips 2010). Ähnliches gilt für Situationen, in denen Kinder und Jugendliche andere Schülerinnen und Schüler oder Lehrkräfte heimlich per Smartphone aufnehmen und durch Verbreiten der Aufnahmen lächerlich machen.

Jedoch geht die Überwachung gar nicht in allen Fällen von den Schulen oder Schülerinnen und Schülern aus. So statten einige Eltern ihre Grundschulkinder mit Smartwatches aus, die mit einer Funktion zum Fernaktivieren der Tonübertragung („Remote Voice Monitoring") ausgestattet sind. Damit wollen sie bei Bedarf in den Unterricht hineinlauschen und überprüfen, ob ihre Sprösslinge fair von Lehrkräften oder Mitschülerinnen und Mitschülern behandelt werden. Manchmal mischen sich die Eltern aus der Ferne auch direkt ein: Die Smartwatch überträgt dann ihre Stimme in den Klassenraum. An vielen Schulen hat man den Einsatz solcher Geräte untersagt;[6] falls Kinder doch damit ausgestattet sind, müssen sie die

6 Zum Beispiel: Niedersächsische Landesschulbehörde: *Smartwatches im Schulalltag: Eine (datenschutzrechtliche) Herausforderung.* Online verfügbar unter: https://www.landesschulbehoerde-niedersachsen.de/themen/schulorganisation/datenschutz/daten

Smartwatches für die Unterrichtszeit abgeben. Generell unterfallen Geräte mit heimlicher Abhörfunktion der Kategorie der verbotenen Sendeanlagen.[7]

Mit dem Homeschooling stellen sich Fragen, ob auch in die Zimmer der Kinder und Jugendlichen hineingeschaut werden darf, um festzustellen, ob weitere Personen anwesend sind und unbefugte Hilfestellung geben könnten. Zumindest für das Ablegen von Prüfungen wurde dies bereits an Hochschulen praktiziert, jedoch darf man bezweifeln, dass dies auf Basis einer gültigen Einwilligung geschehen ist (Schneider 2020).

Eine Überwachung kann technisch auch über besondere Tracking-Apps erfolgen, die die Lernenden auf ihrem Smartphone installieren. Im Fall einer US-amerikanische Hochschule sollte anhand der App „SpotterEDU" festgestellt werden, inwieweit die Studierenden den Unterricht schwänzten, zu spät kamen oder zu früh gingen. Außerdem ließ sich feststellen, inwieweit die Studierenden miteinander interagierten oder bestimmte Orte mieden. Man wollte Einzelgänger herausfinden, die vielleicht psychische Probleme hatten, oder aus dem Umstand, dass jemand nie die Cafeteria aufsuchte, ableiten, dass eine Essstörung vorliegen könne (Harwell 2019).

Noch Zukunftsmusik für deutsche Schulen sind Gehirnanalysen per EEG, die angeblich ein individuell zugeschnittenes Lernen ermöglichen sollen. Bedenken bestehen aber, wenn man die Aufmerksamkeit der Schülerinnen und Schüler immer mehr kontrolliert, um Tagträumereien und abschweifende Gedanken einzufangen und die Lernleistung zu optimieren (Tangens 2020). Selbst wenn ein „Gedankenlesen" durch Technik weit weg erscheint, wird an einer Analyse von Reaktionen und Emotionen der Personen gearbeitet. Schon in der Praxis eingesetzt – wenn auch noch nicht in deutschen Schulen – werden Analysesysteme, die Gesichtsausdrücke, Augenbewegungen oder die Stimme auswerten können (Hansen 2021). Dies kann zur Unterstützung der Menschen dienen, birgt aber auch das Risiko einer Manipulation, wenn aus den Daten hervorgeht, wie man z. B. eine positive Reaktion einer Person hervorrufen kann oder worauf sie schnell gestresst reagiert.

---

schutz-im-schulalltag/smartwatches-im-schulalltag-eine-datenschutzrechtliche-herausforderung-1 (Abfrage am: 21.09.2020).

7 Bundesnetzagentur: *Missbrauch von Sendeanlagen – Hinweise zu einzelnen Produktkategorien.* Online verfügbar unter: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Datenschutz/MissbrauchSendeanlagen/HinweiseProduktkategorien/hinweiseproduktkategorien-node.html (Abfrage am: 21.09.2020).

4.3 (Un-)Faire Entscheidungen durch Künstliche Intelligenz

Im Schulbereich wird angestrebt, schul- und regionenübergreifend vergleichbare Bewertungen der Leistungen zu gewährleisten. Hier kommen mittlerweile algorithmische Systeme, teilweise basierend auf Methoden der Künstlichen Intelligenz, zum Einsatz. In Großbritannien zeigte sich damit jedoch ein Problem, denn in fast 40 % der Fälle wurden die Leistungen der Schülerinnen und Schüler heruntergestuft (Quinns/Adams 2020). Zwar hätte der Einsatz von Algorithmen sogar das Potenzial zu mehr Gerechtigkeit, als dies bei Bewertungen durch menschliche und vorurteilsbehaftete Lehrkräfte der Fall ist. Jedoch zeigt sich immer wieder, dass der Einsatz von Künstlicher Intelligenz inhärente Verzerrungen aus der realen Welt nicht ausgleicht, sondern vielmehr verstärkt. Wenn beispielsweise in dem Vorjahr der schlechteste Schüler von Schule X kommt, darf daraus nicht – wie es wohl im britischen Bewertungssystem der Fall war – folgen, dass im aktuellen Jahr wieder ein Schüler an der Schule X die schlechteste Note erhält. Gute Schülerinnen und Schüler, die öffentliche Schulen in ärmeren Bezirken Londons besuchten, hatten bei diesem Algorithmus gar keine Chance, leistungsgerecht bewertet zu werden.

Trotz dieses Debakels wird der künstlichen Intelligenz eine große Rolle in der Schule der Zukunft zugeschrieben. Dies betrifft nicht nur (möglichst faire) Bewertungen, sondern auch das differenzierte und individualisierte Lernen, bei dem das technische System passgenau auf die Fähigkeiten und Potenziale der Lernenden eingehen kann. Im Vergleich dazu fehlt es Lehrkräften an der Zeit oder manchmal auch an der nötigen Geduld für genau auf die jeweilige Person zugeschnittene Wissensvermittlung. Dies betrifft auch Menschen mit Behinderungen, die von besonderer Unterstützung profitieren. Hier stellen sich jedoch nicht nur Datenschutzfragen: Beispielsweise kann der Mehrwert einer vertrauensvollen Lehrer-Schüler-Beziehung (siehe Abschnitt 3.3), die auch von der sozialen Interaktion lebt, damit nicht ersetzt werden.

5. Ergebnisse und Schlussfolgerungen

Dass Fortschritte bei der Digitalisierung in den Schulen notwendig sind, wird keiner bezweifeln. Natürlich ist dafür eine Grundausstattung an Hardware, Software und ausreichender Internet-Anbindung sowohl in den Schulen als auch zu Hause bei den Lehrkräften sowie Schülerinnen und Schülern erforderlich. Empfehlenswert ist eine einheitliche schulische Ausstattung, da ansonsten einige Personen Vor- und andere Nachteile in der

Nutzung haben könnten. Mindestens genauso wichtig ist es, die Lehrkräfte für die Digitalisierung und ihre Chancen und Risiken zu sensibilisieren und auszubilden.

Einige Basisdienste – beispielsweise schulische E-Mail-Adressen, digitale Kalender oder Dokumentablagen – sollten generell für alle bereitgestellt werden: Hier sind die Kultusministerien gefragt, und in mehreren Bundesländern läuft dies auch schon gut. Man muss hier zusätzlich berücksichtigen, dass es nicht nur eine Frage der Technikentwicklung ist, sondern auch der Betrieb geregelt ablaufen muss, z. B. wenn die Nutzerinnen und Nutzer ihre Passwörter vergessen, dass man ein Verfahren für neue und ausgeschiedene Nutzende benötigt und wie man auf gemeldete Datenpannen reagiert. Auch stellt sich die Frage nach der betreibenden Instanz: ein öffentliches Rechenzentrum, das Kultusministerium oder ein privater Anbieter. Man muss sich auch überlegen, ob nur Lehrkräfte und Schülerinnen und Schüler oder auch Sozialarbeiterinnen und Sozialarbeiter in den Schulen oder Eltern ebenfalls darüber angebunden sein sollen.

Auch wenn der Schulbereich Ländersache ist, steht dies einer länderübergreifenden Kooperation beim Konzipieren und Implementieren von Lösungen nicht entgegen. Auch innerhalb der Bundesländer können sich die Schulen mit ihren Erfahrungen austauschen und von Synergien profitieren.

Bei der Auswahl von Dienstleistern und Anbietern darf nicht aus dem Blick geraten, dass Schulen aus wirtschaftlicher Sicht – Kaufkraft, Kundenbindung – interessant sind, aber man genau deswegen jede Abhängigkeit oder gar Beeinflussung der Schülerinnen und Schüler vermeiden sollte. Eigene Entwicklungen, z. B. auf Open-Source-Software, können einen Beitrag zur digitalen Souveränität leisten, die der Bund und die Länder ebenso wie Europa anstreben.

Für die Schulen für Ort gilt es, sich klare Regeln zu geben (oder auch von den Kultusministerien einzufordern), welche Tools und Anwendungen unter welchen Bedingungen eingesetzt werden können, besonders im Bereich der Schulverwaltung und für schulische Veranstaltungen. Sollen beispielsweise eigene Endgeräte (Bring-your-own-device) genutzt werden, und wie werden die Geräte gegen unberechtigte Zugriffe geschützt? Wer kümmert sich um Updates oder um die Wartung von Hard- und Software? Welche Kommunikationsmittel sollen auf Klassenfahrten Verwendung finden, z. B. mit Mobiltelefonen? Dürfen Lehrkräfte bestimmte Kommunikation ausschließen, z. B. wenn sie von Eltern über private Adressen, etwa per WhatsApp, kontaktiert werden? Wie kann und soll ein Fernunterricht technisch unterstützt werden? Sollen spezielle digitale Hilfsmittel für individualisiertes Lernen zum Einsatz kommen, die mehr Daten über die

Schülerinnen und Schüler auswerten? Wann benötigt man eine Einwilligung der Eltern oder der Jugendlichen? Dies alles ist auch wichtig, um den Lehrkräften Sicherheit für ihr Tun zu geben und sie vor überbordenden Erwartungen beispielsweise der Eltern zu schützen.

Für den pädagogischen Bereich – im Unterricht – ist ein breiterer Blick auf die verfügbaren Angebote wesentlich, beispielsweise indem man nicht nur eine Suchmaschine oder eine Quelle in den Vordergrund stellt, sondern kritisch den Einsatz verschiedener Angebote beleuchtet. Dazu gehört auch, dass man sich im Unterricht mit Datenschutzerklärungen oder Allgemeinen Geschäftsbedingungen beschäftigt, über Klarnamenpflicht, Pseudonyme und anonyme Nutzung diskutiert und praktische Erfahrungen im Selbstdatenschutz macht. Es bestehen zahlreiche Angebote von Medienanstalten, Polizei, Verbraucherschutz und Datenschützern, die bei Bedarf von Schulen angefordert werden und spezifisch für Klassen, Schulentwicklungstage der Lehrkräfte, Projektwochen oder Elternabende zugeschnitten sein können.[8]

8 Beispielsweise die Angebote des Medienscouts e. V., http://medienscout.info/, des Verbraucherzentrale Bundesverband (vzbv) e. V., https://www.verbraucherbildung.de/suche/materialkompass, der Initiative „Datenschutz geht zur Schule" des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V., https://www.bvdnet.de/datenschutz-geht-zur-schule/, oder auch Veranstaltungen in den einzelnen Bundesländern wie der Datenschutzakademie Schleswig-Holstein, https://www.datenschutzzentrum.de/akademie/, oder des Offenen Kanals Schleswig-Holstein, https://www.oksh.de/mitmachen/lernen/medienkompetenz-mk-fuer-schule/ (Abfrage am: 21.09.2020).

Literatur

Birnhack, Michael / Perry-Hazan, Lotem (2020): *School Surveillance in Context: High School Students' Perspectives on CCTV, Privacy, and Security.* In: Youth & Society 52 (7), S. 1312–1330.

Bitkom (2020): *Corona-Note „mangelhaft": Eltern gehen mit Schulen hart ins Gericht.* Pressemitteilung des Bitkom vom 14.09.2020. Online verfügbar unter: https://www.bitkom.org/Presse/Presseinformation/Corona-Note-mangelhaft-Eltern-gehen-mit-Schulen-hart-ins-Gericht (Abfrage am: 21.09.2020).

Bitkom Research (2020): *Digitale Schule in Corona-Zeiten.* Präsentation von Achim Berg, Bitkom-Präsident. Online verfügbar unter: https://www.bitkom.org/sites/default/files/2020-09/prasentation-bitkom-pk-digitale-schule-in-corona-zeiten-14-09-2020_final.pdf (Abfrage am: 21.09.2020).

Förtsch, Matthias (2018): *Diktatur des Datenschutzes.* Kolumne. Das Deutsche Schulportal. 23.04.2018. Online verfügbar unter: https://deutsches-schulportal.de/kolumnen/zukunft-der-schule-diktatur-des-datenschutzes/ (Abfrage am: 21.09.2020).

Fraillon, Julian / Ainley, John / Schulz, Wolfram / Friedman, Tim / Duckworth, Daniel (2020): *Preparing for Life in a Digital World – IEA International Computer and Information Literacy Study 2018 International Report.* International Association for the Evaluation of Educational Achievement (IEA). Springer.

Hansen, Marit (2021): *Private Haushalte.* In: Hornung, Gerrit / Schallbruch, Martin (Hg.): IT-Sicherheitsrecht. Praxishandbuch. Nomos, S. 620 ff. Im Erscheinen.

Harris, Ainsley (2016): *How Google Is Schooling Apple And Microsoft In the Battle For America's Classrooms.* Fast Company, 12.09.2016. Online verfügbar unter: https://www.fastcompany.com/3062958/how-google-is-schooling-apple-and-microsoft-in-the-battle-for-americas-classrooms (Abfrage am: 21.09.2020).

Harwell, Drew (2019): *Colleges are turning students' phones into surveillance machines, tracking the locations of hundreds of thousands.* In: The Washington Post, 24.12.2019. Online verfügbar unter: https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/ (Abfrage am: 21.09.2020).

Kuketz, Mike (2020): *Bildungswesen: Entlarvung der häufigsten Microsoft-Mythen.* Blog-Beitrag. Online verfügbar unter: https://www.kuketz-blog.de/bildungswesen-entlarvung-der-haeufigsten-microsoft-mythen/ (Abfrage am: 21.09.2020).

Lautebach, Urs (2018): *Informatik für alle! Ein Plädoyer.* 01.02.2020. Online verfügbar unter: https://gi.de/themen/beitrag/informatik-fuer-alle-ein-plaedoyer-1 (Abfrage am: 21.09.2020).

Lindstrom Johnson, Sarah / Bottiani, Jessika / Waasdorp, Tracy E. / Bradshaw, Catherine P. (2018): *Surveillance or Safekeeping? How School Security Officer and Camera Presence Influence Students' Perceptions of Safety, Equity, and Support.* In: Journal of Adolescent Health 63 (6), S. 732–738.

Quinn, Ben / Adams, Richard (2020): *England exams row timeline: was Ofqual warned of algorithm bias?* In: The Guardian, 20.08.2020. Online verfügbar unter: https://www.theguardian.com/education/2020/aug/20/england-exams-row-timeline-was-ofqual-warned-of-algorithm-bias (Abfrage am: 21.09.2020).

Schneider, Marcel (2020): *Jura-Klausuren aus dem Homeoffice.* In: Legal Tribune Online, 19.03.2020. Online verfügbar unter: https://www.lto.de/recht/studium-referendariat/s/corona-virus-jurastudium-klausuren-homeoffice-bucerius-law-school-debatte-taeuschung/ (Abfrage am: 21.09.2020).

Tangens, Rena (2020): *Big Brother Awards 2020: Preisträger Firma Brainco und der Leibniz-Wissenschaftscampus der Uni Tübingen.* Laudatio am 18.09.2020. Online verfügbar unter: https://bigbrotherawards.de/2020/bildung-brainco-und-leibniz-wissenschaftscampus-tuebingen (Abfrage am: 21.09.2020).

Verbraucherzentrale Bundesverband (vzbv) e. V. (2020): *Keine Werbung in der Schule. Aktivitäten von Wirtschaft im Bildungsbereich wirksam begrenzen und kontrollieren.* Positionspapier der Verbraucherzentralen und des Verbraucherzentrale Bundesverbands e. V., 05.03.2020. Online verfügbar unter: https://www.vzbv.de/sites/default/files/downloads/2020/03/11/20-03-05_wirtschaft_in_schule_ak_vz_positionspapier_und_anhang.pdf (Abfrage am: 21.09.2020).

Zips, Martin (2010): *USA: Kamera in Schul-Laptops. Per Webcam direkt ins Kinderzimmer.* In: Süddeutsche Zeitung, 23.02.2010. Online verfügbar unter: https://www.sueddeutsche.de/karriere/usa-kamera-in-schul-laptops-per-webcam-direkt-ins-kinderzimmer-1.20027 (Abfrage am: 21.09.2020).

Kriterien für die Auswahl privatsphäreschützender Messenger-Dienste für Einrichtungen der Sozialen Arbeit

Isabel Zorn, Jule Murmann und Asmae Harrach-Lasfaghi

Abstract

Einrichtungen der Sozialen Arbeit suchen nach nützlichen und rechtlich unbedenklichen Optionen für professionelle digitale Kommunikation. Insbesondere Messenger-Kommunikation (und hier besonders WhatsApp) ist stark im privaten Alltag von Adressat*innen der Sozialen Arbeit integriert. Kann Messenger-Kommunikation daher in der Sozialen Arbeit genutzt werden? Bei der Auswahl geeigneter professioneller Kommunikationstools werden umfangreiche Informationen über die Struktur und Eigenschaften von diversen Kommunikationstools benötigt, damit Einrichtungen begründete Entscheidungen für die Gestaltung ihrer digitalen Kommunikation treffen können. Der Beitrag skizziert die besonderen Anforderungen von Einrichtungen der Sozialen Arbeit bei der Auswahl geeigneter Software am Beispiel Messenger. Aus diesen Anforderungen werden Kriterien für benötigte Informationen als Entscheidungsgrundlage für die Softwareauswahl in drei Kategorien vorgestellt: Datenschutz/Privatsphäre, Barrierearmut, Praktikabilität.

1. Einleitung

Einrichtungen der Sozialen Arbeit sind konfrontiert damit, Entscheidungen darüber zu treffen, ob und wie sie mit ihren Adressat*innen digital kommunizieren. Wegen ihrer Verbreitung und häufigen Nutzung durch Adressat*innen und ihrer nützlichen Features kommen zunehmend ungeplant und auch geplant Messenger-Apps zum Einsatz zur Kommunikation zwischen Fachkräften und Adressat*innen der Sozialen Arbeit (MEKOcloud 2018). Es sollte vermieden werden, dass immer wieder einzelne (oft engagierte!) Mitarbeitende in Einrichtungen mit der Absicht der Verbesserung eines Prozesses mit Kolleg*innen oder Adressat*innen auf dem dienstlichen oder privaten Handy per WhatsApp kommunizieren und damit bewusst oder unbewusst unter Umständen Rechtsverstöße begehen,

z.B. durch Weitergabe der Kontaktdaten aller Personen im Adressbuch ohne deren Einverständnis an das Unternehmen WhatsApp.

Die Wahl solcher Kommunikationskanäle drückt eine Prioritätensetzung im Spannungsfeld zwischen Erreichbarkeit, Zugänglichkeit der Sozialen Arbeit für junge Menschen, Anpassung an Nutzungsgewohnheiten der Adressat*innen sowie der (eventuell nicht hinreichenden) Ausrichtung an Datenschutzgesetzen aus. Entscheidungen der Einrichtungen darüber, ob und welche Software oder Apps (im Folgenden: Software) sie nutzen, benötigen als Grundlage ausreichend gesicherte Informationen darüber, worauf bei der Auswahl zu achten ist und wie einzelne Softwares diese Anforderungen erfüllen. Bislang ist die Informationslage dünn. Zum einen liegen nicht ausreichend aussagekräftige und vergleichbare Daten über die einzelnen Softwares vor. Zum anderen benötigen Einrichtungen der Sozialen Arbeit häufig systematisierte Anforderungskriterien. Wissenschaftliche Literatur zu den Anforderungen solcher Einrichtungen an interne und externe Kommunikation zur Erfüllung ihrer pädagogischen oder sozialarbeiterischen Aufgaben ist kaum existent: Welche Aufgaben sollen und müssen durch Messenger-Kommunikation unterstützt werden? Welche Features können dafür störend oder hilfreich sein? Worauf ist bei der Inklusion der Adressat*innen zu achten? Welche Themen oder Kontexte erfordern oder verbieten die Nutzung von Messengern? Welche rechtlichen, ethischen und organisatorischen Konsequenzen kann die Messenger-Kommunikation nach sich ziehen? Welche Akzeptanz von Messenger-Alternativen zu WhatsApp ist durch die Adressat*innen zu erwarten? Der beschriebene Mangel an Informationen und Alternativen begründet möglicherweise, warum bislang nur wenige Einrichtungen systematisch Messenger einsetzen. Der Bedarf an geeigneten Informationen darf als hoch eingeschätzt werden, wenn Jugendeinrichtungen hier bislang wenig bereitstellen und ihre Mitarbeitenden und Adressat*innen trotz Bedenken über Privatsphäre „googeln", „skypen", „doodeln" und „whatsappen" und somit sensible Daten von teilweise schutzbedürftigen Menschen preisgeben.

Das vorliegende Kapitel zielt darauf, die Anforderungen von Einrichtungen der Sozialen Arbeit an potenzielle Messenger-Kommunikation systematisch zu eruieren und geht der Frage nach: *Welche Kriterien müssen und können Einrichtungen der Sozialen Arbeit bei der Auswahl einer Messenger-Software zugrunde legen?*

2. Wachsender Bedarf an digitaler Kommunikation in der Sozialen Arbeit

Fast alle Jugendlichen besitzen ein Smartphone. WhatsApp zählt für sie zu den beliebtesten Apps und zur aktivsten Internetbeschäftigung von 93% aller Jugendlichen mit einer durchschnittlichen täglichen Zahl von 27 Nachrichten (mpfs 2020: 30f). Sie nutzen WhatsApp, Youtube, GoogleDocs zur Organisation von Schule, Freizeit, Kommunikation und erfreuen sich zunehmender Nutzung durch junge Lernende. Junge Menschen suchen eigene Lösungen zur digitalen Kommunikation passend zu ihren Bedarfen. Dabei besteht das Risiko, dass sich Apps durchsetzen, die nicht nach Potenzialen für Datenschutz und Inklusion ausgewählt wurden und es so keine greifende Regelung geben kann. Wenn Einrichtungen wie z.B. Schulen Apps zur Verfügung stellen, werden diese tatsächlich ebenfalls genutzt (mpfs 2020: 29).

Digitale Kommunikationsbedarfe finden sich auch im Kontext Sozialer Arbeit: beispielsweise Öffentlichkeitsarbeit, Abfragen für Termine, Bekanntgabe von Veranstaltungen, Teilen von Fotos von Veranstaltungen, Erinnerungen an Zeiten und Treffpunkte, Absprachen unter den Fachkräften, Austausch über einen Fall, Dokumentation von Misshandlungen oder Wohnsituationen oder die schnelle Zusendung von Unterlagen. Man mag einwenden, dass all dies auch ohne Messenger möglich war und ist, doch ist zu vermuten, dass viele der genannten Kommunikations- und Informierungsbedarfe bereits über Messenger erfolgen.

Die Soziale Arbeit adressiert entsprechend ihres Auftrags Menschen, die zu eher benachteiligten, vulnerablen Gruppen gehören. Oft sind ihre finanzielle Situation, ihre Lebenssituation, ihr Bildungsstand, ihre Teilhabemöglichkeiten unterdurchschnittlich;; manche sind schlecht erreichbar, wenn sie beispielsweise keinen Wohnsitz und somit keine Postadresse und keinen Festnetzanschluss haben, wenn sie in Gemeinschaftseinrichtungen oder in stark reglementierten Lebensformen leben; sie nutzen evt. nur ein Handy mit Prepaidkarte ohne Guthaben; sie sind von weiteren Benachteiligungen bedroht. Dies betrifft beispielsweise wohnungslose, obdachlose und verarmte Menschen, geflüchtete Menschen, Jugendliche, von häuslicher Gewalt betroffene Frauen oder Kinder. Die Chance, jene Menschen zu erreichen, scheint daher über internetbasierte Kommunikationsformen – wie beispielsweise WhatsApp – aussichtsreich und ist daher zur Erfüllung der Aufgaben für Fachkräfte der Sozialen Arbeit attraktiv. Zudem ist denkbar, dass viele Adressat*innen diese Form der Kommunikation einer ungewohnten brieflichen Kommunikation vorziehen. Somit erfolgt durch diese Nutzung eine Orientierung an ihrer Lebenswelt. Mit diesen Menschen internetbasierte Teilhabeformen einzuüben, kann zudem dazu bei-

tragen, ihre Teilhabechancen zu erweitern (z.B. beschreiben Bosse et al. 2016 die Teilhabemängel in stationären Einrichtungen der Jugend-/Behindertenhilfe).

3. Risiken und Problematiken des Einsatzes von Messengern in der Sozialen Arbeit

3.1. Datenschutz

Personenbezogene Daten dürfen laut DSGVO ausschließlich aufgrund von bestimmten Rechtsgrundlagen und entsprechend des Vertragszwecks und ansonsten nur mit expliziter wirksamer Einwilligung der Betroffenen erhoben, verarbeitet und gespeichert werden. Sie regelt die Grundsätze der Verarbeitung (§ 5), ihre Rechtmäßigkeit (§ 6), die Bedingungen zur Einwilligung (§ 7) sowie die für die Soziale Arbeit besonders relevante Verarbeitung „besonderer Kategorien personenbezogener Daten", dazu zählen besonders sensible Daten. Personenbezogene Daten sind z.B. E-Mailadresse, Telefonnummer, IP-Adresse, Sprache, Tippgeschwindigkeit, Verbleibsdauer, Interessen, Eigenschaften, Kontakte, wenn sie auf eine Person zurückführbar sind. Idealerweise erfolgen Verarbeitungen nur im Kontext des Vertragszwecks und benötigen laut DSGVO keine Einwilligungen! Zusätzliche Einwilligungsabfragen können somit oft ein Zeichen dafür sein, dass zusätzliche, für den Vertragszweck unbenötigte Daten erhoben und verarbeitet werden. Sie werden oft durch Einwilligung in nicht gelesene oder nicht verstandene AGBs eingeholt. Dies erfolgt u.a. bei den oben genannten Softwareangeboten (WhatsApp, Youtube, GoogleDocs). Die Softwares geben die erhobenen Daten an Firmenserver weiter, wo sie gespeichert und verarbeitet werden. Der Datentransfer erfolgt oft unsichtbar, oft unbemerkt im Hintergrund der App. WhatsApp überträgt regelmäßig das gesamte Adressbuch eines Handynutzers an die Firmenserver in den USA, also auch die Daten von nicht einwilligenden Personen. WhatsApp erhebt viele Informationen über die Nutzer*innen und ihre Geräte, einschließlich Geräte-ID und gleicht diese mit der Geräte-ID ab, die z.B. für Facebook genutzt wird, sodass Details über die Nutzenden verknüpfbar sind, z.B. Fotos, Vorlieben, Interessen, Verhalten, Likes. (Pehl/Knödler 2020, WhatsApp o.J.a, o.J.b).

Wegen dieser Weitergabe personenbezogener Daten der Kontaktpersonen muss eine Person, die WhatsApp auf dem Handy installiert hat, juristisch betrachtet alle Personen, deren Daten sie in ihrem Adressbuch gespeichert hat, um Erlaubnis bitten, diese Daten an WhatsApp weiterzuleiten.

Das sog. WhatsApp-Urteil des Amtsgerichts Bad Hersfeld weist Erziehungsberechtigte auf ihre diesbezüglichen Fürsorgepflichten hin (Buchner 2017), eine weitere Klage der Verbraucherzentrale ist am Landgericht Berlin unter Aktenzeichen 52 O 22/17 anhängig.

Weitere Risiken für Übertretungen der DSGVO sind: (a) Information an die Messenger-Firmen z.B. WhatsApp-Eigentümer (Facebook-Konzern) über ein Kommunikationsverhältnis zwischen Fachkraft und Adressat*in samt Geräte- und Verbindungsdaten wie z.B. Telefonnummern, IP-Adresse und eindeutige Gerätekennungen (Metadatenübermittlung!), obwohl ein Kontaktverhältnis in der Sozialen Arbeit nicht veröffentlicht werden soll; (b) Speicherung von Kommunikation auf weiteren datenverarbeitenden Servern (verschickte Anhänge über WhatsApp werden oft automatisch im internen Speicher des Handys gespeichert und bei Synchronisierungen beispielsweise mit Google- oder Samsung-Servern unverschlüsselt an weitere Firmen weiter gereicht); (c) Zugriff weiterer installierter Apps auf den internen Speicher des Handys, sodass Inhalte und Fotos der Kommunikation unverschlüsselt an andere Apps übermittelt werden.

Zum Schutz vor einer rechtlich bedenklichen Nutzung von Kommunikationstools reagieren Einrichtungen mit Verboten, die jedoch in Ermangelung adäquater Alternativen für die Kommunikationsbedarfe nur schwer konsequent durchzuhalten sind.

3.2. Exklusionsrisiken für vulnerbale Personengruppen: Privatsphäreverletzungen und Predictive Analytics

Die automatisierte Verarbeitung von aggregierten Daten ermöglicht es heute schon, über Personen statistische Diagnosen zu erstellen (z.B. Depressionsdiagnostizierung anhand geposteter Instagram-Fotos nach Reece/Danforth 2017) und Vorhersagen zu zukünftigem Verhalten zu machen, z.B. über die Leistungsfähigkeit oder Krankheitsanfälligkeit. Erweiterte Analysemethoden in der Zukunft lassen Potenziale (und Risiken) für Diagnosemöglichkeiten erwarten, die heute noch kaum vorstellbar sind. Insbesondere für benachteiligte Menschen aus vulnerablen Gruppen sind diese Diagnosen und Vorhersagen potenziell benachteiligend, wenn ihnen z.B. geringe Leistungsfähigkeit, hohes Armuts-, Kriminalisierungs-, Illegalisierungs- oder Krankheitsrisiko diagnostiziert oder vorhergesagt und derartige Daten zukünftig zum Verkauf stehen könnten und beispielsweise bei Krankenkassen, Bewerbungsverfahren, Versicherungsleistungen zu weiteren Benachteiligungen und geringeren Teilhabechancen führen. Aktuelle Fälle schildert bereits Algorithmwatch (Kayser-Bril 2019).

Daten von Adressat*innen der Sozialen Arbeit sind aus diesen Gründen besonders schützenswert. Hinzu kommt, dass die Phänomene der digitalen Ungleichheit häufig auf diese Menschen zutreffen. So sind es häufig bildungsbenachteiligte Menschen, die im Zuge digitaler Ungleichheit (Bos et al. 2014, Iske/Kutscher 2020) geringe Versiertheit im effizienten Umgang mit digitalen Tools haben.

Insofern kann ein gegenwartsbezogenes Bestreben, Menschen in pädagogische oder sozialarbeiterische Kontexte zu inkludieren, ohne dabei die Risiken digitaler Kommunikationstools zu berücksichtigen, dazu führen, dass diese zukünftig aufgrund der bei diesen Maßnahmen erhobenen Daten von Exklusionen bedroht sind.

3.3. Medienpädagogische Kompetenz und mangelnde Informationen

Erforderlich sind Medienkompetenz sowie darüber hinaus medien*pädagogische* Kompetenzen bei den Fachkräften. Medienpädagogische Kompetenz befähigt sie u.a. zur Identifizierung von geeigneten Medien im Handlungsfeld entsprechend aller zu berücksichtigenden Vorgaben (Siller et al. 2020). Die Vermittlung von medienpädagogischer Kompetenz in der Ausbildung in pädagogischen Studiengängen oder solchen für Soziale Arbeit ist jedoch gering (Imort/Niesyto 2014, Schulz/ Sozialforschungsstelle TU Dortmund 2019).

Allerdings ist die Perspektive auf die Entwicklung einer medienpädagogischen Kompetenz bei Fachkräften nicht ausreichend: Es bedarf geeigneter Informationen! Selbst bei vorhandener Kompetenz ist die einer Entscheidung für den Einsatz einer Software vorausgehende Recherche so aufwändig, dass sie einzelnen Fachkräften schlecht zugemutet werden kann. Die Recherchelage bezüglich der zu erfüllenden Vorgaben sowie der Erfüllung dieser Vorgaben durch diverse Software ist oft undurchsichtig, die Informationslage dünn. Die Recherchen bei der von uns durchgeführten Messenger-Studie zeigten großen Klärungsbedarf dazu, was Sozialarbeiter*innen nutzen dürfen. Diese Unklarheit und die mangelnde Unterstützung beim Auswahlprozess können dazu führen, dass keine oder eine ungeeignete Nutzungsentscheidung getroffen wird. Die Komplexität des Medienauswahlprozesses zeigte sich beispielhaft im Frühjahr 2020 im Rahmen der Betretungsverbote wegen der COVID-19-Präventionsmaßnahmen, als selbst Hochschulen Unklarheiten bei der Auswahl DSGVO-konformer Kommunikationssoftware wg. teils unzureichender Angaben von Softwareherstellern erlebten. Jugendeinrichtungen empfahlen und nutzten während des Corona-Lockdowns populäre aber nicht hinreichend da-

tenschützende Apps; genutzt wurden beispielsweise explizit: Instagram, Facebook, WhatsApp, Discord, Skype (BAG OKJE 2020). Ob diese datenschutzrechtlich bedenklichen Entscheidungen aufgrund mangelnder Kenntnisse von Alternativen oder nach einer ethischen Güterabwägung der Anpassung an Nutzungsgewohnheiten der Adressat*innen erfolgten, bleibt zu erforschen.

Empfehlenswerte einführende Informationsportale zu sicherer Software allgemein existieren, z.B. Do not track; Digitalcourage; Klicksafe (vgl. Literaturverzeichnis). Außerdem existieren für die private Nutzung aussagekräftige Kriterientabellen für die Sicherheit von Messengern (Cryptoparty 2019, Gekeler 2020, Incobs 2015, Neß o.J., Schönenberger 2016, Verbraucherzentrale 2018, Wikipedia 2020, Williams o.J.), mit hilfreichen detaillierten Angaben zu datenschutzrechtlich relevanten Features der Softwares. In keiner Tabelle sind aber alle benötigten Informationen (zu allen Messengern, zu Mindestalter, zu Betriebssystemen, zu Barrierefreiheit) zusammengefasst, die für den institutionellen Einsatz nötig sind. Daher sind mühsame zusätzliche Recherchen, Transfers, Verknüpfungen durchzuführen und die unterschiedliche Aktualität der Tabellen zu beachten.

4. Besondere Anforderungen in der Sozialen Arbeit an Messenger-Kommunikation

Im Folgenden werden als Grundlage für die Entwicklung geeigneter Kriterien die besonderen Anforderungen in Einrichtungen der Sozialen Arbeit skizziert.

4.1. Datenschutz und personenbezogene Daten

Aus ihrem Auftrag ergibt sich, dass die Einrichtungen der Sozialen Arbeit vorrangig mit vulnerablen Gruppen und daher mit besonders sensiblen Daten umgehen. Bei der Erfüllung ihrer Aufgaben müssen die Einrichtungen daher beispielsweise die Vorgaben der Verbände und Träger beachten und sehen sich neben der DSGVO je nach Träger auch den kirchlichen Datenschutzgesetzen, sowie der Ethik des Berufsverbands (DBSH 2014) verpflichtet. Die DSGVO muss anwendbar sein (z.B. Firmensitz und Server in der EU). Keine weiteren zusätzlichen Einwilligungen sollten erforderlich sein, die über Art. 5 hinausgehen. Datenerhebung, -speicherung

und -verarbeitung sollten dem Gebot der Datensparsamkeit bei der Speicherung und Verarbeitung folgen.

4.2. Behördenkommunikation

Sozialarbeitseinrichtungen müssen oft mit Behörden in rechtlichen Angelegenheiten ihrer Adressat*innen kommunizieren. Insofern kann Kommunikation mit den Adressat*innen rechtlich relevant werden. So stellen sich Fragen nach Möglichkeiten der Veraktung dieser Kommunikation: ob ein Messenger eine zum Drucken nutzbare Desktop-Version anbietet, so dass Ausdrucke der Kommunikation leicht möglich sind, muss geprüft werden[1]. Ebenso ist zu klären, welche personenbezogenen Daten durch welche Stellen für welche Zwecke verarbeitet werden sollen und dürfen und ob mit dem Messenger empfangene oder versandte personenbezogene Informationen Aktenrelevanz haben könnten. Öffentliche Stellen sind verpflichtet, die Rechtmäßigkeit ihres (Verwaltungs-)Handelns gegenüber der oder dem Betroffenen und ggf. gegenüber den Kontrollorganen wie z. B. Gerichten jederzeit nachzuweisen. Die Nachweispflicht im Zusammenhang mit personenbezogener Datenverarbeitung ergibt sich aus den Vorgaben der DSGVO. Ferner stellen sich Fragen zur Speicherung und Löschung der in einem Messenger gespeicherten Daten, die auf privaten Geräten gespeichert sind. Teilweise werden durch individuelle Handy-Einstellungen in Unkenntnis ursprünglich Ende-zu-Ende verschlüsselte Messenger-Daten wie Fotos auf dem Endgerät unverschlüsselt in der Galerie oder bei gewissen Synchronisierungseinstellungen auch auf Google- oder Samsung-Servern unverschlüsselt synchronisiert.

Bei Kommunikation im Kontext Sozialarbeit ist zu beachten, ob Geheimhaltungspflichten anzuwenden sind und ob Sozialdaten übermittelt werden, denn hier bestehen besondere Schweigepflichten, die auch digital eingehalten werden müssen.

4.3. Bildungsauftrag

Viele Einrichtungen der Sozialen Arbeit haben einen kompensatorischen Bildungsauftrag z.B. im Zuge gesellschaftlicher und digitaler Transformati-

1 Manche Messenger benötigen kein Smartphone und laufen als Desktop-Software oder funktionieren zusätzlich (Threema Web) als Desktop-Lösung.

on zur Befähigung einer individuellen Lebensführung. Dieser Bildungsauftrag sollte unter den Bedingungen von Digitalisierung in der Gesellschaft und Veränderung der Lebenswelten und Kommunikationsformen auch die Vermittlung von Medienkompetenz – und hier auch von Kenntnissen über sichere Kommunikation und Datenschutz – umfassen, um Selbstbestimmung und Teilhabe auch bei digitaler Kommunikation zu fördern. Wo sonst können insb. benachteiligte Jugendliche dies lernen?

4.4. Inklusion

Inklusion ist für Einrichtungen der Sozialen Arbeit Pflicht und Auftrag, hier ist insbesondere die UN-Behindertenrechtskonvention mit den Art. 9, 21, 22, 24 zu nennen, die sich auf Zugänglichkeit zu allen Informationen und IKT-Technologien sowie zu Bildung beziehen, um gleichberechtigte Teilhabe an allen gesellschaftlichen Prozessen zu ermöglichen. Insofern muss Inklusion auch bei Medienangeboten mitgedacht werden (Zorn et al. 2019): Bei der Auswahl einer Messenger-Software soll die Zugänglichkeit und Barrierefreiheit beachtet werden, um niemanden strukturell von Kommunikationsprozessen zu exkludieren.

4.5. Freiwilligkeit der Nutzung

Die Nutzung muss insbesondere in der Sozialen Arbeit freiwillig und ohne Androhung von Nachteilen erfolgen können. Die Notwendigkeit zum Einholen von Einwilligungen ist aus juristischer Sicht zu vermeiden (Nebel 2021).

5. Kriterien für die Auswahl von Software in der Sozialen Arbeit

Trotz des hohen und steigenden Bedarfs für datensichere Kommunikation und Software im Bildungs- und Sozialarbeitskontext ist ein Manko an umfassender Information für praktikable Kommunikationssoftware zu konstatieren.

Auf der Grundlage der o.g. besonderen Anforderungen an solche Einrichtungen gilt es demnach, Kriterien zu entwickeln, die an Messenger-Software angelegt werden müssen, wenn die Software im Kontext von Ein-

richtungen der Sozialen Arbeit verwendet werden soll. Bislang aggregierte Informationen über Messenger müssten ergänzt werden.

Solche Kriterien müssen für die Messenger-Auswahl in drei Kategorien entwickelt werden: a) Datenschutz und Privatsphäre; b) Barrierefreiheit und Inklusion; c) Praktikabilität des Einsatzes in Institutionen.

5.1. Datenschutz und Privatsphäre

Grundlagen für die Entwicklung von Kriterien sind: (1) DSGVO und kirchliche Datenschutzverordnungen, (2) DBSH-Ethik, (3) gesetzliche Vorgaben zu Geheimhaltung, strafrechtlicher Schweigepflicht und Sozialdatenschutz in der Sozialen Arbeit.

*DSGVO***:** Die Erfüllung der Richtlinien der DSGVO ist Grundvoraussetzung für die Auswahl einer Software in allen institutionellen Kontexten (während Privatpersonen hier auch ohne Interesse an ihren Rechten entscheiden dürfen).

Zu prüfende Kriterien dafür sind u.a.: Ist die DSGVO anwendbar und ist sie erfüllt? Wo stehen die Server, die Daten speichern? Wird Kommunikation standardmäßig verschlüsselt? Sind keine besonderen Einwilligungen erforderlich? Welche personenbezogenen Daten werden erhoben, gespeichert, verarbeitet, weitergegeben? Können Kontaktdaten geschützt werden? Werden Daten von Kindern adäquat geschützt?

DBSH-Ethik: Nach der Ethik des Berufsverbands Soziale Arbeit sind Prüfkriterien zu entwickeln, mit denen die Einhaltung ethischer Haltungen wie z.B. Vertraulichkeit, Transparenz oder Nicht-Wissen (DBSH 2014: 26f) bei der Nutzung eines Messengers überprüft werden können. Bei Nicht-Wissen ist z.B. relevant, ob durch das technische Tool bekannt werden kann, worüber und mit wem Klient*innen noch kommunizieren außer mit der Fachkraft und ob die Fachkraft in Unkenntnis solcher Aktivitäten und Inhalte bleiben kann (Negativbeispiel dafür ist die Sicht auf private Statusmeldungen der Adressat*innen bei WhatsApp, die in der Regel zur privaten Kommunikation gehören, aber dennoch von der Fachkraft eingesehen werden könnten). Wissen aus privaten Aktivitäten kann zu ethischen Konflikten führen. Es ist zu klären, ob der Zugang zu Handy und zur Messenger-Kommunikation geregelt und sperrbar ist. Die Nutzung des Messengers durch die Adressat*innen soll freiwillig erfolgen und beendet werden können.

Gesetzliche Vorgaben zu Geheimhaltung, strafrechtlicher Schweigepflicht und Sozialdatenschutz: Prüfkriterien sind, ob Geheimhaltungen in der Kommunikation anfallen werden und ob Sozialdaten übermittelt werden. Gesetzli-

che Vorgaben zu Geheimhaltung, strafrechtlicher Schweigepflicht und Sozialdatenschutz in der Sozialen Arbeit müssen eingehalten werden, dies ist insb. in § 203 Abs. 3, 4 Satz 2 Nr. 1 StGB sowie in Bestimmungen des § 80 SGB X geregelt. Es besteht eine Verschwiegenheitspflicht für die im professionellen Kontext geteilten Inhalte. Werden diese Inhalte über eine Messenger-App geteilt, ist zu prüfen, ob der Messenger-Anbieter die Verschwiegenheit übernimmt. Davon kann praktisch gesehen bei einer Ende-zu-Ende verschlüsselten App ausgegangen werden, rechtlich kann dies aber eine Grauzone sein. Es bleibt zu klären, wie dies bei kostenfreien Messengern mit Ende-zu-Ende-Verschlüsselung juristisch zu bewerten ist, wenn technisch bedingt nur die beiden Kommunikationspartner Zugriff auf die Kommunikation haben und vom Anbieter keine Metadaten gespeichert werden.

Rechtssicherheit kann durch Abschluss eines Auftragsverarbeitungsvertrags erzielt werden. Ein Kriterium ist also, ob eine solche mit dem Anbieter des Produkts abschließbar ist. Diese Möglichkeit kann praktisch kaum für alle freien Apps bestehen, sondern kann erst durch Vertragsabschluss für eine Bezahlvariante eines Messengers möglich werden, beispielsweise also für Work-/Pro-Versionen von Messengern, also organisationsinternen Lösungen. Meist sind aber Consumer- und Work-Versionen einer Messenger-App kompatibel und gegebenenfalls die Notwendigkeit des Kaufs einer Pro-Version nur für die professionellen Fachkräfte erforderlich (ausführlich zu allen rechtlichen Prüfungen vgl. Pehl/Knödler 2020). Die Möglichkeiten eines Auftragsverarbeitungsvertrags sind für eine Einrichtung rechtssicher und somit vorteilhaft, da sie eine gegebenenfalls notwendige Einwilligung der Nutzenden überflüssig machen, die immer Schwierigkeiten (Rücknahme der Einwilligung, Einwilligungen bei Machgefällen) mit sich bringen kann.

5.2. Barrierearmut

Grundlage für die hohe Relevanz der Berücksichtigung von Barrierearmut und somit der Entwicklung von Prüfkriterien sind Normen, inklusive Usability und zielgruppenspezifische Bedarfe.

Normen

Die UN-Behindertenrechtskonvention (UN-BRK) verpflichtet dazu, alle Menschen ungeachtet einer Behinderung an Kommunikation, Information und den dazugehörigen Technologien, an Bildung und gesellschaftlichen Prozessen teilhaben zu lassen (Art. 9, 21, 22, 24). Verbunden mit Vorgaben aus Sozialgesetzbüchern zu Teilhabe (SGB VIII) und Inklusion (SGB XII) oder der BITV 2.0 (Barrierefreie-Informationstechnik-Verordnung) ergibt sich daraus, dass digitale Technologien und ihr Einsatz in Informations-, Kommunikations- und Bildungsprozessen der Sozialen Arbeit barrierefrei und inklusiv sein sollen. Vorgaben dazu macht die BITV 2.0, die aber bislang wenig spezifisch für Apps ist. Der Einsatz einer Messenger-App, die z.B. nicht von blinden Jugendlichen eines Jugendzentrums zur gemeinsamen Kommunikation genutzt werden kann, müsste demnach als unzulässig, jedenfalls aber als exkludierend interpretiert werden.

Die Berücksichtigung von Barrierearmut ist in der Praxis anspruchsvoll, insbesondere da die Nutzenden sehr unterschiedliche Betriebssysteme und -versionen verwenden. Für die Entwicklung von Kriterien für Apps kann die Nutzung einer an der TU Dortmund entwickelten Leitlinie für Apps hilfreich sein: Beispiele für Kriterien zur Barrierearmut sind Bedienbarkeit, Erlernbarkeit, Oberflächenästhetik, Inhalt, Zweckmäßigkeit (Reh@pp-Quality 2016). Hier zeigen sich Analogien zu „klassischen" Kriterien der Software-Ergonomie nach der DIN EN ISO 9241 Normenreihe: Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Erwartungskonformität, Lernförderlichkeit, Steuerbarkeit, Fehlertoleranz, Individualisierbarkeit.

Kriterien für die Bedienbarkeit sind beispielsweise die Varianz von Einstellungsmöglichkeiten: Können Einstellungen zu Barrierearmut individuell je nach vorliegendem Bedarf getätigt oder assistive Technologien mit der Software kombiniert werden? Reagiert die jeweilige App auf die in den meisten Smartphones mittlerweile integrierten Bedienungshilfen? Lässt sich z.B. die Ansicht der Texte in der App mithilfe der Bedienungshilfen größer machen? Interaction Designer müssten hier mitgestalten und mit User-Testern, die auf jeweilige Barrierefreiheit angewiesen sind, diverse Nutzungskontexte durchspielen.

Zu erwägen ist, ob aufgrund der sehr diversen Anforderungen durch unterschiedliche Sinneseinschränkungen (Hören, Sehen), Mobilitätseinschränkungen, verwendeter Assistenztechnologien etc. eine personenunabhängige Vorauswahl getroffen werden sollte, oder ob je nach Nutzenden eine App ausgewählt werden kann.

Inklusive Usability

Unabhängig von regulierter Barrierefreiheit sollte die Bedienung möglichst allen Menschen leichtfallen können. Kriterien für eine intuitive Bedienung sind beispielsweise, ob es bei Installation bereits zu Schwierigkeiten kommen kann, ob viele Bedienungsfehler auftreten, ob Bedienungsweisen intuitiv oder umständlich gestaltet sind. Dabei kann auch ein gegebenenfalls notwendiger Bezahlvorgang eine Rolle spielen.

Zielgruppenspezifische Bedarfe

Bei der Nutzung in Einrichtungen der Sozialen Arbeit sollte mit einem weiten Inklusionsbegriff (nicht nur auf Behinderungen bezogen!) bei Überlegungen zu Barrierearmut gearbeitet werden: Es zeigen sich zunehmend heterogene Voraussetzungen und Bedarfe bei Kindern und Jugendlichen, die sich nicht nur entlang von Behinderungen festmachen lassen, sondern auch in Bezug auf ihre Hintergründe wie finanzielle Ausstattung, Bildungsstand, familiäre Erlaubnisse und Verbote, Sprachkenntnisse, Medienkompetenzen. Bezüglich der Sprachkenntnisse ist für manche Adressat*innen der Sozialen Arbeit die Möglichkeit von Sprachnachrichten relevant, um im Fall von z.B. Lese-/Schreib-/Sprachschwierigkeiten ohne Stigmatisierung die Teilhabe zu erleichtern. Konkrete Kriterien leiten sich daraus ab: Benötigte Bedienungs- und Nutzungskenntnisse, Altersbeschränkungen (Alter der Adressat*innen ist oftmals unter 16 Jahren: dann sind ohne besondere Einwilligung nur Apps ohne Erhebung personenbezogener Daten wie Email-Adresse oder Telefonnummer erlaubt), Nutzbarkeit bei verschiedenen Geräteausstattungen und diversen Betriebssysteme, auch alte Versionen, Eignung der App bei Lese- und Rechtschreibschwäche oder sogar Analphabetismus.

5.3. Praktikabilität im Kontext der Einrichtung

Damit eine datensichere, barrierearme App auch zum beabsichtigten Nutzungserfolg in einer Organisation führen kann, sind weitere Kriterien für ihre Praktikabilität zu entwickeln. Eine App, die unpraktisch im Handling ist oder die wegen fehlender benötigter Features nicht den gewünschten Nutzungserfolg erzielen kann, wird sich in der Praxis bei den Nutzenden nicht durchsetzen können. Insbesondere diese dritte Kategorie enthält As-

pekte, die für die spezifische Arbeit in der Sozialen Arbeit relevant sein können und für die bislang kaum Kriterien in bekannten Prüftabellen entwickelt und abgebildet sind.

(1) Nutzer*inneneigenschaften/Alter:
Welche Personengruppen sollen die App nutzen, wie ist ihr Alter? Die Altersfreigabe für Softwares, die personenbezogene Daten erheben, ist in Deutschland 16 Jahre. Personenbezogene Daten sind beispielsweise eine anzugebende Telefonnummer oder E-Mail-Adresse für die Anmeldung, wie es bei WhatsApp der Fall ist. In den App-Stores wird beispielsweise für WhatsApp die Altersfreigabe „USK 0 Jahre" angegeben. Diese Angabe der Unabhängigen Selbstkontrolle (USK) der Medienwirtschaft ist hier aber nicht rechtlich bindend, sondern die Allgemeinen Geschäftsbedingungen (AGB) und die DSGVO.

(2) Finanzierung:
Ist eine App kostenfrei oder kostenpflichtig nutzbar? Eine als sicher einzustufende und viele Merkmale erfüllende App wie Threema ist kostenpflichtig. Sie kostet einmalig ca. 3,99 Euro. Jedoch stellt ein Bezahlvorgang an sich für viele Adressat*innen eine große Hürde dar, wenn sie keine Kreditkarte besitzen, keine Daten von sich preisgeben möchten oder nur geringe Nutzungsfertigkeiten besitzen. Eine Organisation kann aber Lizenzen kaufen und an spätere Nutzende verschenken.

(3) Zuständigkeiten, Einverständniserklärungen:
Müssen die Nutzenden bei den Herstellern oder bei der Organisation ihr Einverständnis erklären? Was passiert, wenn sie dies nicht tun möchten?

(4) Features:
Interne und externe Nutzung: Ermöglicht der Messenger die Kommunikation nur innerhalb des Einrichtungskontexts oder ermöglicht er auch externe Kommunikation, z.B. für private Kontakte?
Kommunikationsangebote: Werden beliebte Features wie Anrufe, Videochat, Gruppenchat (verschlüsselt?) angeboten? Gibt es Einschränkungen beim Versand von Videos, Bildern, Sprachnachrichten? Dies kann die Akzeptanz und Alltagsintegration mit beeinflussen.

(5) Alltagspraxis und -integration:
Motivation: Wie werden Nutzende motiviert, die Software in ihre Alltagspraxis zu integrieren, insbesondere, wenn sie möglicherweise bereits eine Alltagspraxis für die Kommunikation mit einem anderen Messenger (häufig WhatsApp) entwickelt haben und es explizite oder

gewohnheitsbedingte Widerstände gegen die Nutzung einer zusätzlichen App gibt?
Weiterbildungsbedarfe, Abläufe: Ergeben sich Weiterbildungsbedarfe für Fachkräfte oder Adressat*innen? Ist die Software selbsterklärend? Verändert die Nutzung Arbeitsabläufe oder Kommunikations-, Dokumentations- oder Organisationsstrategien?

(6) Technischer Aufwand der Betreuung und Nutzung:
Aufwand: Hier ist zu prüfen, ob die Nutzung für die späteren Nutzenden technisch unaufwändig erscheint (Finanzierung) und ob der Betrieb technische Wartung und somit Personal erfordert.
Gerätebesitz, Dienstgeräte: Welche Geräte können verwendet werden? Können/müssen private Geräte verwendet werden oder können/sollten Geräte durch die Einrichtung bereitgestellt werden?
Integration in bestehende Softwarenutzungen: Ist die Messenger-App kompatibel mit anderen softwaregestützten Kommunikations- und Organisationsabläufen und ohne dauerhaften Mehraufwand integrierbar?

(7) Betriebssysteme:
Kompatibilität mit allen gängigen Betriebssystemen, auch älteren Versionen ist notwendig, wenn vulnerable Adressat*innen ihre eigenen Geräte nutzen sollen, die nicht reguliert werden können.

(8) Desktopversion:
Ist für die Nutzung ein Smartphone notwendig oder lässt sich mit der Software auch über Computer kommunizieren? Adressat*innen können Computer nutzen, die in der Einrichtung zur Verfügung gestellt werden können. Handybesitz ist keine Voraussetzung. Für Fachkräfte erleichtert die Desktopnutzung die Dokumentation durch die Druckmöglichkeit.

6. Fazit und Ausblick

Mängel bei der Anwendbarkeit von DSGVO führen u.E. dazu, dass viele populäre Messenger nicht für den Einsatz in Schule oder Sozialer Arbeit geeignet sind[2]. Ein großes Problem beim Datenschutz ist der mangelnde

2 Z.B. WhatsApp, Telegram, Viber, Skype, Signal, Discord. Discord verarbeitet Daten aus der Kommunikation. https://praxistipps.chip.de/discord-im-home-office-nutzen-das-muessen-sie-wissen_119629
Discord speichert auf Servern, die nicht der GDPR unterliegen. Wenn man sich nicht auf Datenschutz berufen kann und dies nicht einfordern oder einklagen

Schutz vor Weitergabe und Verarbeitung der Adresseinträge auf einem Gerät sowie der Umgang der Anbieter mit Metadaten. Bei den DSGVO-konformen Messengern können die weiteren Kriterien Barrierearmut und Praktikabilität geprüft werden, um Lösungen entsprechend der spezifischen Anforderungen der Sozialen Arbeit zu finden. Eine Übersicht der Messenger wurde im Rahmen des BMBF-geförderten Projekts IDIT erstellt und ist weiter bearbeitbar (Zorn et al. 2020).

Interessante Alternativen existieren unter jenen Messengern, die Institutionen kaufen und bei denen sie individuelle Verträge samt Auftragsverarbeitungsvereinbarungen und individuellen Klauseln zum Datenschutz mit den Herstellern abschließen[3]. Neben kostenpflichtigen Angeboten bestehen auch Möglichkeiten der Nutzung von Open Source Produkten und dem eigenen Serverbetrieb zur Verarbeitung der Daten, z.B. Mattermost, XMPP-Softwares[4]. Erwägenswert ist eine gemeinsame Entwicklung von nicht-proprietären Messengern (z.B. Open Source wie Mattermost oder XMPP-Messenger) auf Bundes- und Landesebene, evt. mit Kultusministerien (die für Schulen ähnliche Interessen verfolgen) und mit den großen Trägern und Bundesverbänden und mit Stabstellen der Landesdatenschutzbeauftragten. Ein sicherer, DSGVO-konformer Serverbetrieb sollte aufgrund der Datenschutzkomplexität sinnvoll und dürfte in Anbetracht des großen Sektors der Sozialen Arbeit gegenüber eingekauften Lösungen preisgünstig sein. Vermutlich ist ohnehin die technische Weiterentwicklung privatsphäreschützender Softwares für den in Frage stehenden Kontext notwendig, damit sie zunehmend auch die in den Punkten Barrierearmut und Praktikabilität beschriebenen Kriterien erfüllen können, dies ließe sich mit freier Open Source Software verwirklichen.

Ein Nicht-Handeln der Einrichtungen verhindert zudem auch nicht grundsätzlich die Nutzung von Messengern. Vielmehr ist zu befürchten, dass dadurch die informelle Nutzung und Verbreitung jener Messenger

---

kann, fallen nach unserer Einschätzung viele Anwendungseinsätze schlicht aus, bei denen Datenschutz vorgeschrieben ist – formale Bildung, Soziale Arbeit. Discord erhebt, verarbeitet personenbezogene Daten und teilt sie mit Geschäftspartnern und verknüpft sie – spricht: gibt sie weiter https://discord.com/privacy . Im Juni 2020 hat Facebook einen Rechtsstreit verloren – es wurde Facebook untersagt, die Daten seiner diversen Firmen (Whatsapp, Facebook, Instagram) miteinander zu verknüpfen. https://netzpolitik.org/2020/bundesgerichtshof-facebook-beutet-nutzer-kartellrechtlich-relevant-aus/.

3 Z.B. Threema Work, Wire Pro, OwnChat, Chiffry, school.cloud, SchoolFox u.v.a..m.

4 https://www.freie-messenger.de/sys_xmpp/server/ ; Anleitung: https://www.freie-messenger.de/dateien/conversations/Anleitung_Conversations.PDF.

zunimmt, die Daten nicht schützen, Barrierefreiheit nicht respektieren und dass dies zunehmend zu Exklusionen führt. Insofern sind Einrichtungen der Sozialen Arbeit hier auch entsprechend ihres Bildungsauftrags aufgefordert, Lösungen zu finden und anzubieten.

Darüber hinaus könnte mit einem solchen Angebot eines XMPP-Servers durch das Aufzeigen der Machbarkeit datenschützender Messenger-Kommunikation die theoretische und praktische Medienkompetenz eines breiten Bevölkerungsanteils fördern. Nutzende könnten zudem damit auch extern kommunizieren.

Die Weiterentwicklung von Kriterien für organisationale Umsetzbarkeit oder Praktizierbarkeit (und von Softwareentscheidungen) sollten daher in pädagogischen Kontexten nicht ausschließlich mit technischen, sondern auch mit pädagogischen Fachkräften erfolgen und geprüft werden, bevor organisationale Entscheidungen getroffen werden, weil Technikentscheidungen pädagogisches Handeln beeinflussen (Kutscher et al. 2020). Weil die zu treffenden Entscheidungen umfassend geprüft werden müssen und Auswirkungen auf Arbeitsabläufe haben, ist eine Entscheidung durch obere Hierarchieebenen anzuraten, damit die Frage nach effizienten Kommunikationstools nicht einzelnen Fachkräften überlassen wird.

Literatur

BAG OKJE [Bundesarbeitsgemeinschaft Offene Kinder- und Jugendeinrichtungen e.V.] (2020): *Information: Offene Kinder- und Jugendarbeit in Corona-Zeiten, BAG OKJE, Bundesarbeitsgemeinschaft Offene Kinder- und Jugendeinrichtungen e.V. (BAG OKJE)*. https://www.offene-jugendarbeit.net/index.php/okja-in-corona-zeiten/okja-in-coronazeiten [Abfrage am: 09.09.2020].

Bos, Wilfried / Eickelmann, Birgit / Gerick, Julia / Goldhammer, Frank / Schaumburg, Heike / Schippert, Knut / Senkbeil, Martin / Schulz-Zander, Renate / Wendt, Heike (Hg.) (2014): *ICILS 2013. Computer- und informationsbezogene Kompetenzen von Schülerinnen und Schülern in der 8. Jahrgangsstufe im internationalen Vergleich*. Münster: Waxmann.

Buchner, Benedikt (2017): *DuD Recht AG Bad Hersfeld: Elterliche Pflichten bei WhatsApp-Nutzung der Kinder*. In: Datenschutz und Datensicherheit DuD, (9), S. 584-592.

Cryptoparty (2019): *cryptopartykbn:messenger.* https://www.cryptoparty.in/cryptopartykbn/messenger [Abfrage am: 13.06.2020].

DBSH [Deutscher Berufsverband für Soziale Arbeit e.V.] (2014): *Berufsethik DBSH*. In: Forum Sozial, (4), S. 3–43.

Gekeler, M. (2020). *Warum nicht … Übersicht über Messenger-Systeme.* https://www.freie-messenger.de/warum/warumnicht/ [Abfrage am: 15.01.2021]

Imort, Peter / Niesyto, Horst (Hg.) (2014): *Grundbildung Medien in pädagogischen Studiengängen*. München: kopaed.

Incobs (2015): *Barrierefreiheit von Messenger-Apps*. https://www.incobs.de/artikel/items/barrierefreiheit-von-messenger-apps.html [Abfrage am: 26.06.2020].

Iske, Stefan / Kutscher, Nadia (2020): *Digitale Ungleichheiten im Kontext Sozialer Arbeit*. In: Kutscher, Nadia / Ley, Thomas / Seelmeyer, Udo / Siller, Friederike / Tillmann, Angela / Zorn, Isabel (Hg.). Handbuch Soziale Arbeit und Digitalisierung. Weinheim [u.a.]: Beltz Juventa, S. 116–128.

Kayser-Bril, Nicolas (2019:. *Personal Scoring in the EU: Not quite Black Mirror yet, at least if you're rich* –. Köln, Tagung Superscoring. https://www.superscoring.de/wp/wp-content/uploads/2019/08/Kayser-Bril_SuperScoring-Essay_2207.pdf.

Kutscher, Nadia / Ley, Thomas / Seelmeyer, Udo / Siller, Friederike / Tillmann, Angela / Zorn, Isabel (Hg.) (2020): *Handbuch Soziale Arbeit und Digitalisierung*. Weinheim [u.a.]: Beltz Juventa.

MEKOcloud (2018): *Dokumentation des Fachtags: WhatsApp in der Jugendarbeit?* https://www.mekocloud.de/2018/01/whatsapp-in-der-jugendarbeit/ [Abfrage am: 07.09.2020].

mpfs [Medienpädagogischer Forschungsverbund Südwest] (2020): *JIM-Studie 2019. Jugend, Information, Medien. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger.*

Nebel, Maxi (2021): *Digitales Lernen – Datenschutzrechtliche Rechtsgrundlagen von Lernplattformen für Kinder und Erwachsene*, in diesem Band.

Neß, Karsten (o.J.): *Privacy Handbuch*. Messenger. https://www.privacy-handbuch.de/handbuch_74.htm [Abfrage am: 26.06.2020].

Pehl, Manuel / Knödler, Christoph (2020): *Messenger-Dienste in der Sozialen Arbeit - datenschutzkonform nutzen*. Regensburg: Walhalla u. Praetoria Verlag.

Reece, Andrew G. / Danforth, Christopher M. (2017): I*nstagram photos reveal predictive markers of depression*. In: EPJ Data Science, 6, S. 15. DOI: 10.1140/epjds/s13688-017-0110-z.

Reh@pp-Quality (2016): *App-QKK. App-Qualitätskriterienkatalog.* Dortmund. http://www.rehatechnologie.fk13.tu-dortmund.de/rehapp/Medienpool/Dateien-zum-Download/App-QKK.pdf [Abfrage am: 13.06.2020].

Schönenberger, Erik (2016): *WhatsApp, E-Mail, SMS & Co. auf Sicherheit und Nachhaltigkeit bewertet*. https://www.digitale-gesellschaft.ch/2016/11/07/whatsapp-e-mail-sms-co-auf-sicherheit-und-nachhaltigkeit-bewertet-produktvergleich/ [Abfrage am: 26.06.2020].

Schulz, Ann Christin (2019): *Ausbildung zur digitalen Teilhabe? Eine Analyse der Lehrangebote zu Medienkompetenz in sozialen und pädagogischen Studienfächern an deutschen Hochschulen*. Beiträge aus der Forschung Band 202. Dortmund: Sozialforschungsstelle TU Dortmund.

Siller, Friederike / Tillmann, Angela / Zorn, Isabel (2020): *Medienkompetenz und medienpädagogische Kompetenz in der Sozialen Arbeit*. In: Kutscher, Nadia / Ley, Thomas / Seelmeyer, Udo / Siller, Friederike / Tillmann, Angela / Zorn, Isabel (Hg.). Handbuch Soziale Arbeit und Digitalisierung. Weinheim [u.a.]: Beltz Juventa, S. 314-332.

Verbraucherzentrale (2018): *Datenschutzregeln bei Messengern mit Verschlüsselung im Überblick.* https://www.verbraucherzentrale.de/sites/default/files/migration_files/media243857A.pdf.

WhatsApp (o.J.a): *How we work with the Facebook Companies.* https://faq.whatsapp.com/general/security-and-privacy/how-we-work-with-the-facebook-companies?eea=1 [Abfrage am: 07.09.2020].

WhatsApp (o.J.b): *Privacy Policy.* https://www.whatsapp.com/legal/?l=de#privacy-polic.

Wikipedia (2020): *Liste von mobilen Instant-Messengern* – Wikipedia. https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern [Abfrage am: 13.06.2020].

Williams, Marc (o.J.): *Secure Messaging Apps Comparison | Privacy Matters*. https://www.securemessagingapps.com/ [Abfrage am: 13.06.2020].

Zorn, Isabel / Murmann, Jule / Harrach-Lasfaghi, Asmae (2020): *Rechercheergebnisse DSGVO-konforme Messenger-Apps für Bildungseinrichtungen.* Köln: TH Köln.

Zorn, Isabel / Schluchter, Jan R. / Bosse, Ingo (2019): *Theoretische Grundlagen inklusiver Medienbildung.* In: Bosse, Ingo / Schluchter, Jan-René / Zorn, Isabel (Hg.). Handbuch Inklusion und Medienbildung. Weinheim [u.a.]: Beltz Juventa, S. 16–34.

Das Recht von Kindern und Jugendlichen auf Privatheit in digitalen Umgebungen: Handlungsempfehlungen des Forum Privatheit

Ingrid Stapf, Judith Meinert, Jessica Heesen, Nicole Krämer, Regina Ammicht Quinn, Felix Bieker, Michael Friedewald, Christian Geminn, Nicholas Martin, Maxi Nebel und Carsten Ochs

1. Einleitung

Die Jahrestagung des Forum Privatheit im November 2019 hat das Thema „Aufwachsen in überwachten Umgebungen" in Deutschland erstmals interdisziplinär aufgegriffen. Dabei zeigte sich eine Diskrepanz zwischen dem gesellschaftlichen und politischen Orientierungs- und Steuerungsbedarf einerseits und der wissenschaftlichen Forschung an der Schnittstelle von Theorie und Praxis andererseits.

Mit dem Aufkommen überwachungsbasierter Medientechnologien von Smart Toys, Babysitter-Kameras im Teddybär bis hin zu Sprachassistenzsystemen wie Alexa, individualisierte Lernsoftware, Tracking-Apps oder Videoüberwachung in der Kita, stellt sich die Frage, was Privatheit von Kindern heute ausmacht: Bedarf es bei Kindern anderer Konzepte als bei Erwachsenen? Wie können sie den Schutz ihrer Daten im Altersverlauf steuern? Und wer trägt die Verantwortung?

Dieser Beitrag analysiert das Recht von Kindern auf Privatheit mit Blick auf digitale Umwelten, bezieht sich auf aktuelle empirische Daten und leitet daraus Forderungen an Politik und Medienregulierung, den Bildungsbereich sowie mediale Anbieter ab. Ziel des Beitrags ist es außerdem, einen gesellschaftlich-politischen Diskurs anzustoßen, Anforderungen für die Praxis zu formulieren sowie weiteren Forschungsbedarf aufzuzeigen. *Unsere Kernthese ist: Die Rechte von Kindern in digitalen Handlungswelten müssen stärker durchgesetzt und berücksichtigt werden. Dazu gehören explizit das Recht auf informationelle Selbstbestimmung, der Datenschutz, die freie Entfaltung der Persönlichkeit und ein geschützter Privatbereich.*

Demokratische Freiheits- und Gleichheitsrechte sollen Kindern eine offene Zukunft ermöglichen. Da Kindheit eine besonders verletzliche Entwicklungsphase ist und sich wichtige Fähigkeiten erst noch ausbilden, bedürfen Kinder eines umfassenden Schutzes durch Fürsorgetragende und

den Staat. Sie sollen gleichzeitig aber auch als handelnde Subjekte ihre Selbstbestimmung erproben können. Hierzu werden Befähigungsmaßnahmen wesentlich, welche die Mündigkeit von Kindern in der Demokratie (und im „digitalen Gemeinwesen") zum Ziel haben. Das Thema Privatheit von Kindern wird hierbei von einem Spannungsfeld geprägt: auf der einen Seite steht der fürsorgliche Schutz im Interesse des Kindes, auf der anderen jedoch paternalistische Überwachungspraktiken, die kindliche Selbstbestimmungsansprüche in Frage stellen.

Aus der fortschreitenden „Mediatisierung von Kindheit" resultiert Handlungsbedarf mit Blick auf damit verbundene Risiken. Denn Kinder und Jugendliche bis 18 Jahren machen rund ein Drittel der weltweiten Internetznutzer*innen aus. Dieser Beitrag füllt eine Lücke, da das Zusammenspiel von Privatheit und Kinderrechten bislang noch kaum wissenschaftlich differenziert untersucht wurde.

Kinderrechte wurden – ergänzend zu den allgemeinen Menschenrechten – 1989 völkerrechtlich in der UN-Kinderrechtskonvention (UN-KRK) verankert und gelten seit 1992 als einfaches Recht in Deutschland. Die Rechte von Kindern werden zudem in Artikel 24 der EU-Grundrechtecharta verbrieft. Die UN-KRK betont die Rolle von Kindern als subjektive Handlungsträger mit eigenen Rechten und etabliert in 54 Artikeln das beste Interesse von Kindern als leitendes Prinzip im Zusammenspiel von Schutz-, Förderungs- und Beteiligungsrechten. In Artikel 16 UN-KRK ist das Recht auf „Schutz der Privatsphäre und Ehre" formuliert.

Aktuelle Entwicklungen zur Aufnahme von Kinderrechten ins Grundgesetz bedürfen einer rechtzeitigen Auseinandersetzung mit der Bedeutung der spezifischen Problemlagen rund um ein Recht auf Privatheit von Kindern in digitalen Kontexten. Diese Auseinandersetzung möchte das Paper anstoßen.

2. *Privatheit im Kontext der Digitalisierung*

Kindheit ist nicht nur eine biologische Lebensphase, sondern wird auch gesellschaftlich-kulturell konstruiert. In Deutschland herrscht ein stark schutzbetonter Blick auf Kinder vor, der im Recht zur Redensart vom Kind als der „Heiligen Kuh des BGB" geführt hat. Dahinter steht die Idee, dass Kinder geschützte Räume brauchen, um ihre Persönlichkeit und auch ihre Selbstbestimmung erproben und erlernen zu können. Das Kinderzimmer galt lange als Raum des Rückzugs, in dem sich der im Kindheitsverlauf wachsende Wunsch von Kindern nach eigenen Bereichen, Erfahrungen und Beziehungen entwickelt.

Im Zuge der zunehmenden Digitalisierung haben Kinder und Jugendliche heute jedoch im Internet nicht nur einen umfassenden Zugriff auf mediale Inhalte, globale Plattformen und eine Vielfalt an Informationen, sondern geben dabei gleichzeitig viele ihrer persönlichen Daten preis. Das geschieht einerseits im Rahmen einer aktiven, selbst-initiierten Weitergabe, beispielsweise, wenn ein Social-Media-Profil mit persönlichen Daten gefüllt wird und in Interaktionen mit anderen Nutzer*innen Fotos, Daten und Informationen ausgetauscht werden. Diese aktive Preisgabe von Daten und persönlichen Informationen birgt die Gefahr, dass Gleichaltrige diese zum Beispiel für Cybermobbing-Angriffe nutzen (horizontale Privatheitsbedrohung). Andererseits stellt auch die passive Sammlung, Analyse und der Verkauf von Daten durch Unternehmen eine Gefahr dar, der sich Kinder und Jugendliche nicht vollständig bewusst sind (vertikale Privatheitsbedrohung).

2.1 Der Begriff Privatheit in digitalen Kontexten

Privatheit ist eine wesentliche Bedingung für Demokratie und Rechtsstaatlichkeit. Als Sammelbegriff ist Privatheit jedoch keine rein rechtliche Kategorie, denn der Begriff der Privatheit umfasst zahlreiche Teilaspekte. Dazu gehören auch Rechte wie das auf informationelle Selbstbestimmung, das Recht auf Schutz des Privaten und das Recht auf Datenschutz sowie das Persönlichkeitsrecht, das Post- und Fernmeldegeheimnis, die Unverletzlichkeit der Wohnung und das sogenannte IT-Grundrecht, das den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme zum Ziel hat.

Für den digitalen Bereich ist das Recht auf informationelle Selbstbestimmung zentral. Es unterscheidet sich jedoch strukturell stark vom paternalistischen Ansatz der Bestimmung eines schützenswerten Bereiches von außen („Privatsphäre“), indem die Selbstbestimmung des Einzelnen zum Maßstab erhoben wird (Geminn/Roßnagel 2015, Nebel 2015). Bei einem schutzbetonten Ansatz legen Dritte, nämlich staatliche Behörden, die Justiz und auch die Rechtswissenschaften fest, was „privat“ und damit geschützt ist. Diese fremdbestimmte Vorstellung wird dem Einzelnen gleichsam auferlegt, meist durch staatliche Akteure, die die Grenzen der Privatheit festlegen. Demgegenüber steht hinter der informationellen Selbstbestimmung ein freiheitsorientierter Ansatz, welcher die autonome Entscheidungsfähigkeit der Akteure in den Vordergrund stellt. Erwachsenen traut man diese Selbstbestimmung grundsätzlich voll zu, wohingegen bei Kindern die Grenzen individuell ausgelotet werden müssen.

2.2 Aktuelle Herausforderungen mit Blick auf Medien und Kinder

Die aktuellen Nutzungszahlen belegen nicht nur, dass bereits sehr junge Kinder über ein eigenes Smartphone verfügen und Zugang zum Internet haben, sondern auch, dass sie täglich Apps wie WhatsApp und YouTube sowie digitale Spiele nutzen (Hajok 2019, Rathgeb/Behrens 2018b). Weiterhin steigt die Nutzung mit dem Alter stark an, sodass unter den 12- bis 19-Jährigen bereits 97% ein eigenes Smartphone besitzen und 89% täglich online sind (Engels 2018, Rathgeb/Behrens 2018a).

Die beliebtesten Apps von Kindern und Jugendlichen sind momentan US-amerikanische Apps wie WhatsApp, Instagram, YouTube und Snapchat (Rathgeb/Behrens 2018a). Auch die chinesische App TikTok gewinnt zunehmend an Popularität (Monllos 2019). Laut einer Studie lehnen 67% der befragten Jugendlichen die Speicherung ihrer persönlichen Daten durch diese Apps ab (Engels 2018). Das hat jedoch überwiegend keinen Einfluss auf ihr Nutzungsverhalten – ein bekanntes Phänomen, das unter dem Namen „privacy paradox" (Barnes 2006, Norberg/Horne/Horne 2007) erforscht und diskutiert wird (Baruh/Secinti/Cemalcilar 2017). Livingstone, Stoilova und Nandagiri (2019) beobachten, dass Kinder im Internet einerseits freiwillig persönliche Informationen online teilen und dabei Risiken für ihre Sicherheit und ihre Privatheit in Kauf nehmen, obwohl sie andererseits ihre Privatheit schützen wollen. Der Widerspruch besteht darin, dass soziale Teilhabe nur bei Aufgabe herkömmlicher Privatheitsvorstellungen zu haben ist. Studien mit Erwachsenen betonen darüber hinaus, dass ein Gefühl von Machtlosigkeit und Resignation sowie mangelnde Wahlmöglichkeiten ein Grund für das privacy paradox sind (Matzner et al. 2016, Stoycheff 2016). Andere wiederum betonen, dass es in Bezug auf das scheinbar widersprüchliche Nutzungsverhalten um eine Abwägung verschiedener Wertvorstellungen geht, die eher mit Konzepten zur Risikoanalyse statt mit Paradoxien treffend beschrieben werden können. Dienlin und Trepte (2015) wiesen nach, dass es sich tatsächlich nur scheinbar um eine Paradoxie handelt, da eine genauere Analyse auf Basis der psychologischen „Theory of Planned Behavior" sehr wohl eine Deckungsgleichheit von Einstellungen und privatheitsbezogenem Verhalten zeigt, wenn man nach spezifischen Einstellungen und Intentionen fragt. Gerade bei jüngeren Kindern kommt das Problem hinzu, wieviel Wissen und Erfahrungen schon vorausgesetzt werden können, um derartige Abwägungen überhaupt treffen zu können.

Die gängigen Anwendungen wie Facebook, Instagram, TikTok und Snapchat haben eine Altersbeschränkung von 13 Jahren, bei WhatsApp beispielsweise wurde diese im Zuge des Geltungsbeginns der EU-Daten-

schutzgrundverordnung im Mai 2018 auf 16 Jahre angehoben. Allerdings handelt es sich dabei um eine Formalität ohne praktische Bedeutung, da sich die Apps ohne Altersüberprüfung herunterladen und nutzen lassen. Dies wirft insgesamt die Frage auf, ob eine solche Form der Selbstkontrolle ein valides Instrument ist, um Kinder und Jugendliche von der Nutzung datenschutzkritischer Anwendungen abzuhalten. Vor dem Hintergrund des hohen Belohnungswertes dieser Anwendungen erscheint es zudem weder erwartbar noch vertretbar, Heranwachsende mit dem Ziel einer Gefahrenreduktion von einer Nutzung abhalten zu wollen.

Mit der zunehmenden Mediatisierung von Kindheit (Kutscher 2012, Tillmann/Hugger 2014) nutzen Kinder also schon sehr früh eigene digitale Geräte. Damit erhalten sie Zugang zu Inhalten, Netzwerken und Plattforme. Diese ermöglichen nicht nur neuartig und umfassend die Wahrnehmung ihrer Rechte auf Information, medialen Zugang und Teilhabe, sondern beeinträchtigen gleichzeitig auch ihre Persönlichkeitsrechte. Da digital vernetzte Medien mobil und abseits elterlicher Kontrolle genutzt werden und der rechtliche Jugendmedienschutz durch den digitalen Wandel grundlegend herausgefordert ist, sind schon jüngere Kinder erhöhten Risiken – von Cybergrooming oder Cybermobbing, extremistischen Inhalte bis hin zu Pornografie oder extremen Gewaltdarstellungen – ausgesetzt, die sich auf ihre Entwicklung auswirken können (Brüggen et al. 2019).

Der Prozess intensiver Datensammlung, Beobachtung und Überwachung wird als Bestandteil der „Datafizierung" bezeichnet (Lupton/Williamson 2017). Auch Daten von Kindern werden hier zu „Gütern", die mit Vermarktungsinteressen verbunden sind. Viele Angebote einer mediatisierten Kindheit beschneiden die Rechte von Kindern auf eine offene Zukunft und das Erproben von Selbstbestimmung in einem für Kinder oft nicht einschätzbaren öffentlichen und kommerziell durchdrungenen Raum (Fahlquist 2015, Friedewald et al. 2020). Hierzu gehören Spiele-Apps mit Captology-Technik, einer Computertechnologie, welche das Beurteilungs- und Entscheidungsverhalten von Menschen zu beeinflussen versucht (z.B. Pokémon-Go, Candy-Crush Saga), personalisierte Werbung mit Aufforderungscharakter bis hin zu rein kommerziellen Zwecken (z.B. Instagram, TikTok), im kindlichen Spiel eingesetzte Smart Toys, die systematisch Daten auswerten und speichern (z.B. der Roboter i-Que, Cloud Pets, Hello Barbie), die Verwendung von Klassenchats, welche Daten systematisch sammeln und auswerten (z.B. WhatsApp), das Preisgeben des Standorts von Kindern in sozialen Medien (z.B. TikTok) oder die von Fürsorgetragenden gewollte Überwachung im familiären oder schulischen Umfeld durch Tracking-Apps (z.B. Little Nanny GPS Tracker) sowie individualisierte und Profile erstellende Lernsoftware (z.B. Quizlet). Um be-

stimmte Apps und Dienste kostenlos nutzen zu können, sind Kinder und Jugendliche häufig bereit, persönliche Daten preiszugeben – ohne dabei die volle Tragweite der vermeintlichen harmlosen Informationsweitergabe überschauen zu können (Engels 2018).

In digitalen Kontexten werden die Entscheidungen und Praktiken von Kindern und Jugendlichen durch die soziale Umgebung, allem voran durch das vorgelebte Verhalten ihrer Eltern und der Peer-Group beeinflusst (vgl. Kapitel 4: Einfluss- und Schutzfaktoren bei der Internetnutzung durch Kinder und Jugendliche). Ob Kinder persönliche Daten teilen oder zurückhalten, verhandeln sie in einem Kontext vernetzter Kommunikation und damit verknüpfter Praktiken. Livingstone et al. (2019) differenzieren hierbei zwischen einer relationalen Privatheit (das Daten-Ich, das über das eigene Sozialverhalten online geschaffen wird), einer institutionellen Privatheit (durch das Sammeln und Auswerten persönlicher Daten durch staatliche Stellen, Bildungs- oder Gesundheitseinrichtungen) und einer kommerziellen Privatheit (persönliche Daten, die von Unternehmen wirtschaftlich verwendet werden). Hinsichtlich letzterer fühlen sich Kinder am ohnmächtigsten.

3. Kinder als besonders vulnerable Gruppe

Kinder und Jugendliche werden immer wieder als besonders vulnerabel bezeichnet, weil sich Kinder und Jugendliche hinsichtlich ihrer kognitiven Voraussetzungen von Erwachsenen unterscheiden. Sie haben weniger Vorwissen und Erfahrungen zu bestimmten gesellschaftlichen Prozessen und pflegen eine für ihre Altersgruppe spezifische Herangehensweise an Medien.

3.1 Kognitive Voraussetzungen

Kinder unter elf Jahren sind typischerweise in ihrer Entwicklung noch nicht weit genug vorangeschritten, um Konzepte wie „Privatheit" vollumfänglich zu begreifen; auch sind Kinder weniger in der Lage, das monetäre Potenzial von Daten und deren Nutzung für Profiling einzuschätzen (Livingstone et al. 2019). Erst beginnend im Jugendalter wird die Fähigkeit zum abstrakteren Denken ausgebildet, was auch das Erkennen von (intransparenten) Zusammenhängen umfasst, dem sogenannten formal-operationalen Denken (vgl. Piaget 1972). Insbesondere bei Kindern in der Pu-

bertät wurde nachgewiesen, dass verschiedene neuronale Verschaltungen temporär eingeschränkter funktionieren im Vergleich zur Kindheit oder dem Erwachsenenalter (Powell 2006). Dies kann das Verständnis – zum Beispiel der potenziellen Konsequenzen der Online-Selbstoffenbarung – zusätzlich erschweren.

Vor dem Hintergrund ihrer noch nicht vollständig abgeschlossenen Entwicklung sind Kinder und Jugendliche somit auch besonders anfällig für Online-Dienste, die auf kurzfristige Erfolgserlebnisse, Belohnungsanreize und soziale Honorierung setzen und im Gegenzug Datenprofile der Nutzenden sammeln – sowohl aus aktiv veröffentlichten Daten als auch durch die passive und intransparente Speicherung von Klicks, Nutzungsverhalten, Webseitenbesuchen und Likes. Prominente Beispiele dafür sind – neben WhatsApp, Instagram, Facebook, Reddit und Snapchat, die über soziale Belohnungssysteme arbeiten – digitale Spiele-Apps wie Pokémon-Go oder die Video- und Musik-App TikTok. Die Mechanismen dieser Applikationen basieren auf einer Bindung der Nutzenden durch wiederholte Push-Nachrichten, Belohnungen für erreichte Ziele, soziale Vernetzung mit anderen Nutzenden oder Spieler*innen und der Möglichkeit einer Bühne zur Selbstdarstellung. Diese sind für die jüngeren Nutzer*innen schwer zu durchschauen oder gar – sofern die Nutzungsdynamik einmal begonnen hat – zu durchbrechen.

3.2 Fehlender Erfahrungshintergrund

Zahlreiche Publikationen weisen darauf hin, dass Kinder und Jugendliche sich der Gefahren für Privatheit und Datenschutz und den potenziellen Folgen eher wenig bewusst sind (Heeg et al. 2018, Naplavova et al. 2014). Werden Kinder konkreter befragt, welche Gefahren sie im Internet vermuten, lässt sich ein deutlicher Effekt der Medienberichterstattung der vergangenen Jahre feststellen: Befürchtungen von Kindern und Jugendlichen in Bezug auf eine Verletzung ihrer Online-Privatheit beziehen sich vor allem auf andere Nutzer*innen und somit vertikale Privatheitsbedrohungen. Eine häufig artikulierte Gefahr ist zum Beispiel Online-Mobbing bzw. Cyberbullying, welches durch die Beschränkung der Sichtbarkeit einzelner Fotos oder Beiträge oder des gesamten Profils zu verhindern versucht wird (Borgstedt et al. 2014). Ebenso sind die Gefahren des Cybergroomings eher präsent, die in einer qualitativen Studie in neun europäischen Ländern als Gefahr der Kontaktanbahnung durch Fremde detailliert beschrieben wird (Mascheroni/Jorge/Farrugia 2014). Über die Hintergründe und potenziel-

len Gefahren der Datenökonomie besteht dagegen kaum Bewusstsein (Livingstone et al. 2019).

3.3 Altersgruppenspezifische Herangehensweise an Medien

Kinder und Jugendliche gelten oft als „Digital Natives", da sie von frühester Kindheit an mit den Möglichkeiten des Internets aufgewachsen sind. Auch wenn sie mit digitalen Medien aufwachsen, heißt dies aber nicht, dass eine kritische Reflexion der Effekte und Nebenfolgen der Nutzung von Informations- und Medientechniken nicht gelernt werden müsste (vgl. kritisch zum Begriff „Digital Natives" Genner/Süss 2017, Prinzing 2019). Neben positiven Konsequenzen wie einer hohen technischen Affinität führt die quasi selbstverständliche Nutzung auch dazu, dass bestimmte Persuasionsmechanismen (wie die Aufforderung Inhalte zu abonnieren) und die Existenz personalisierter Werbung nicht (mehr) hinterfragt und als selbstverständliche Bestandteile der Funktionsweise des modernen Internets empfunden werden (Wang et al. 2019).

Auf der anderen Seite nähern sich Kinder den neuen digitalen Angeboten vor allem aus ihrer Erfahrungswelt heraus: Hier kann besonders die Tatsache problematisch sein, dass sich Kinder neue Spiele durch einfaches Ausprobieren aneignen – ohne vorab Informationen oder Warnungen zu beachten. Gefahren können dadurch erst retrospektiv überhaupt erkannt werden (Borgstedt et al. 2014). Generell zeigt sich dabei, dass der Grad der Sichtbarkeit der eigenen Aktivitäten in Online-Applikationen nur schwer eingeschätzt werden kann. Das geht sogar so weit, dass die „Öffentlichkeit" einer Interaktion an den jeweils beteiligten Akteur*innen festgemacht wird, wodurch ein WhatsApp-Chat zwischen zwei Personen als vollkommen privat empfunden wird (Borgstedt et al. 2014), obwohl trotz der Ende-zu-Ende-Verschlüsselung private Inhalte von teilnehmenden Nutzer*innen weitergeteilt werden können, Metadaten transparent sind oder Sicherheitsrisiken durch die Speicherung von Fotos bestehen. Ein Verständnis der Datenverarbeitung wird dadurch erschwert, dass sich die Nutzungsbedingungen primär an Eltern als Sorgeberechtigte wenden. Diese sind aber nicht notwendigerweise an der Nutzung beteiligt und zusätzlich sind die Bedingungen oftmals sowohl für Kinder als auch deren Eltern kaum verständlich. Folglich kann nicht von einer informierten Entscheidung ausgegangen werden.

Dies ist aus datenschutzrechtlicher Sicht problematisch, da eine ausreichende Informationsgrundlage eine zentrale Voraussetzung einer wirksamen Einwilligung in die Datenverarbeitung nach Artikel 7 Abs. 1 DSGVO

– bei Kindern in Verbindung mit Artikel 8 DSGVO – ist. Nur bei Kenntnis aller entscheidungsrelevanten Informationen können die Nutzer*innen Risiken und Vorteile abschätzen und dann sachgerecht über die Einwilligung entscheiden. In der Praxis zeichnet sich jedoch ein gegenteiliges Bild ab, da Nutzer*innen in den seltensten Fällen über alle nötigen Informationen verfügen, um die Risiken und Nachteile einer Einwilligung in ein angemessenes Verhältnis zu setzen. Häufig überwiegt aufgrund dieser Informationsasymmetrie für die Nutzenden der mit „kostenlosen" Spielen und Apps verbundene Vorteil gegenüber den potenziellen und vom Anbieter nicht transparent dargestellten Risiken der Datenverarbeitung (ausführlich zur Einwilligung vgl. Roßnagel et al. 2020).

Kinder wollen in ihrem medialen Handeln häufig einfach bestimmte Angebote nutzen und pflegen ihre Freundschaften ohne zwischen „analog" und „digital" zu unterscheiden. Damit ist Privatheit von Kindern – noch stärker als bei Erwachsenen – als kontextbezogen und relational zu sehen. Je jünger und unerfahrener sie sind, desto schwieriger ist es folglich für Kinder, ihre Daten und ihre Privatsphäre selbst zu schützen und dies auch im Wissen um mögliche Folgen für sie und andere informiert und selbstbestimmt zu tun.

4. Einfluss- und Schutzfaktoren bei der Internetnutzung durch Kinder und Jugendliche

Der (soziale) Kontext beeinflusst die Art und Weise, wie Kinder und Jugendliche das Internet und Soziale Medien nutzen. Hervorzuheben sind dabei Fürsorgetragende wie die Eltern (oder auch andere Erwachsene wie Lehrer*innen und Erzieher*innen) sowie gleichaltrige Bezugspersonen. Ein weiterer bestimmender Kontext sind die so genannten Affordances, d.h. der Angebotscharakter der Anwendungen selbst. Im Folgenden wird für jeden Bereich diskutiert, inwieweit die einzelnen Aspekte den Privatheitsschutz verstärken oder auch hemmen können.

4.1 Fürsorgetragende als Einflussfaktoren

Ein starker Treiber für die generelle Internetnutzung, aber auch die Verwendung bestimmter Apps ist die Orientierung an Anderen. Im jüngeren Alter richten sich Kinder besonders an ihren Eltern und älteren Geschwistern aus. Das bedeutet, dass nicht nur das eigene Internetverhalten am Mo-

dell der Eltern und deren Umgang mit Apps wie zum Beispiel Instagram und der unbeschränkten Veröffentlichung von Familienfotos (Sharenting) ausgerichtet wird, sondern auch, dass darüber hinaus eine Habitualisierung der Anwesenheit und Nutzung von Technologien stattfindet, die notwendigerweise die Weitergabe von Daten erfordern. Das kann sich auf die Nutzung von Smart-Home-Steuerungs-Apps, den Einsatz von virtuellen Assistenten wie Alexa oder Siri sowie die Verwendung von Online-Diensten zur Strukturierung des Familienalltags (z.B. die Aufräum-App Highscore House) beziehen.

Besonders bei konkreten Verhaltensweisen haben Eltern einen hohen Einfluss: Im Sinne des Modelllernens übernehmen Kinder und Jugendliche das Verhalten der Eltern, die oft über ein umfangreicheres Wissen über Zusammenhänge und potenzielle Gefahren verfügen, das sie an die Kinder und Jugendliche vermitteln können. Allerdings ist auch von Seiten der Eltern eine Überforderung zu beobachten und eine adäquate Risikoeinschätzung der Nutzung von Apps oder Spielen und der damit verbundenen Datenverarbeitung wird durch die hohe Komplexität oftmals erschwert (Kutscher/Bouillon 2018, Manske/Knobloch 2017). Hinzu kommt, dass auch Unterschiede im Wissensstand und Umgang der Eltern mit dem Schutz persönlicher Daten (z.B. basierend auf sozioökonomischen Unterschieden) bedacht werden müssen, die sich dann nachfolgend auch nachteilig auf die Kompetenz der Kinder und Jugendlichen auswirken und zur Verschärfung sozialer Ungleichheiten im Rahmen einer Wissenskluft beitragen können (Paus-Hasebrink et al. 2018). Generell zeigt sich, dass zum Beispiel Altersnutzungsbeschränkungen von Online-Apps und digitalen Spielen lediglich als „pädagogische Empfehlung" verstanden werden (vgl. Hajok 2019). Das betrifft weiterführend auch die Ausdifferenzierung von Kommunikationsräumen als privat oder öffentlich; so wird beispielsweise WhatsApp im Vergleich zu Facebook häufig als stärker geschützter privater Raum wahrgenommen, was aufgrund der Ende-zu-Ende-Verschlüsselung auch berechtigt ist. Dennoch werden auch hier Metadaten und Kontaktinformationen gesammelt und ausgewertet.

Insgesamt sind Kinder und Jugendliche heute mit omnipräsenten und vielschichtigen Medienangeboten und Technologien konfrontiert. Um diese chancenorientiert und selbstbestimmt nutzen zu können, müssen sie mit Kompetenzen und Wissen (z.B. über komplexe Trackingverfahren von Webseiten und Apps) sowie kritischer Urteilskraft zu einem reflektierten Umgang mit einhergehenden Risiken für Datensicherheit und den Schutz von persönlichen Informationen befähigt werden. Da dieses Wissen auch über Erfahrungen vertieft wird, sind Maßnahmen der Befähigung möglichst auf konkrete Kontexte ihrer Lebenswelt zu beziehen und sollten

über Selbstbefähigung das Ziel selbstbestimmten Handelns verfolgen (Stapf 2019, 2021). Ein solches Wissen sollte – auf Basis der beschriebenen Überforderung vieler Eltern – vorrangig in den Bildungsinstitutionen, also durch Schule und Lehrer*innen, vermittelt und im familiären Kontext vertieft werden. Für diesen Bildungsauftrag sind ausreichende Ressourcen vorzusehen und die Implementierung entsprechender Kompetenzen im Bereich von Lehrerbildung und Fortbildungen sowie eine Anpassung der schulischen Curricula zu ermöglichen.

4.2 Peers als Einflussfaktoren

Weiterhin orientieren sich Kinder und vor allem Jugendliche an Gleichaltrigen. Teil der Gruppe zu sein wird dabei als wichtiger wahrgenommen, als der Schutz der eigenen Daten. Die Vorteile mit anderen online zu kommunizieren (und daraus resultierend eigene Daten zu teilen) werden direkter wahrgenommen, wohingegen Risiken wie z.B. die Vorfilterung von Informationen und Produkten, Cybermobbing oder auch ein Identitätsdiebstahl oftmals erst verspätet wahrgenommen werden (können).

Ein zentrales Motiv jugendlicher Mediennutzung liegt im Folgen von Gruppendynamiken, um Teil der Gemeinschaft als auch der online stattfindenden Interaktionen und Dialoge zu sein und deshalb in der Nutzung bestimmter Apps (über die durch vernetzte Profile auch Verbindungen untereinander bestehen, z.B. Instagram, TikTok), die von Gleichaltrigen genutzt werden. Es ist zum Beispiel gemeinhin üblich, WhatsApp-Gruppen für die Kommunikation im Klassenverband zu nutzen (Rathgeb/Behrens 2018a). Datenschutzkritischen Applikationen stehen Kinder und Jugendliche demnach machtlos gegenüber, da eine Nichtnutzung für sie aufgrund impliziter Kommunikationsnormen im Klassenverband, Freundeskreis oder Sportverein nicht in Frage kommt und mit einer sozialen und kommunikativen Abgeschnittenheit einhergehen würde (Engels 2018).

Da sich Kinder und Jugendliche noch in der Phase der Identitätsbildung befinden, hat sowohl der Einfluss anderer als auch die Relevanz sozialer Interaktionsprozesse eine höhere Wichtigkeit. Gerade die noch nicht abgeschlossene Persönlichkeitsentwicklung, einhergehend mit der Festigung des Selbstkonzepts, die individuell unterschiedlich und nicht an feste Altersschritte geknüpft stattfindet, macht Kinder und Jugendliche sehr beeinflussbar. Hierdurch können sie leicht, auf impulsive Weise und ohne kritische Reflexion von dem Nutzungsverhalten ihrer Peergroups angesteckt werden.

In Kombination mit der alters- und erfahrungsbedingten Unwissenheit der Heranwachsenden (z.B. in Bezug auf mögliche zukünftige Konsequenzen ihrer heutigen Handlungen als auch der Langfristigkeit einiger Nutzungsentscheidungen) ist es wichtig, dass Kinder und Jugendliche in besonderer Weise geschützt werden (Dreyer 2018, 2020). In diesem Kontext kommt den Prinzipen der datenschutzgerechten Gestaltung (Datenschutz by Design) und der Auswahl datenschutzfreundlicher Voreinstellungen (Datenschutz by Default) eine besondere Bedeutung zu (Bieker/Hansen 2017). Datenschutz muss bei Anwendungen, die sich an Kinder und Jugendliche richten, von Entwicklungsbeginn an umgesetzt werden. Zudem müssen Apps in einer Art und Weise vorkonfiguriert sein, dass nicht mehr Daten als die, die zur Erreichung des Zwecks erforderlich sind, verarbeitet werden und nur Grundfunktionen aktiviert sind. Für jede Erweiterung sollte dann eine eigene informierte Einwilligung der Nutzenden oder ihrer gesetzlichen Vertreter*innen erforderlich werden.

4.3 „Affordances" der Anwendungen als Einflussfaktor

Der Angebotscharakter der medialen Anwendungen führt dazu, dass Kinder und Jugendliche geradezu zu einer ungeschützten Nutzung aufgefordert werden. So stellen die Anwendungen die Vorteile und den Belohnungswert im Sinne einer Teilhabe am sozialen Leben und der Verfügbarkeit von Information über gesellschaftlich relevante Themen durch die Art und Weise ihrer Gestaltung klar in den Vordergrund, während potenzielle Risiken der Nutzung in den Hintergrund treten. Dies erhöht die Bereitschaft der Kinder und Jugendlichen, private Informationen zu teilen. So sind Kinder und Jugendliche gerade im Austausch gegen eine kostenlose Nutzung bestimmter Apps und Dienste bereit, persönliche Daten preiszugeben – oftmals ohne die volle Tragweite der vermeintlich harmlosen Informationsweitergabe übersehen zu können (Engels 2018). Dies entspricht dem empirisch gut belegten Ansatz des „privacy calculus" (Culnan/Armstrong 1999), der zeigt, dass ein kurzfristiger Nutzen häufig über langfristige (weniger überblickbare) Folgen gestellt wird. Die entsprechenden Studien beziehen sich allerdings ausschließlich auf Erwachsene und fokussieren dabei stark auf rationale Überlegungen, was für Kritik am Ansatz sorgt. So gilt es bislang als ungeklärt und muss hinterfragt werden, ob und in welcher Weise diese rationalen Überlegungen bei Kindern überhaupt stattfinden. Hinzu kommt, dass die Anwendungen nahelegen, dass sie eigentlich privat sind (etwa ein Austausch mit Freunden auf Instagram).

Um diesen Einflussfaktor zu einem Schutzfaktor machen zu können, müssten die Anwendungen folglich so verändert werden, dass die Gefahren unmittelbar sichtbarer und damit für die Nutzer*innen einschätzbarer werden – was nicht im Sinne von Anbietern sein dürfte, deren Geschäftsmodell auf dem Sammeln und Auswerten von Daten beruht. Bereits nach der DSGVO müssen Anbieter von Anwendungen, die personenbezogene Daten verarbeiten, ohnehin über die Weitergabe von Daten transparent und in einer für die Nutzenden verständlichen Weise etwa auf die Weitergabe von Daten hinweisen. Dies kann durch so genannte Privacy Icons (Holtz/Nocun/Hansen 2011) erreicht werden, die mit Symbolen einen Überblick über die Datenverarbeitung bieten können (Artikel 12 Abs. 7 DSGVO). In jedem Fall müssen die Anbieter im Sinne des Datenschutzes durch datenschutzfreundliche Voreinstellungen, d.h. by default (Artikel 25 Abs. 2 DSGVO), auch sicherstellen, dass Daten der Nutzenden nicht standardmäßig mit Dritten geteilt werden oder gar öffentlich einsehbar sind. Diese Datenschutzanforderungen werden häufig ignoriert, was exemplarisch in der Studie „Deceived by Design" (Kaldestad 2018) herausgearbeitet wurde. Auf der einen Seite müssen daher die Sanktionierungsmöglichkeiten verbessert werden, auf der anderen Seite sollten die Politik und diejenigen Akteure, bei denen Anwendungen zum Einsatz kommen, auch positive Anreize dafür schaffen, dass Hersteller und Anbieter von Beginn an in ihren Systemen die Datenschutz-Grundsätze, und damit auch die Transparenz über die Verarbeitung und die Risiken, einbauen (Bieker/Hansen 2017, Datenethikkommission 2019).

5. Der kinderrechtliche Ansatz mit Blick auf Privatheit

Selbst bestimmen zu können, welche persönlichen Räume andere betreten oder welche Informationen sie einsehen oder verwenden dürfen, ist ein zentrales Menschenrecht. So ist in Artikel 16 der UN-Kinderrechtskonvention (UN-KRK) verbrieft, dass „kein Kind (…) willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden" darf. Die UN-KRK verbrieft Kindern seit 1989 ausdrücklich grundlegende Rechte als Subjekte. Seit dieser völkerrechtliche Vertrag 1992 von Deutschland ratifiziert und umgesetzt wurde, gilt er als einfaches Recht. Die UN-KRK hat damit den Rang eines Bundesgesetzes und ist von allen staatlichen Stellen zu beachten. Kommt es zu einer Kollision mit einer anderen gesetzlichen Vorschrift, kommt der UN-KRK, anders als etwa den Grundrechten des Grundgesetzes, kein Vor-

rang zu. Allerdings können die relevanten Grundrechte – wie das Recht auf informationelle Selbstbestimmung – völkerrechtsfreundlich dahingehend ausgelegt werden, dass das kollidierende nationale Recht im Sinne der UN-KRK ausgelegt wird. Damit kommt völkerrechtlichen Verträgen, obwohl sie „nur" gleichrangig mit anderen Gesetzen gelten und keinen Vorrang genießen, in der Praxis eine erhöhte Bedeutung zu.

Im Zuge der aktuellen Diskussion einer Aufnahme von Kinderrechten ins Grundgesetz ist die Frage nach Privatheit auch in digitalen Kontexten ein zentrales politisches Thema, das Auswirkungen in unterschiedliche Lebensbereiche (von Schule bis Familie und die mediale Regulierung) haben könnte.

Daher erscheint eine kinderrechtliche Perspektive für die informationelle Selbstbestimmung von Kindern und Jugendlichen weiterführend. Entscheidend ist hierbei der Blick auf Heranwachsende als handelnde Subjekte und nicht nur Objekte des Schutzes von Fürsorgetragenden. Dies wird über die vier Grundprinzipien Recht auf Gleichbehandlung bzw. Nicht-Diskriminierung, Vorrang des Kindeswohls, Recht auf Leben und Entwicklung und Achtung vor der Meinung des Kindes angestrebt (Maywald 2012). Den 54 Artikeln der UN-KRK ist das Kindeswohl in Artikel 3 übergeordnet:

> „Bei allen Maßnahmen, die Kinder betreffen, gleichviel ob sie von öffentlichen oder privaten Einrichtungen der sozialen Fürsorge, Gerichten, Verwaltungsbehörden oder Gesetzgebungsorganen getroffen werden, ist das Wohl des Kindes ein Gesichtspunkt, der vorrangig zu berücksichtigen ist."

Rechte gleichen Gehalts enthält auch das Grundgesetz, dort jedoch implizit. Sie aktivieren umfangreiche Schutzpflichten. Explizite Rechte des Kindes enthält auch die EU-Grundrechtecharta (GRCh), zwar nicht in dem Umfang der UN-KRK, dafür aber auf verfassungsrechtlicher Ebene und nicht bloß im Rang eines einfachen Gesetzes. Nach Artikel 24 Abs. 1 Satz 1 GRCh haben Kinder „Anspruch auf den Schutz und die Fürsorge, die für ihr Wohlergehen notwendig sind". Außerdem gelten für Kinder auch alle anderen Grundrechte, wie das Recht auf Privatleben nach Artikel 7 GRCh und auf Datenschutz nach Artikel 8 GRCh.

Aus Sicht der Kinderrechte sind auch Fragen der Privatheit auf das Wohlergehen von Kindern ausgelegt. Kindern soll eine gute und gelingende Kindheit sowie gute Chancen und wichtige Fähigkeiten mit Blick auf ihr Erwachsenenleben eröffnet werden. Hierzu braucht es ein auf die kindlichen Fähigkeiten zugeschnittenes Zusammenspiel von Schutz-, Förderungs- und Beteiligungsrechten (Stapf 2021).

Woran ist dieses Wohl dann auszurichten, wenn man bedenkt, dass Kindheit eine Entwicklungsphase ist? Mit Blick auf Kinder geht es darum, ihr Wohlergehen sowohl in ihrer Gegenwart, aber immer auch mit Blick auf die Entwicklungsdimension ihrer „evolving capacities" (Lansdown 2005), auf ihre überhaupt mögliche Zukunft auszurichten. Joel Feinberg (1980) spricht hierbei von „the child's right to an open future".

Eine offene Zukunft mit Blick auf Privatheit impliziert beispielsweise eine besondere Sorgfalt im Umgang mit kindlichen Daten, ein Recht Heranwachsender auf Vergessenwerden im Netz sowie auf Datensparsamkeit mit Blick auf Datenspuren, die Kinder im Netz hinterlassen. Denn die auf Verhaltensvorhersage und -formung (predictive analytics, nudging usw.) angelegten Geschäftsmodelle der meisten kommerziell erfolgreichen Internet-Plattformen stehen dem Prinzip der offenen Zukunft diametral entgegen (van Dijck/Poell/de Waal 2018, Roßnagel et al. 2020, Zuboff 2019). Dies bedeutet ein erhöhtes Schutzbedürfnis von Kindern im Netz. Und es erfordert, zusammen mit den kindlichen Rechten auf Informations- und Meinungsfreiheit (Artikel 13 UN-KRK), dass Kinder aufgrund für sie verständlicher Informationen eigene Entscheidungen zum Schutz ihrer Privatheit treffen lernen können. Um dies zu ermöglichen sind Bildungsrechte für Kinder verbrieft (Artikel 28/29 UN-KRK). Hierzu erforderlich werden Befähigungsmaßnahmen im Elternhaus sowie systematisch in der Schule und in schulischen Einrichtungen. Dazu wird ein ebenfalls verbriefter Kinder- und Jugendschutz (Artikel 17 UN-KRK) auch in digitalen Kontexten notwendig, der den heutigen Nutzungsbedingungen wie Mobilität und Medienkonvergenz entspricht. All dies erfordert ein Spektrum positiver Angebote für Kinder im Netz. Denn Kinder sind nicht nur immer jünger, wenn sie im Netz unterwegs sind, man kann sie aufgrund der Bedingungen „mediatisierter Welten" (Krotz/Hepp 2012) auch weder praktisch noch sinnvoll von allen digitalen Angeboten ausschließen, bis sie selbst rechtlich einwilligen können.

Ein weiteres Querschnittsrecht von Kindern ist ihr Recht auf Beteiligung (Artikel 12 UN-KRK). Die Aufgabe der Eltern ist es, das Wohl des Kindes als Treuhänder seiner Interessen zu vertreten (vgl. auch Artikel 24 Abs. 3 GRCh). Dem Wohl des Kindes entspricht es auch, seine Persönlichkeit zu entwickeln und zu entfalten. Dieses erfordert eine angemessene Beteiligung bezogen auf den kindlichen Entwicklungsstand: „Die Vertragsstaaten sichern dem Kind, das fähig ist, sich eine eigene Meinung zu bilden, das Recht zu, diese Meinung in allen das Kind berührenden Angelegenheiten frei zu äußern, und berücksichtigen die Meinung des Kindes angemessen und entsprechend seinem Alter und seiner Reife" (vgl. auch Arti-

kel 24 Abs. 1 Satz 2 und 3 GRCh, dazu mit weiteren Nachweisen Roßnagel 2020).

Dieses Recht im Kontext des Digitalen ernst zu nehmen, umfasst Anforderungen an die Medienbildung, die Medienregulierung sowie die universitäre Forschung. Evidenzbasierte Medienforschung über Kinder, aber auch mit Kindern, kann Maßnahmen ermöglichen, welche Entscheidungskompetenzen von Kindern und ihr sicheres Erlernen von Selbstschutzmechanismen fördern. Angesichts aktueller Diskussionen zur Aufnahme von Kinderrechten ins Grundgesetz besteht ein dringender gesellschaftlicher Reflexions- und Diskussionsbedarf.

6. Spannungsfelder: Privatheit von Kindern in digitalen Kontexten

Die Privatheit von Kindern in digitalen Umwelten zu stärken und optimale Bedingungen für ihren Schutz, ihre Befähigung und ihre Teilhabe zu ermöglichen, bedarf einer Berücksichtigung der damit verbundenen Spannungsfelder und Herausforderungen in Abwägung mit möglichen Potenzialen. Über die gesetzlichen Regelungen und die unverzichtbaren Maßnahmen zur Medienbildung hinaus sollten weitere technische Voraussetzungen zum Schutz von Kindern getroffen werden. Hier werden neben neuen theoretischen Konzepten technische Innovationen ebenso notwendig wie interdisziplinäre Forschung als Grundlage von Politikgestaltung. Darüber hinaus sollten dringend auch rechtliche und technische Schutzmaßnahmen vorangetrieben werden, die insbesondere die intransparente Speicherung und Weiterverbreitung von Nutzungsdaten im nationalen wie internationalen Rahmen adressieren.

- *Damit eine Einwilligung wirksam ist, müssen die relevanten Informationen verständlich dargestellt werden, es bedarf daher einer Anpassung an die Fähigkeiten und Interessen von Kindern:* Wie ist beispielsweise damit umzugehen, dass sich in der frühen Kindheit wichtige Fähigkeiten, die Voraussetzung für das Treffen selbstbestimmter Entscheidungen sind, erst entwickeln? Wie müssten Informationen zum Schutz von Daten für Kinder formuliert und visualisiert sein, um sicherzustellen, dass Kinder eine Einwilligung geben können? Wie verhält sich dies im Altersverlauf, z.B. bei noch sehr kleinen Kindern im Vergleich zu Jugendlichen kurz vor dem Erwachsenenalter?
- *Eltern- und Kinderrechte sollten im Zusammenspiel gedacht werden:* Kinderrechte umfassen auch die Pflicht zur Fürsorge durch die Eltern. Sorgeberechtigte haben die erzieherische Vermittlung zentraler Kompeten-

zen zu übernehmen und dabei gleichzeitig das Kind zur Wahrnehmung seiner Freiheitsrechte im digitalen Raum zu befähigen (Croll 2019). Welche Befähigungsmaßnahmen werden dann auch für Eltern, Erziehende und Lehrende notwendig? Inwieweit können Institutionen wie z.B. Schulen, die Fürsorgepflichten wahrnehmen, datenschutzfreundliche Infrastrukturen zur Verfügung stellen? Wie lässt sich die Pflicht zur Fürsorge der Eltern mit der wachsenden Selbstbestimmung von Kindern vereinbaren mit Blick auf den dafür notwendigen Erwerb von Kompetenzen und Fähigkeiten? Inwieweit wirkt sich dies auf schulische Aufgaben und Lehrpläne oder auf die Umsetzung der Anforderungen von Datenschutz insgesamt und speziell von Datenschutz by Design und by Default aus?

- *Schutz-, Beteiligungs- und Befähigungsrechte greifen ineinander, können aber auch zu Spannungsfeldern führen:* Alle Kinderrechte gelten grundsätzlich gleichwertig. In der Regel könnten anzustrebende Schutzmaßnahmen sinnvoll mit Befähigungs-, aber auch mit Beteiligungsmaßnahmen verbunden werden, da dies vor allem für ältere Kinder zu Selbstschutzmaßnahmen führen kann und Kinder dies auch als Wunsch artikulieren (Frense 2020). Verschiedene Kinderrechte stehen aber oft auch im Widerspruch zueinander. So führen erhöhte Beteiligung (Artikel 12 UN-KRK) oder Meinungsäußerung (Artikel 13 UN-KRK) auch zu erhöhten Gefahren mit Blick auf kindliche Schutzrechte, wie bei Hate Speech, Cybermobbing oder der Preisgabe von Daten. Im rechtlichen Konfliktfall kommen hier auf grundrechtlicher Ebene Verfahren der praktischen Konkordanz zum Tragen. Wie können solche Konfliktlinien jedoch schon präventiv im Jugendmedienschutz sinnvoll aufgegriffen werden? Wie lässt sich dies in der Regulierungspraxis ausgestalten und in der Medienbildung zugrunde legen?
- *Spannungsfelder zwischen den Generationen:* Kinder, die aktuell in mediatisierten Lebenswelten aufwachsen, entwickeln in ihrer gelebten Praxis ein anderes und sich wandelndes Verständnis von Privatheit. Wie kann Privatheit als wichtiger Wert für die freiheitliche Demokratie an die jetzt aufwachsende Generation vermittelt werden? Wie ist damit umzugehen, dass Kinder oft kompetenter in der Techniknutzung und nicht selten auch bezogen auf das Technikverständnis sind als ihre Eltern? Wie sind beispielsweise Klassenchats mittels Messenger-Diensten in der Schule zu bewerten, die unter der DSGVO-Altersgrenze von 16 liegen und der Einwilligung der Eltern bedürften? Und was folgt daraus für die Verantwortungsübernahme hinsichtlich der Beurteilung möglicher Konsequenzen der Techniknutzung und des Handelns im digitalen Umfeld?

- *Herausforderungen im Kontext der Kommerzialisierung von Kindheit:* Wie lassen sich Forderungen an positive Angebote stellen und Anreizsysteme auf einem zunehmend kommerziell durchdrungenen globalen Markt etablieren? Die Nichtnutzung digitalisierter Technologien ist keine wirkliche Alternative, vielmehr sollten Ansätze zur Befähigung von Kindern, Jugendlichen und den für sie verantwortlichen Personen dazu führen, dass informierte Entscheidungen zur Wahrung der informationellen Selbstbestimmung getroffen werden können. Um eine Überforderung zu vermeiden und Schutzansprüche nicht zu individualisieren (Karaboga et al. 2014), ist es gleichzeitig ebenso wichtig, Kindern ein sicheres digitales Kommunikationsumfeld zu bieten. In diesem sollten Einschränkungen – bis hin zum Verbot – der kommerziellen Verwertung der Daten von Kindern und restriktive Löschungsvorgaben Standard sein. Und wie könnte eine auf der Analyse von Nutzungsdaten von Kindern basierende Produktentwicklung so reguliert werden, dass der Schutz vor wirtschaftlicher Ausbeutung (Artikel 32 der UN-KRK) gewährleistet wird, solange gezielte auf die kindlichen Bedürfnisse ausgerichtete Kauf- und Nutzungsanreize bestehen?

7. Fazit und Empfehlungen

Die folgenden Empfehlungen verstehen sich als ein erster Impuls, um die politische und gesellschaftliche Diskussion zum Thema Privatheit und Kinder voranzutreiben:

1. Die Privatheit von Kindern ist auch im Digitalen ein verbrieftes Kinderrecht

Selbst bestimmen zu dürfen, welche Räume andere betreten oder welche Informationen sie einsehen oder verwenden dürfen, ist ein Menschenrecht. So ist auch in Artikel 16 der UN-KRK verbrieft, dass „kein Kind (…) willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden“ darf. Die UN-Kinderrechtskonvention als völkerrechtlicher Vertrag garantiert Kindern seit 1989 grundlegende Rechte als Subjekte. Seit sie 1992 von Deutschland ratifiziert und umgesetzt wurde, muss sie auch hier bei der Auslegung nationalen Rechts Berücksichtigung finden. Den durch das Grundgesetz, die EU-Grundrechtecharta und die Europäische Menschen-

rechtskonvention verbrieften Rechten von Kindern muss zu stärkerer Durchsetzung und praktischer Relevanz im Bereich der Nutzung digitaler Technik verholfen werden. Auch im Zuge der aktuellen Diskussion über eine Aufnahme von Kinderrechten ins Grundgesetz ist dies ein zentrales politisches Thema. Dem Grundgesetz fehlt in seiner derzeitigen Fassung die explizite Aussage, dass der Schutz der in seinen Katalog von Grundrechten aufgenommenen Rechte bei Kindern andere Dimensionen haben kann, als dies bei Erwachsenen der Fall ist, wenngleich dies allgemein akzeptiert ist. Dem stehen aktuelle Durchsetzungsdefizite bezogen auf grundrechtlich geforderten Schutz im Rahmen der Digitalisierung gegenüber, die zwar allgemein auch für Erwachsene gelten, für Kinder aufgrund erhöhter Vulnerabilität allerdings stärker wirksam werden könnten.

2. *Mit der Sicherung kindlicher Privatheit ist das Recht des Kindes auf eine offene Zukunft verbunden*

Aus Sicht der Kinderrechte sind Fragen der informationellen Selbstbestimmung und Privatheit auf das Wohlergehen von Kindern ausgelegt. Es geht darum, Kindern eine gute und gelingende Kindheit und gute Chancen und wichtige Fähigkeiten mit Blick auf ihr Erwachsenenleben zu eröffnen. Darunter fällt es auch, Kindern ein Recht auf eine offene Zukunft zu gewährleisten. Anbieter sollten verpflichten werden, neu zu schaffende rechtliche und technische Standards einzuhalten. Dazu könnten Vorschriften gehören, dass Kinder grundsätzlich von personalisierter Werbung und Tracking ausgenommen werden müssen; oder ein Verbot von Profilbildung bei Kindern. Ein weiterer Vorschlag ist die Auflage, in sensiblen Kontexten gewonnene Daten über Kinder regelmäßig zu löschen, sofern dem nicht Kindeswohlinteressen entgegenstehen. Damit verbunden wären verschärfte Anforderungen an die Datenminimierung und ein deutlich über Artikel 17 DSGVO hinausgehendes, echtes Recht Heranwachsender auf Vergessenwerden im Netz, so auch z.B. alle im Rahmen einer Bildungs-App gewonnenen Daten, sobald das Kind die Schule verlässt, kombiniert mit einem Weitergabeverbot während der Nutzungsdauer. Entgegenstehende Kindeswohlinteressen, die für eine andauernde Speicherung auch sensibler Daten von Kindern sprechen, können etwa am Erhalt von Untersuchungsergebnissen bestehen, die Missbrauch dokumentieren.

Die Berücksichtigung der besonderen Schutzinteressen im Umgang mit kindlichen Daten impliziert außerdem, den grundsätzlichen Ausschluss der Einwilligung durch Kinder in die Verarbeitung besonderer Kategorien personenbezogener Daten. Ausnahmen sind nur in solchen Fällen denk-

bar, in denen es um höchstpersönliche Sachverhalte, etwa die Intim- und Geheimsphäre des Kindes, geht, die auch gegenüber den Sorgeberechtigten geschützt ist. Dies gilt etwa im Rahmen der Beratung in einer Not- oder Konfliktlage gemäß § 8 Abs. 3 SGB VIII, bei der sensible Daten ohne Kenntnis der Personensorgeberechtigten erhoben, sowie überdies die Aufnahme einer Verpflichtung zur Berücksichtigung des Verständnisvermögens und der Hilfsbedürftigkeit von Kindern bezogen auf Form und Inhalt der Benachrichtigung nach einer Schutzverletzung und auch die Berücksichtigung der Grundrechte und Interessen von Kindern bei der Risikoanalyse und bei der Festlegung von Schutzmaßnahmen in der Datenschutz-Folgenabschätzung (ausführlich Roßnagel 2020, s. zu konkreten Vorschlägen Roßnagel/Geminn 2020).

3. *Maßnahmen zum Schutz von Kindern müssen stets von Befähigungsmaßnahmen begleitet werden*

Sowohl Staat, Schule als auch Eltern sollten Medienerziehung und Medienbildung vorantreiben, indem sie Kinder über ihre Privatheitsrechte informieren. Dazu sollten Kinder zunächst die verschiedenen Formen von Privatheit in digitalen Kontexten kennen und auch lernen, diese selbst anzupassen. Bereits in jungen Jahren brauchen Kinder Eltern, Erziehende und Lehrende, die im Bereich Medienbildung kompetent sind. Der Digitalpakt der Bundesregierung sollte daher neben der Anschaffung datenschutzkonformer Hard- und Software (Datenschutz by Design und Default) und der Bereitstellung entsprechender Infrastrukturen auch die didaktische und pädagogische Förderung digitaler Kompetenzen in Erziehungs- und Bildungseinrichtungen im Blick haben. Ziel dabei wäre es, dass Kinder selbst informierte Entscheidungen treffen können und für sie verständliche, transparente Informationen erhalten.

4. *Anreizsysteme für Datenschutz by Design und by Default bei Plattformbetreibern, Unternehmen und Bildungseinrichtungen sollten staatlich gefördert werden*

Selbstbestimmung im Digitalen sollte der Standard sein – und nicht erst von Seiten der Nutzenden aktiv über Privacy-Einstellungen aktiviert werden müssen. Dies ist besonders wichtig, wenn sich Angebote auch an Kinder richten oder von Kindern genutzt werden. Es muss für Kinder selbst

zumindest verständlich und anpassbar sein, in welchem Kontext von Privatheit und Öffentlichkeit sie sich jeweils befinden und dies muss für sie einfach während der Benutzung einfach erkennbar sein, z.B. über auditive Mitteilungen oder Rückmeldungen („Wenn Du das abschickst, können es alle Menschen sehen, die das gleiche Angebot nutzen.“) oder über visuelle Gestaltung. Bei den Inhalten und der Art und Weise der Hinweise ist aber darauf zu achten, dass sie nicht verstörend wirken oder zu anderen negativen Effekten führen, etwa, weil die Kinder davon ausgehen, dass in jeder Risikosituation eine Mitteilung erscheint. Die Selbstbestimmung von Kindern im Digitalen sollte bereits bei der Konzeption digitaler Angebote berücksichtigt werden. Unternehmen sollten staatliche Anreizsysteme vorfinden, sodass für sie der Einbau von Datenschutz by Design und by Default am Ende Wettbewerbsvorteil und nicht -nachteil ist.

5. Die Digitalisierung entwickelt sich rasant. Privatheit und Datenschutz als die Demokratie sichernde Menschenrechte zu gewährleisten, bedarf gesamtgesellschaftlicher, interdisziplinärer und kontextsensibler Ansätze

Die Möglichkeit zu entscheiden, welche Informationen in bestimmten Kontexten oder mit bestimmten Personen geteilt werden und welche nicht, ist mit weiteren kindlichen Grundrechten verknüpft. Sie ist grundlegend für persönliche Autonomie und Menschenwürde. Damit ermöglicht Privatheit erst viele Aktivitäten und Strukturen einer demokratischen Gesellschaft. Sie ist ein Kernthema freiheitlicher Demokratien im Zuge der Digitalisierung. Zu erkennen, wie Heranwachsende Privatheit heute im Digitalen erleben, verstehen und wie sich dies im Altersverlauf entwickelt ist ein Desiderat aktueller und zukünftiger Forschung.

Notwendig hierzu ist ein „holistic child-rights-oriented approach“ (Milkaite/Lievens 2019), in dem beispielsweise neue rechtliche oder Regulierungsmaßnahmen mit Blick auf ihre Auswirkung auf das gesamte Spektrum von Kinderrechten beurteilt und diese systematisch mitgedacht werden. Um dies voranzubringen, braucht es interdisziplinär ansetzende Langzeitstudien, auch unter Beteiligung von Kindern und Jugendlichen, inklusive Partizipationsformen für Kinder auch bei der Gestaltung von Maßnahmen, innovative technische Ansätze, gesellschaftliche Diskurse und einen zukunftsfähigen und flexiblen Kinder- und Jugendmedienschutz.

Literatur

Barnes, Susan B. (2006): *A privacy paradox: Social networking in the United States.* In: First Monday, 11(9). Online verfügbar unter: https://doi.org/10.5210/fm.v11i9.1394 (Abfrage am: 29.09.2020).

Baruh, Lemi / Secinti, Ekin / Cemalcilar, Zeynep (2017): *Online privacy concerns and privacy management: A meta-analytical review.* In: Journal of Communication 67(1), S. 26-53.

Bieker, Felix / Hansen, Marit (2017): *Datenschutz "by Design" und "by Default" nach der neuen europäischen Datenschutz-Grundverordnung*. In: RDV, Zeitschrift Recht der Datenverarbeitung (4), S. 165-170.

Borgstedt, Silke / Roden, Ingo / Borchard, Inga / Rätz, Beate / Ernst, Susanne (2014): *DIVSI U25-Studie: Kinder, Jugendliche und junge Erwachsene in der digitalen Welt.* Heidelberg: Sinus-Institut. Online verfügbar unter: https://www.divsi.de/publikationen/studien/divsi-u25-studie-kinder-jugendliche-und-junge-erwachsene-in-der-digitalen-welt/index.html (Abfrage am: 29.09.2020).

Brüggen, Nils / Dreyer, Stephan / Gebel, Christa / Lauber, Achim / Müller, Raphaela / Stecher, Sina (2019): *Gefährdungsatlas. Digitales Aufwachsen. Vom Kind aus denken. Zukunftssicher handeln.* Bundesprüfstelle für jugendgefährdende Medien. Online verfügbar unter: https://www.klicksafe.de/service/aktuelles/news/detail/bundespruefstelle-fuer-jugendgefaehrdende-medien-veroeffentlicht-gefaehrdungsatlas/ (Abfrage am: 29.09.2020).

Croll, Jutta (2019): *Das Recht des Kindes auf Privatsphäre in einer digitalisierten Lebenswelt. Frühe Kindheit* 2 (19), S. 24-31. Online verfügbar unter: http://fruehe-kindheit-online.de/product_info.php?info=p423_das-recht-des-kindes-auf-privatsphaere-in-einer-digitalisierten-lebenswelt.html (Abfrage am: 29.09.2020).

Culnan, Mary J. / Armstrong, Pamela K. (1999): *Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation.* In: Organization Science 10 (1), S. 104-115.

Datenethikkommission der Bundesregierung (2019): *Gutachten der Datenethikkommission*. Online verfügbar unter: https://datenethikkommission.de/ (Abfrage am: 29.09.2020).

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: European journal of social psychology 45(3), S. 285-297.

Dreyer, Stephan (2018): *On the Internet, nobody knows you're a kid. Zur (Nicht-)Erkennbarkeit Minderjähriger in digitalen Medienumgebungen.* In: merzWissenschaft (6), S. 65-78.

Engels, Barbara (2018): *Datenschutzpräferenzen von Jugendlichen in Deutschland: Ergebnisse einer Schülerbefragung.* In: IW-Trends-Vierteljahresschrift zur empirischen Wirtschaftsforschung 45 (2), S. 3-26.

Fahlquist, Jessica Nihlén (2015): *Responsibility and privacy - ethical aspects of using GPS to track children.* In: Children & Society 29 (1), S. 38-47.

Feinberg, Joel (1980): *The child's right to an open future in whose child. Childrens' rights, parental authority, and state power*. Totowa, NJ: Rowman and Littlefield, S. 123-153.

Friedewald, Michael / Quinn, Regina Ammicht / Hagendorff, Thilo / Hansen, Marit / Heesen, Jessica / Hess, Thomas / Krämer, Nicole / Lam- la, Jörn / Matt, Christian / Roßnagel, Alexander / Waidner, Michael (2018): *Tracking. Beschreibung und Bewertung neuer Methoden*. White Paper. In: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Online verfügbar unter: file:///Users/admin/Downloads/Forum-Privatheit-Whitepaper-Tracking-1.pdf (Abfrage am 2.3.2021).

Frense, Elena (2020): *Partizipativer Jugendmedienschutz. Anforderungen an einen zeitgemäßen Jugendmedienschutz aus Perspektive von Kindern und Jugendlichen*. Wochenschau Verlag.

Geminn, Christian / Roßnagel, Alexander (2015): *„Privatheit" und, „Privatsphäre" aus der Perspektive des Rechts - ein Überblick*. In: JuristenZeitung 70 (14), S. 703-708.

Genner, Sarah / Süss, Daniel (2017): *Socialization as media effect. The international encyclopedia of media effects*, S. 1-15.

Hajok, Daniel (2019): *Der veränderte Medienumgang von Kindern. Tendenzen aus 19 Jahren KIM-Studie.* In: JMS Jugend Medien Schutz-Report 42 (3), S. 6-8.

Heeg, Rahel / Genner, Sarah / Steiner, Olivier / Schmid, Magdalene / Suter, Lilian / Süss, Daniel (2018): *Generation Smartphone. Ein partizipatives Forschungsprojekt mit Jugendlichen.* Online verfügbar unter: http://www.generationsmartphone.ch./ (Abfrage am: 29.09.2020).

Holtz, Leif-Erik / Nocun, Katharina / Hansen, Marit (2010): *Towards displaying privacy information with icons.* In: Simone Fischer-Hübner / Penny Duquenoy / Marit Hansen / Ronald Leenes and Ge Zhang (eds.), Privacy and Identity Management for Life: 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010, Revised Selected Papers, Springer, Berlin, Heidelberg, 2011, pp. 338-348.

Kaldestad, Øyvind H. (2018): *Report: Deceived by Design. Forbrukerrådet.* Online verfügbar unter: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/ (Abfrage am: 29.09.2020).

Karaboga, Murat / Schütz, Philip / Friedewald, Michael / Zoche, Peter / Matzner, Tobias / Mothes, Cornelia / Nebel, Maxi / Ochs, Carsten / Simo Fhom, Hervais (2014): *Selbstdatenschutz. White Paper.* In: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Online verfügbar unter: https://www.forum-privatheit.de/download/selbstdatenschutz-2-auflage-2014/ (Abfrage am: 29.09.2020).

Krotz, Friedrich / Hepp, Andreas (2012): *Mediatisierte Welten: Forschungsfelder und Beschreibungsansätze.* Bremen: Springer-Verlag.

Kutscher, Nadia (2012): *Medienbildung in der Kindheit.* In: MedienPädagogik. Zeitschrift für Theorie und Praxis der Medienbildung 22, S. 1-16.

Kutscher, Nadia / Bouillon, Ramona (2018): *Kinder. Bilder. Rechte. Persönlichkeitsrechte von Kindern im Kontext der digitalen Mediennutzung in der Familie.* In: Schriftenreihe des Deutschen Kinderhilfswerkes e. V. (4), S. 1-97.

Lansdown, Gerison (2005): *The evolving capacities of the child.* UNICEF Innocenti Research Centre, Innocenti Insights 5(18).

Livingstone, Sonia / Stoilova, Maria / Nandagiri, Rishita (2019): *Children's data and privacy online: growing up in a digital age: an evidence review.* London School of Economics and Political Science: London, UK.

Lupton, Deborah / Williamson, Ben (2017): *The datafied child: The dataveillance of children and implications for their rights.* In: New Media & Society 19(5), S. 780-794.

Manske, Julia / Knobloch, Tobias (2017): *Datenpolitik jenseits von Datenschutz*. In: Stiftung Neue Verantwortung, S. 1-97.

Mascheroni, Giovanna / Jorge, Ana / Farrugia, Lorleen (2014): *Media representations and children's discourses on online risks: Findings from qualitative research in nine European countries.* In: Cyberpsychology: Journal of Psychosocial Research on Cyberspace 8(2). Online verfügbar unter: https://cyberpsychology.eu/article/view/4310/3361 (Abfrage am: 29.09.2020).

Matzner, Tobias / Masur, Philipp K. / Ochs, Carsten / von Pape, Thilo (2016): *Do-It-Yourself Data Protection—Empowerment or Burden?* In: Data protection on the move, S. 277-305.

Maywald, Jörg (2012): *Kinder haben Rechte! Kinderrechte kennen-umsetzen-wahren. Für Kindergarten, Schule und Jugendhilfe (0-18 Jahre).* Weinheim: Beltz.

Milkaite, Ingrida / Lievens, Eva (2019): *Children's rights to privacy and data protecton around the world: challenges in the digital realm.* In: European Journal of Law and Technology 10(1).

Monllos, Kristina (2019): *As TikTok's popularity rises, buyers say the ad team needs to grow to keep up.* Online verfügbar unter: https://digiday.com/marketing/tiktok-popularity-rises-buyers-say-ad-team-needs-grow-keep/ (Abfrage am: 29.09.2020).

Naplavova, Magdalena / Ludik, Tomas / Hruza, Petr / Bozek, Frantisek (2014): *General Awareness of Teenagers in Information Security.* In: International Journal of Information and Communication Engineering 8(11), S. 3552-3555.

Nebel, Maxi (2015): *Schutz der Persönlichkeit - Privatheit oder Selbstbestimmung, Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht.* In: Zeitschrift für Datenschutz, S. 517-522.

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.

Paus-Hasebrink, Ingrid / Sinner, Philip / Prochazka, Fabian / Kulterer, Jasmin (2018): *Auswertungsstrategien für qualitative Langzeitdaten: Das Beispiel einer Langzeitstudie zur Rolle von Medien in der Sozialisation Heranwachsender.* Auswertung qualitativer Daten, S. 209-225.

Piaget, Jean (1972): *Intellectual evolution from adolescence to adulthood.* In: Human Development 15(1), S. 1-12.

Powell, Kendall (2006): *Neurodevelopment: How does the teenage brain work?* In: Nature 442, S. 865–867.

Prinzing, Marlis (2019): *Eingeboren? Oder nur eingewandert ins Digitale? Warum die Abkehr vom Mythos einer Generation von Digital Natives Voraussetzung einer verantwortungsorientierten Bildungs- und Gesellschaftspolitik ist.* In: Stapf, Ingrid / Prinzing, Marlis / Köberer, Nina (Hg.): Aufwachsen mit Medien. Zur Ethik mediatisierter Kindheit und Jugend. Baden-Baden: Nomos, S. 283-295.

Rathgeb, Thomas / Behrens, Peter (2018a): *Jugendliche, Information, Medien. Basisuntersuchung zum Medienumgang Zwölf-bis 19-Jähriger. JIM-Studie 2018.* Medienpädagogischer Forschungsverbund Südwest.

Rathgeb, Thomas / Behrens, Peter (2018b): *Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang Sechs-bis 13-Jähriger. KIM-Studie 2018.* Medienpädagogischer Forschungsverbund Südwest.

Roßnagel, Alexander (2020): *Der Datenschutz von Kindern in der DS-GVO.* In: Zeitschrift für Datenschutz, S. 88-92.

Roßnagel, Alexander / Bile, Tamer / Nebel, Maxi / Geminn, Christian / Karaboga, Murat / Ebbers, Frank / Bremert, Benjamin / Stapf, Ingrid / Teebken, Mena / Thürmel, Verena / Ochs, Carsten / Uhlmann, Markus / Krämer, Nicole / Meier, Yannic / Kreutzer, Michael / Schreiber, Linda / Simo, Hervais (2020): *Einwilligung. Möglichkeiten und Fallstricke aus der Konsumentenperspektive*. In: Forum Privatheit und selbstbestimm-tes Leben in der digitalen Welt. Online verfügbar unter: file:///Users/admin/Downloads/Whitepaper-Einwilligung-4.pdf (Abfrage am 2.3.2021).

Roßnagel, Alexander / Geminn, Christian (2020): *Datenschutz-Grundverordnung verbessern! – Änderungsvorschläge aus Sicht der Verbraucher.* In: Datenschutz und Datensicherheit-DuD. 44, S. 287-292.

Stapf, Ingrid (2019): *„Ich sehe was, was Du auch siehst." Wie wir die Privatsphäre von Kindern im Netz neu denken sollten und was Kinder möglicherweise dabei stärkt – ein kinderrechtlicher Impuls.* In: frühe Kindheit 2(19), S. 12-25.

Stoycheff, Elizabeth (2016): *Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring*. In: Journalism & Mass Communication Quarterly 93(2), S. 296-311.

Tillmann, Angela / Hugger, Kai-Uwe (2014): *Mediatisierte Kindheit–Aufwachsen in mediatisierten Lebenswelten.* In: Friedrichs, H. / Junge, T. / Sander, U. (Hg.): Jugendmedienschutz in Deutschland. Wiesbaden: VS Verlag-Verlag, S. 31-45.

Van Dijck, José / Poell, Thomas / De Waal, Martijn (2018): *The platform society: Public values in a connective world.* Oxford University Press.

Wang, Xuewei / Shi, Weiyan / Kim, Richard / Oh, Yoojung / Yang, Sijia / Zhang, Jingwen / Yu, Zhou (2019): *Persuasion for Good: Towards a Personalized Persuasive Dialogue System for Social Good.* Online verfügbar unter: https://arxiv.org/pdf/1906.06725.pdf (Abfrage am: 29.09.2020).

Zuboff, Shoshana (2019): *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Profile Books.

Exemplarische Ressourcen und Initiativen

Im deutschsprachigen Raum

- Dokumentation der Jahrestagung des Forum Privatheit 2019: https://www.forum-privatheit.de/jahreskonferenz-2019/
- https://www.klicksafe.de/ speziell zur Privatheit: https://www.klicksafe.de/themen/datenschutz/privatsphaere/ und Datenschutz: https://www.klicksafe.de/themen/datenschutz/

Im internationalen Raum

- Richtlinien des Europarats zu Kinderrechten in digitalen Umwelten: http://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a
- Aktuelle Studien zu Privatheit von Kindern: http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline
- Ein Toolkit für Kinder, Erziehende, Eltern und Policy Maker: http://www.lse.ac.uk/my-privacy-uk
- Plattform für ein besseres Internet für Kinder zum Austausch von Wissen, Expertise und Best Practice: https://www.betterinternetforkids.eu/
- Non-Profit-Organisation zur Stärkung der Sicherheit von Kindern im Internet: https://www.childnet.com/
- Industry Toolkit von UNICEF (2018): https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

Autorinnen und Autoren

Dr. Regina Ammicht Quinn ist Professorin am und Sprecherin des Internationalen Zentrums für Ethik in den Wissenschaften (IZEW) der Universität Tübingen.
E-Mail: regina.ammicht-quinn@uni-tuebingen.de

Jutta Croll ist Vorstandsvorsitzende der Stiftung Digitale Chancen und Leiterin des Projekts Kinderschutz und Kinderrechte in der digitalen Welt.
E-Mail: jcroll@digitale-chancen.de

Andrea Drexl studiert im Master Angewandte Forschung in der Sozialen Arbeit und ist studentische Hilfskraft am JFF – Institut für Medienpädagogik in Forschung und Praxis, München.
E-Mail: andrea.drexl@jff.de

Dr. Stephan Dreyer ist Senior Researcher für Medienrecht & Media Governance am Leibniz-Institut für Medienforschung | Hans-Bredow-Institut, Hamburg.
E-Mail: s.dreyer@leibniz-hbi.de

Dr. Susanne Eggert ist stellvertretende Leiterin der Abteilung Forschung am JFF – Institut für Medienpädagogik in Forschung und Praxis, München.
E-Mail: susanne.eggert@jff.de

Silvan Flückiger ist wissenschaftlicher Mitarbeiter am Robo-Lab an der Pädagogischen Hochschule der Fachhochschule Nordwestschweiz (FHNW).
E-Mail: silvan.flueckiger@fhnw.ch

Elena Frense ist wissenschaftliche Mitarbeiterin der Stiftung Digitale Chancen, Lehrbeauftragte im Masterstudiengang Childhood Studies and Children's Rights an der Fachhochschule Potsdam und Mitbegründerin der Kinderrechtsinitiative Children's Rights Academy.
E-Mail: efrense@digitale-chancen.de

Dr. Michael Friedewald leitet das Geschäftsfeld Informations- und Kommunikationstechnik am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe. Er ist Koordinator des Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.
E-Mail: michael.friedewald@isi.fraunhofer.de

Dr. Christian Geminn ist Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel.
E-Mail: c.geminn@uni-kassel.de

Marit Hansen ist Landesbeauftragte für Datenschutz Schleswig-Holstein.
E-Mail: marit.hansen@datenschutzzentrum.de

Asmae Harrach-Lasfaghi ist Betriebswirtin (B.A.), Kindheits- und Familienpädagogin (B.A.) und studiert aktuell den Master Pädagogik und Management in der Sozialen Arbeit. Sie arbeitet als wissenschaftliche Hilfskraft an der TH Köln am Forschungsschwerpunkt Nonformale Bildung.
E-Mail: asmae.lasfaghi@gmx.de

PD Dr. Jessica Heesen ist Leiterin des Forschungsschwerpunkts Medienethik und Informationstechnik am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen und Mitglied im Forum Privatheit.
E-Mail: jessica.heesen@uni-tuebingen.de

Dr. Gerrit Hornung ist Professor für Öffentliches Recht, IT-Recht und Umweltrecht an der Universität Kassel.
E-Mail: gerrit.hornung@uni-kassel.de

Dr. Andreas Janson ist Postdoktorand und Projektleiter Institut für Wirtschaftsinformatik der Universität St.Gallen (IWI-HSG).
E-Mail: andreas.janson@unisg.ch

Leonie Kreidel ist Studierende der Psychologie und studentische Hilfskraft am Fachgebiet Wirtschaftsinformatik der Universität Kassel.
E-Mail: leonie.kreidel@wi-kassel.de

Dr. Nicole Krämer ist Professorin für Sozialpsychologie – Medien und Kommunikation an der Universität Duisburg-Essen in der Fakultät für Ingenieurwissenschaften.
E-Mail: nicole.kraemer@uni-due.de

Dr. Jan Marco Leimeister ist Professor für Wirtschaftsinformatik an der Universität Kassel sowie am Institut für Wirtschaftsinformatik an der Universität St. Gallen (IWI-HSG).
E-Mail: leimeister@uni-kassel.de

Sonia Livingstone DPhil (Oxon), FBA, FBPS, FAcSS, FRSA, OBE is a professor in the Department of Media and Communications at the London School of Economics and Political Science.
E-Mail: S.Livingstone@lse.ac.uk

Dr. Nicholas Martin ist Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für System- und Innovationsforschung ISI im Competence Center Neue Technologien.
E-Mail: nicholas.martin@isi.fraunhofer.de

Yannic Meier ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Sozialpsychologie – Medien und Kommunikation an die Universität Duisburg-Essen in der Fakultät für Ingenieurwissenschaften.
E-Mail: yannic.meier@uni-due.de

Dr. Judith Meinert ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Sozialpsychologie – Medien und Kommunikation an die Universität Duisburg-Essen in der Fakultät für Ingenieurwissenschaften.
E-Mail: judith.meinert@uni-due.de

Jule Murmann ist wissenschaftliche Mitarbeiterin am Institut für Medienforschung und Medienpädagogik der TH Köln.
E-Mail: jule.murmann@th-koeln.de

Dr. Carsten Ochs ist Postdoc am Fachgebiet Soziologische Theorie der Universität Kassel.
E-Mail: carsten.ochs@uni-kassel.de

Rishita Nandagiri is an LSE Fellow in Health and International Development (HID) at the Department of International Development.
E-Mail: r.nandagiri@lse.ac.uk

Dr. Maxi Nebel ist wissenschaftliche Mitarbeiterin in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) unter der Leitung von Prof. Dr. Alexander Roßnagel am Wissenschaftlichen Zentrum für Informations-Technikgestaltung (ITeG) an der Universität Kassel.
E-Mail: m.nebel@uni-kassel.de

Andreas Oberlinner ist wissenschaftlicher Mitarbeiter am JFF – Institut für Medienpädagogik in Forschung und Praxis, München.
E-Mail: andreas.oberlinner@jff.de

Jen Persson ist Direktorin der zivilgesellschaftlichen NGO defenddigitalme.
E-Mail: jen@defenddigitalme.com / Website: https://defenddigitalme.org/

Dr. Senta Pfaff-Rüdiger ist wissenschaftliche Mitarbeiterin am JFF – Institut für Medienpädagogik in Forschung und Praxis, München.
E-Mail: senta.pfaff-ruediger@jff.de

Ricarda T.D. Reimer ist Leiterin der Fachstelle Digitales Lehren und Lernen an der Pädagogischen Hochschule der Fachhochschule Nordwestschweiz (FHNW).
E-Mail: ricarda.reimer@fhnw.ch

Dr. Alexander Roßnagel ist Seniorprofessor für öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel, Sprecher des Forums Privatheit und selbstbestimmtes Leben in der digitalen Welt sowie Datenschutzbeauftragter des Landes Hessen.
E-Mail: a.rossnagel@uni-kassel.de

Dr. Sofia Schöbel ist Postdoktorandin und Projektleiterin am Fachgebiet Wirtschaftsinformatik der Universität Kassel.
E-Mail: sofia.schoebel@uni-kassel.de

Dr. Andreas D. Schulz ist Lehrer an einer Schule in Kassel und Lehrbeauftragter an der Universität Kassel.
E-Mail: adschulz@uni-kassel.de

Dr. Matthias Söllner ist Professor für Wirtschaftsinformatik und Systementwicklung an der Universität Kassel.
E-Mail: soellner@uni-kassel.de

Dr. Ingrid Stapf ist Mitglied im Forum Privatheit und forscht am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) an der Universität Tübingen zu Themen der Informations- und Medienethik. Sie habilitiert sich zu einer Kinder-Medien-Ethik im digitalen Zeitalter.
E-Mail: ingrid.stapf@uni-tuebingen.de

Dr. Mariya Stoilova holds a post-doctoral research position at the London School of Economics and Political Science (LSE).
E-Mail: m.stoilova@lse.ac.uk

Reinhold Schulze-Tammena, StD ist Fachbereichsleiter für Gesellschaftswissenschaften am Schiller-Gymnasium Berlin (Staatliche Europaschule Berlin).
E-Mail: reinhold.schulze-tammena@gmx.de

Dr. Isabel Zorn ist Professorin für Medienpädagogik am Institut für Medienforschung und Medienpädagogik an der TH Köln und Leiterin des Forschungsschwerpunkt Digitale Technologien und Soziale Dienste (DiTeS).
E-Mail: isabel.zorn@th-koeln.de