

Franco Rau, Britta Galanamatis, Lars Gerber &amp; Anna Geritan

## Digitale Bildung und Datenschutz: Eine Herausforderung für die Lehrer\*innenbildung

### Abstract

Datenschutz und informationelle Selbstbestimmung sind Bestandteile aktueller Leitbilder einer Digitalen Bildung. Im Kontext der COVID-19-bedingten Schulschließungen in Deutschland und der vorrangigen Nutzung digitaler Medien zeigte sich jedoch, dass Datenschutz in der Schule aus bildungswissenschaftlicher Perspektive kaum untersucht und in der bildungsadministrativen und pädagogisch-praktischen Schulwirklichkeit nicht systematisch verankert ist. Der Beitrag veranschaulicht diese Diskrepanz und diskutiert weiterführend die Frage, welche Gestaltungsperspektiven sich für die Lehrer\*innenbildung eröffnen.

Privacy, data protection, and informational self-determination are components of current mission statements for “Digitale Bildung”. During the COVID-19 pandemic, schools in Germany were closed for a significant amount of time, which led to a significantly increased use of digital media. These conditions revealed that privacy and data protection in schools have hardly been investigated from an educational science perspective and have not been systematically implemented in schools. The article shows this discrepancy and discusses the question of which perspectives open up for teacher education.

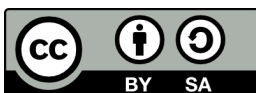
### Schlagwörter:

Digitale Bildung, Datenschutz, Privatheit, Digitalisierung, Schulentwicklung, Schule  
digital literacy, data protection, privacy, school development, school

### 1. Schulschließungen, Datenschutz und Digitale Bildung

Seit Beginn der pandemiebedingten Schulschließungen werden Fragen zur Gestaltung digitaler Lernumgebungen sowie des Datenschutzes zunehmend öffentlich diskutiert. In diesem Zusammenhang geht es auch um das Verhältnis von Datenschutz, der als zentrales Grundrecht markiert wird, und datengetriebenen Geschäftsmodellen, z. B. beim Einsatz zentraler Schulsoftware. Susanne Eisenmann als Bildungsministerin für Baden-Württemberg erhielt 2020 beispielsweise den sogenannten BigBrotherAward in der Kategorie „Digitalisierung“, weil sie relevante Dienste der landesspezifischen Bildungsplattform von Microsoft betreiben lassen wollte (vgl. Fischer, Wawrzyniak & Simon, 2020).<sup>1</sup> Fragen zum Datenschutz wurden insbesondere thematisiert, weil Lehrpersonen und Schüler\*innen

<sup>1</sup> Als internationales Projekt dokumentieren die BigBrotherAwards eklatante Datenschutzprobleme und problematische Datenpraktiken in unterschiedlichen Kategorien (z. B. Bildung, Wirtschaft). In Deutschland organisiert der Verein Digitalcourage e. V. die Veranstaltung und die Jury besteht u. a. aus Mitgliedern wie der Deutschen Vereinigung für Datenschutz und dem Chaos Computer Club (vgl. <https://bigbrotherawards.de/ueber-uns>).



auf digitale Informations- und Kommunikationsformate während der Schulschließungen angewiesen waren, wenn sie sich untereinander austauschen und organisieren wollten (z. B. Videokonferenzsysteme, Instant-Messenger, Lehr-Lernplattformen). Da eine leistungsfähige schulische Infrastruktur in Deutschland nicht flächendeckend vorhanden war (und noch immer nicht vorhanden ist), wurden häufig Anwendungen genutzt, die aus einer datenschutzrechtlichen Perspektive problematisch sind (vgl. BlnBDI, 2021a; vgl. HBDI, 2021a: S. XXIV f.). Während verschiedene unabhängige Datenschutzbehörden des Bundes und der Länder unterschiedliche Anwendungen im letzten Jahr aufgrund der Pandemiesituation duldeten (vgl. HBDI, 2021a), weisen sie regelmäßig daraufhin, dass Datenschutz ein Grundrecht darstellt, welches nicht beliebig einzuschränken ist (vgl. Smolczyk & Kugelman, 2021). Zugleich wird Datenschutz in der Bildungspraxis nicht selten als Bremse für eine innovative Lernkultur diskutiert (vgl. z. B. Scheppler & Wampfler, 2021).

Die Diskussion über eine zeitgemäße Bildung in einer digital geprägten Welt hat nicht mit der Pandemie begonnen, aber durch diese enorm an Aufmerksamkeit gewonnen. Zugleich entsteht mitunter der Eindruck, dass die komplexe Debatte auf die Organisation des digitalen Distanzunterrichts fokussiert und auf die technische Digitalisierung von Lehrmitteln verengt wird. ‚Digitale Bildung‘ in diesem begrenzten Verständnis birgt die Gefahr, der Komplexität des Themas nicht gerecht zu werden und „relevante Aspekte zu vernachlässigen“ (Döbeli Honegger, 2020: S. 4). In Abgrenzung von dieser Vorstellung verstehen wir den Terminus ‚Digitale Bildung‘ nach Irion (2020) als „Sammelbegriff für bildungsrelevante Fragen und Zielsetzungen angesichts der digitalen Transformationsprozesse in der Gesellschaft“ (Irion, 2020: S. 57). In Anlehnung an Irion interessieren wir uns für Datenschutz als bildungsbezogene Aufgabe im Kontext von Digitalisierungs- und Mediatisierungsprozessen, statt nur die Eignung sogenannter digitaler Tools in den Blick zu nehmen. Nach Hof (2017) geht es dabei nicht nur um Daten, die von Personen aktiv und bewusst bereitgestellt werden, sondern auch um unbewusst und unwissentlich abgegebene Daten (z. B. via Tracking) und Schlussfolgerungen, die aus den vorliegenden Daten über den Einzelnen gezogen werden können (z. B. Profiling) (vgl. Hof, 2017).

In Form eines narrativen Reviews wird gezeigt, dass Datenschutz aus bildungspolitischer Perspektive ein zentrales Element digitaler Bildung sein sollte und Lehrpersonen vor neuen Anforderungen und Aufgaben stehen (Abschnitt 2). Wie komplex diese Aufgaben für Lehrer\*innen sind, wird in Betrachtung des Forschungsstandes aus unterschiedlichen Perspektiven skizziert und durch eine erste Begriffsdiskussion konkretisiert (Abschnitt 3). An Praxisbeispielen wird diskutiert, in welchen Spannungsfeldern Lehrpersonen aktuell handeln müssen und welchen Herausforderungen sie begegnen (Abschnitt 4). Um Lehrpersonen und Personen der inneren und äußeren Schulentwicklung zu befähigen, Datenschutz als bildungsbezogene Aufgabe im Kontext aktueller Digitalisierungs- und Mediatisierungsprozesse zu erkennen und realisieren zu können, wird abschließend argumentiert, dass sich auch die Lehrer\*innenbildung dem Thema Datenschutz sowie datenbezogenen Praktiken und Risiken aktiv stellen muss.

## 2. Leitbild: Datenschutz als Bestandteil digitaler Bildung

Der „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten“ wurde vom Bundesverfassungsgericht als Voraussetzung verstanden, um unter den „modernen Bedingungen der Datenverarbeitung“ (BVerfGE 65, 1 (33)) die eigene Persönlichkeit frei entfalten zu können. Diese Bedingungen betreffen auch Privatheits- bzw. Datenschutzrechte von Schüler\*innen, da ihre personenbezogenen Daten (z. B. Orte, Verhalten, Bewertungsdispositionen) in ihrer Freizeit und im Schulkontext beispielsweise bei der Nutzung scheinbar kostenloser Apps verarbeitet werden können. Es sollte insofern nicht überraschen, dass in bildungspolitischen Leitbildern Datenschutz bzw. das Recht auf informationelle Selbstbestimmung als systematischer Bestandteil digitaler Bildung gefordert wird (vgl. KMK, 2012: S. 6; vgl. KMK, 2017; vgl. BMBF, 2016). In Betrachtung der öffentlichen Diskussion sowie in Gesprächen mit Lehrenden an Schulen und in der Lehrer\*innenbildung entsteht gleichwohl der Eindruck, dass die Bedeutung und der Umfang der Aufgaben nicht allen Personen bewusst ist. Die folgenden Ausführungen eröffnen einen ersten Überblick über die Relevanz des Datenschutzes sowie damit verbundene Anforderungen. Die spezifischen Kompetenzen der Lehrenden werden am Beispiel von zwei exemplarischen Handlungsfeldern skizziert: Datenschutz als pädagogischer Aufgabenbereich zur Vermittlung von Medien- bzw. Datenkompetenz und Datenschutz als struktureller Aufgabenbereich zur Gestaltung digitaler Lernumgebungen.

### 2.1 Relevanz des Datenschutzes aus bildungspolitischer Perspektive

Die Relevanz des Datenschutzes im Kontext der Digitalisierung und Mediatisierung wird seit über zehn Jahren in diversen bildungspolitischen Positions- und Strategiepapieren markiert. Dazu gehören Beschlüsse und Strategiepapiere der Kultusministerkonferenz (vgl. KMK, 2012; vgl. KMK, 2017) und der Bundesregierung (2021) sowie von Bund und Ländern initiierte Expertenberichte und -empfehlungen (vgl. Deutscher Bundestag, 2011; vgl. BMFSFJ, 2013).

Ein zentrales Argument der verschiedenen Papiere widmet sich den technischen Digitalisierungsprozessen, die einerseits neue Möglichkeiten eröffnen und zugleich neue Gefahren beinhalten (vgl. KMK, 2012; vgl. KMK, 2017). Im Beschluss der KMK zur „Medienbildung in der Schule“ werden diesbezüglich „interaktive Medienangebote, soziale Online-Netzwerke und mediengestützte Dienstleistungen“ (KMK, 2012: S. 3) benannt. Aus der Perspektive der KMK betreffen diese „die Gesellschaft insgesamt wie den Einzelnen, insbesondere seine Privatsphäre, seine Persönlichkeitsrechte und seine Datenschutzgrundrechte“ (KMK, 2012: S. 3). Zu den zentralen Handlungsfeldern zur Ermöglichung einer umfassenden Medienbildung in der Schule gehört für die KMK bereits im Jahr 2012 der Bereich „Urheberrecht und Datenschutz“. An dieses Papier anknüpfend wird auch im Strategiepapier der KMK (2017) deutlich, dass die „Digitalisierung unserer Welt“ neue Fragestellungen und Herausforderungen mit sich bringt, die sich beispielsweise „zum Schutz der Privatsphäre“ (ebd.: S. 8) stellen. In den aufgeführten Handlungsfeldern zur

Erarbeitung angemessener Lösungen und Entscheidungen finden sich Aspekte des Datenschutzes u. a. als Facette digitaler Kompetenz, als Element einer zeitgemäßen Infrastruktur sowie zu klärende rechtliche Rahmenbedingungen (vgl. KMK, 2017).

Im Rahmen der Enquete-Kommission „Internet und digitale Gesellschaft“ wurde bereits vor zehn Jahren darauf hingewiesen, dass das Thema Datenschutz häufig vergessen werde, wenn „in der Praxis real auftretende Gefahren“ zum Jugendschutz diskutiert werden. Ein zentrales Problem bestehe darin, dass „fehlendes Wissen und fehlende Kompetenz immer wieder zu Verstößen gegen das Urheberrecht, den Datenschutz oder die Persönlichkeitsrechte anderer“ (Deutscher Bundestag, 2011: S. 13) führen. Ansätze zum Umgang mit diesen Problemen sieht die Enquete-Kommission in der systematischen Förderung von Medienkompetenz als gesamtgesellschaftlicher Querschnittsaufgabe. In der aktuellen Datenstrategie der Bundesregierung (2021) wird festgestellt, dass weder digitale Kompetenzen noch spezifische „Datenkompetenzen“ bisher curricular systematisch verankert sind. Dies betrifft sowohl Schüler\*innen und als auch Lehrpersonen. Als Zielperspektive wird der Anspruch formuliert, dass Schüler\*innen lernen, „wie Daten erhoben, verarbeitet, kritisch ausgewertet und genutzt werden.“ (Bundesregierung, 2021: S. 44). Die Relevanz dieser Zielperspektive ergibt sich aus der Erkenntnis, dass Lernende bereits in jungen Jahren anfangen „mit Daten umzugehen (etwa durch das Preisgeben der eigenen personenbezogenen Daten auf Social Media oder das Beitragen auf Open-Data-Plattformen)“ (ebd.). Umso wichtiger ist es, dass Schüler\*innen befähigt werden, bewusste Entscheidungen treffen zu können und einen „mündigen Umgang mit den eigenen Daten zu lernen“ (ebd.).

Im Vergleich der verschiedenen Strategie- und Positionspapiere wird deutlich, dass eine zeitgemäße Gestaltung digitaler Bildung nicht ohne die Berücksichtigung des Datenschutzes erfolgen sollte. Die kontinuierliche Veränderung technischer Möglichkeiten zur Datenerfassung, -speicherung und automatischen Verarbeitung und die damit verbundenen Praktiken sind zentrale Argumente, um auf die Bedeutung des Datenschutzes hinzuweisen.

## 2.2 Datenschutz als Unterrichtsthema und Vermittlungsaufgabe für Lehrpersonen

Die KMK hat in den vergangenen Jahren „Medienkompetenz“ (KMK, 2012: S. 4) bzw. den „kompetenten Umgang mit digitalen Medien“ (KMK, 2017: S. 13) zu einer grundlegenden Kulturtechnik erklärt. Wenngleich sich die Beschlüsse und Strategiepapiere hinsichtlich der verwendeten Begriffe unterscheiden, beinhalten sie konzeptionell die gemeinsame Zielperspektive, dass es für einen zeitgemäßen Datenschutz bzw. für die informationelle Selbstbestimmung der Lernenden in einer digital geprägten Welt eines spezifischen Wissens und spezifischer Kompetenzen bedarf. So versteht die KMK (2012) eine „umfassende Medienbildung“ als „unabdingbare Ergänzung des gesetzlichen Jugendmedien- und Datenschutzes“ (KMK, 2012: S. 6). Medienbildung kann aus Sicht der KMK (2012: S. 6) zur „Datensparsamkeit“ befähigen und die „digitale Sicherheit der persönlichen Kommunikation“ fördern. Damit wird ein Beitrag zur „eigenverantwortlichen informationellen Selbstbestimmung und zum persönlichen Datenschutz“ (KMK, 2012: S. 6) geleistet. Im Modell

der „Kompetenzen in der digitalen Welt“, über die Schüler\*innen am Ende ihrer Schullaufbahn verfügen sollen, werden die entsprechenden Fähigkeiten im Bereich „Schützen und sicher Agieren“ näher konkretisiert. Dieser Bereich umfasst explizit Aspekte der Datensicherheit sowie des Datenschutzes. Darunter versteht die KMK (2017) Aktualisierungen von Sicherheitseinstellungen, die Berücksichtigung von Jugendschutz- und Verbraucherschutzmaßnahmen, die Berücksichtigung von „Maßnahmen für Datensicherheit und gegen Datenmissbrauch“ und den Schutz der „Privatsphäre in digitalen Umgebungen durch geeignete Maßnahmen“ (KMK, 2017: S. 17). Wenngleich die KMK markiert, dass nicht „jedes Fach zur Entwicklung aller Kompetenzen“ beitragen wird, so sollen in Summe aller fachspezifischen Ausprägungen die Lernenden die Gelegenheit haben, sich alle Kompetenzen anzueignen (vgl. KMK, 2017: S. 20). Für die Lehrpersonen stellt sich die Frage, welche fachlichen Bezüge sich zu Themen des Datenschutzes eröffnen und wie sich diese vermitteln lassen.

Für die Vermittlung entsprechender Wissensbereiche und Kompetenzen sind Lehrpersonen in ihrem jeweiligen Fachunterricht zuständig. Damit sie diesem Anspruch gerecht werden können, soll u. a. eine verbindliche Verankerung von Medienbildung in der ersten und zweiten Phase der Lehrer\*innenbildung sowie die Entwicklung von angemessenen Fortbildungsangeboten erfolgen (vgl. KMK, 2012: S. 7; vgl. KMK 2017: S. 24 ff.). Als Ziel formuliert die KMK, dass Lehrpersonen „durch ihre Kenntnisse über Urheberrecht, Datenschutz und Datensicherheit“ in der Lage sind, ihre Lernenden zu befähigen, „bewusst und überlegt mit Medien und eigenen Daten in digitalen Räumen umzugehen und sich der Folgen des eigenen Handelns bewusst zu sein“ (KMK, 2017: S. 28). Die Entwicklung von Medienkompetenz und medienpädagogischer Kompetenz ist in diesem Zusammenhang als spezifische Aufgabe für Lehrpersonen zu verstehen (vgl. KMK, 2012: S. 7; KMK, 2017: S. 25).

Die Perspektive, Datenschutz als Facette von Medienkompetenz und damit als Thema des Unterrichts zu etablieren sowie als Vermittlungsaufgabe von Lehrpersonen zu betrachten, wird in bildungspolitischen Diskursen auch außerhalb der Kultusministerkonferenz diskutiert. Für die Enquete-Kommission ist Förderung von Medienkompetenz eine gesamtgesellschaftliche Querschnittsaufgabe, bei der Lehrpersonen einen relevanten Beitrag leisten sollen. Praktische Ansätze zur Realisierung dieser Aufgabe umfassen u. a. den Bereich der „Lehrerfortbildung“ sowie die „stärkere und verpflichtende Verankerung medienpädagogischer Inhalte in den Lehrplänen aller Schularten“ (Enquete, 2011: S. 35). In der aktuellen Datenstrategie der Bundesregierung finden sich vergleichbare Zielstellungen und Aufgaben. Beispielsweise sollen alle Schüler\*innen lernen, „wie Daten erhoben, verarbeitet, kritisch ausgewertet und genutzt werden“ (Bundesregierung, 2021: S. 44). Um dieses Ziel näher zu kommen, sollte „Datenkompetenz“ in „Lehrplänen verankert und altersgerecht aufbereitet werden“ (ebd.). Zugleich wird auf das Problem hingewiesen, „dass eine systematische oder flächendeckende Integration von Datenkompetenzen in die Lehrerinnen- und Lehrerbildung noch nicht geschehen ist“ (ebd.).

Mit der Vorstellung der exemplarisch ausgewählten Positionen wurde verdeutlicht, dass aus bildungspolitischer Perspektive unstrittig ist, dass Datenschutz und Digitale Bildung zusammenzudenken sind. Eine wiederkehrende Forderung lautet dabei, Datenschutz als Facette von Medienkompetenz zu betrachten, deren Vermittlung ein verpflichtendes Element des Schulunterrichts sowie der Lehrer\*innenbildung darstellt. Aus unterschiedlichen Positionen heraus wird auch markiert, dass damit neue Aufgaben für alle Phasen der Lehrer\*innenbildung entstehen.

### 2.3 Datenschutz als Kriterium zur Gestaltung digitaler Lernumgebungen

Ein zweiter zentraler Aufgabenbereich zur Realisierung von Datenschutz wird in der Gestaltung digitaler Lernumgebungen gesehen. Von Lehrpersonen wird erwartet, dass sie digitale Medien in systematischer Weise im Unterricht verwenden (vgl. KMK, 2017). In der Nutzung digitaler Lernumgebungen wird u. a. die Chance gesehen, einen Beitrag zur Individualisierung des Lernens zu leisten und so einen angemessenen Umgang mit heterogenen Lerngruppen zu ermöglichen (vgl. KMK, 2017: S. 13). Auf der Ebene der Unterrichtsgestaltung wird von Lehrer\*innen auch erwartet, „durch ihre Kenntnisse über Urheberrecht, Datenschutz und Datensicherheit sowie Jugendmedienschutz den Unterricht als einen sicheren Raum zu gestalten“ (KMK, 2017: S. 27 f.). Der systematische Einsatz digitaler Medien wird in diesem Zusammenhang sowohl an die jeweilige pädagogische Relevanz als auch an die Gestaltung sicherer und datenschutzkonformer Umgebungen geknüpft.

Diese Gestaltungsaufgabe zur Infrastrukturentwicklung betrifft Lehrer\*innen über ihren konkreten Unterricht hinaus bei der (Mit-)Gestaltung der jeweiligen Lernplattformen der eigenen Schulen sowie der Nutzung eigener oder externer digitaler Plattformen und Anwendungen außerhalb des eigenen Unterrichts. Aus Sicht der KMK (2012) stehen Schulen im Kontext der Digitalisierung auch vor rechtlichen Herausforderungen, welche u. a. die Gebiete „Datenschutz, Jugendschutz und Persönlichkeitsrecht“ betreffen (vgl. KMK, 2012: S. 8). Dafür bedarf es einer Sensibilisierung und Unterstützung aller an Schule beteiligten Akteur\*innen. Die KMK (2012) empfiehlt dafür „schulische Multiplikatorennetzwerke“ sowie die Kooperation mit weiteren Einrichtungen, wie beispielsweise den „Landesbeauftragten für Datenschutz“ (vgl. KMK, 2012: S. 8). Näher bestimmt werden entsprechende Empfehlungen und Anforderungen im Strategiepapier der KMK (2017). Es wird u. a. darauf hingewiesen, dass auf Ebene der schulischen Infrastruktur die genutzten „Plattformen, Lernumgebungen und Netzwerke datenschutzkonform sein“ (ebd.: S. 14) sollen. Zudem bedarf es der Entwicklung eines „Datenschutzkonzepts, nebst Verfahrensbeschreibung sowie eventueller Vereinbarungen zur Auftragsdatenverarbeitung“ (ebd.: S. 41).

Mit der KMK-Strategie (2017) wird an Lehrkräfte explizit die Aufgabe formuliert, sich in unterschiedlichen Rollen an der Gestaltung und der Nutzung digitaler Lernumgebungen zu beteiligen. Bei Nutzung sogenannter digitaler „Werkzeuge“ sowie bei der Entwicklung und Gestaltung digitaler Lernumgebungen ist der Datenschutz zu beachten.

Wissen über Datenschutz sowie datenbezogene Praktiken und Risiken benötigen Lehrpersonen u. a. in ihrer Rolle als Lehrende bei der Auswahl digitaler Medien für den Unterricht, in der potenziellen Rolle als Datenschutzbeauftragte einer Schule sowie als potenzielles Mitglied in schulischen Gremien zur Schulentwicklung, in denen Fragen zur Digitalisierung und des Datenschutzes ein relevantes Thema darstellen.

### 3. Datenschutz in der Schule: Erkenntnisse und zentrale Begriffe

Wie gezeigt werden konnte, wird der Begriff „Datenschutz“ in zahlreichen bildungspolitischen Strategie- und Positionspapieren verwendet, um den Anspruch an eine Digitale Bildung zu markieren (vgl. KMK, 2012; vgl. KMK, 2017; vgl. Bundesregierung, 2021) und damit verbundene Handlungsfelder als Vermittlungs- und Gestaltungsaufgabe näher zu bestimmen. Zugleich bleiben die verwendeten Termini wie „Datenschutz“, „Datensicherheit“ oder (personenbezogene) „Daten“ häufig unbestimmt. Bei öffentlichen sowie schulinternen Diskussionen wird diese Unbestimmtheit zum Problem, wenn die beteiligten Personen die gleichen Begriffe verwenden, aber damit unterschiedliche Bedeutungen verbinden. Mit den folgenden Ausführungen wird daher der Versuch unternommen, die aktuelle bildungswissenschaftliche Diskussion zum Datenschutz in der Schule zu skizzieren und die zentralen Begriffe in einem ersten Versuch näher zu bestimmen.

#### 3.1 Datenschutz in der Schule als kaum untersuchtes Forschungsfeld

In der bildungswissenschaftlichen Diskussion über digitale Bildung werden Fragen zur informationellen Selbstbestimmung und des Datenschutzes bisher nur randständig diskutiert. Die modernen Bedingungen der Datenverarbeitung, die Hof (2017: S. 102 ff.) mit den Begriffen „Datafication“, „Hyperconnectivity“ und „Commercialization“ charakterisiert, werden im Schulkontext durch einen neutralen Werkzeugbegriff auf sprachlicher Ebene häufig ausgeblendet (vgl. Kraut, 2012). Medienpädagogische Forschungsarbeiten zur Reflexion von Algorithmen und Datafizierung (vgl. Gapski, 2015; Iske, 2016; Eder, Mikat & Tilman, 2017) haben keinen Fokus auf Schule. Der Jugendmedienschutz beschäftigt sich zwar mit medienbezogenen Risiken (vgl. Friedrichs, Junge & Sander, 2013), allerdings werden datenbezogene Risiken im Kontext institutioneller Bildung nur selten diskutiert (vgl. Zorn, Harrach-Lasfaghi & Murmann, 2019). Mit Blick auf Veröffentlichungen aus Deutschland kann festgehalten werden, dass bei der Modellierung digitaler Kompetenzen Datenschutzaspekte unter dem Begriff „data literacy“ bisher vornehmlich für den Hochschulkontext diskutiert werden (vgl. Heidrich, Bauer & Krupka, 2018; vgl. Schüller, 2019). Der Bedarf nach einer Modellierung von „data literacy“ wird auch international gefordert (vgl. Audenhove, Broeck & Mariën, 2020). In empirischen Studien mit Schüler\*innen (vgl. Eickelmann, Bos, Gerick, Goldhammer, Schaumburg, Schwippert, Senkbeil & Vahrenhold, 2019) werden datenschutzbezogene Kompetenzen kaum erfasst. Mit Blick auf die Privatheit Heranwachsender sprechen Stapf, Ammicht Quinn, Friedewald, Heesen,

und Krämer (2021) von einem neuen interdisziplinären Forschungsgebiet. Auch in Studien mit Lehrkräften (vgl. Lorenz, Bos, Endberg, Eickelmann, Grafe & Vahrenhold, 2017) wird Datenschutz als Thema in Deutschland bisher selten untersucht.

Ein relevantes Thema war Datenschutz in den letzten Jahren insbesondere in praxisorientierter Begleitforschung von Pilot- und Modellschulprojekten (z. B. Kammerl, Unger, Günther & Schwedler, 2016; Gerick et al., 2019; Gerick & Eickelmann 2020; Rau, Grell, Geritan, Galanamatis & Gerber, 2021; Reichwein, 2021). Sowohl bei der Umsetzung pädagogischer Konzepte zum Lehren und Lernen in einer digital geprägten Welt (z. B. Kammerl et al., 2016; Rau et al., 2021) als auch bei der Implementierung spezifischer technischer Infrastruktur (z. B. Gerick et al., 2019; Reichwein, 2021) zeigten sich vielfältige Herausforderungen und Überforderungen, die unter dem Begriff Datenschutz diskutiert werden. Bei der Schulorganisation zeigten sich Probleme in einem Modellschulprojekt dahingehend, dass die Mehrheit der Schulen kein Datenschutzkonzept hatte (vgl. Gerick et al., 2019: S. 85 ff.). Bei der Unterrichtsgestaltung erweist sich die Auswahl von datenschutzkonformen digitalen Anwendungen zur Interaktion mit Schüler\*innen als Herausforderung für Lehrpersonen (z. B. Gerick & Eickelmann, 2020; Rau et al., 2021). Datenschutz wird in diesem Kontext nicht als selbstverständlicher und realistischer Bestandteil digitaler Bildung betrachtet, sondern von Lehrenden als Hindernis digitaler Bildung beschrieben.

Aus rechtlicher Perspektive lassen sich die datenschutzrechtlichen Anforderungen im Schulbetrieb als „komplex“ beschreiben (vgl. Heckmann, 2019). Wenngleich zu Aspekten des Datenschutzes und zum schulischen Datenschutzrecht Ausführungen existieren (vgl. Sassenberg, 2019), führen diese Ausführungen nicht zu einer systematischen Beachtung in der Schulentwicklung. So stellen Dehnert et al. (2019) fest: „Sofern in den Schulen vor Ort keine Personen verfügbar sind, die über datenschutzrechtliche Grundkenntnisse verfügen, muss sich die Umsetzung der Datenschutzverordnung in vielen Fällen auf das Abarbeiten von Checklisten und das Ausfüllen von Musterdokumenten beschränken“ (Dehnert, Glahe, Kunze & Schulze, 2019: S. 296). Entsprechend verweist Feustl (2021) darauf, dass Lehrpersonen aus Gründen der Risikoreduzierung einer von ihnen wahrgenommenen Rechtsunsicherheit beim Einsatz digitaler Medien im Unterricht zurückhaltend sind. Statt digital souverän agieren zu können, setzen sich Lehrpersonen aufgrund von subjektiv empfundener Unsicherheit erst gar nicht mit digitalen Medien auseinander (vgl. Feustl, 2021).

### 3.2 Datenschutz: Versuch einer Annäherung an zentrale Begriffe

Der Begriff **Datenschutz** ist in vielen Kontexten etabliert und zugleich ungenau und missverständlich (vgl. von Lewinski, 2014: S. 1). Oberflächlich wird der Begriff mitunter so gedeutet, dass es dabei um den Schutz von Daten gehe. In seiner Dekonstruktion des Begriffes führt von Lewinski (2014) in den Datenschutz als „einen Schutz von Rechtspositionen von Personen“ (von Lewinski, 2014: S. 4) ein. Eine erste Annäherung an die vielfältigen Begriffsverständnisse bietet für ihn die Auseinandersetzung mit den Teilfragen „was



(,Schutzgut') wird (vom ,Datenschutz') bei wem (,Betroffener') und vor wem (,verantwortliche Stelle') wie (,Schutzkonzept') geschützt" (ebd.: S. 6). Datenschutz ist in diesem Sinne nicht auf den Schutz von Daten bezogen, sondern „auf den Schutz vor Daten(verarbeitungen)" (von Lewinski, 2014: S. 4). Auch Petrlc & Sorge (2017: S. 11) betonen, dass der Begriff Datenschutz in Deutschland nicht den Schutz von Daten bezeichne, sondern den „Schutz des Einzelnen vor Beeinträchtigung in seinem Persönlichkeitsrecht durch Umgang mit seinen personenbezogenen Daten" (Petrlc & Sorge, 2017: S. 11). Für den folgenden Beitrag orientieren wir uns am Begriffsverständnis von Pohle & Hölzel (2020) und bezeichnen mit dem Begriff Datenschutz die „Menge der Vorkehrungen zur Verhinderung unerwünschter Folgen von Informationsverarbeitung" (Pohle & Hölzel, 2020: S. 1). Eine systematische Übersicht über unerwünschte Folgen und Risikokategorien der Verarbeitung personenbezogener Daten bzw. Informationen wurde von Drackert (2014) entwickelt. Er unterscheidet u. a. strukturelle Risiken auf der Makroebene (z. B. wie gesellschaftlich-politische und wirtschaftliche Risiken) und überwiegend individuelle Risiken (z. B. Schamgefühl, Informationspermanenz und Entkontextualisierung; vgl. Drackert, 2014). Insbesondere das Internet als „weltweites Netzwerk" (Lehnard, 2020: S. 2) bzw. die „weltweite Vernetzung" (HBDI, 2021a: S. XXIV) besitzt ein Gefährdungspotenzial und stellt neue Herausforderungen für den Datenschutz dar. Vorkehrungen zum Datenschutz können u. a. auf rechtlicher Ebene (Datenschutzrecht) sowie auf technischer und organisatorischer Ebene (Datensicherheit) verortet werden.

Das **Datenschutzrecht** beschreibt die „Menge der Datenschutz-Rechtsnormen" (Pohle & Hölzel, 2020: S. 1), wobei beispielsweise die Datenschutz-Grundverordnung (DS-GVO) im Zuge der Verarbeitung personenbezogener Daten mit dem Ziel Anwendung findet, „die Grundrechte und Grundfreiheiten natürlicher Personen" zu schützen (Art. 1 Abs. 2 DS-GVO). Eine zentrale Problematik im Rahmen der Debatte um Datenschutz ist, dass in dieser in der Regel nicht vorangestellt wird, auf welche Schutzgüter Bezug genommen wird. Im Datenschutzrecht werden beispielsweise verschiedene Schutzgüter nebeneinandergestellt, beispielsweise finden sich in Artikeln und Erwägungsgründen zur DS-GVO u. a. benannt: „Menschenrechte und Grundfreiheiten" (Art. 45 Abs. 2 lit. a DS-GVO), „menschliche Würde, berechnigte Interessen und Grundrechte" (Art. 88 Abs. 2 DS-GVO), „Rechte und Freiheiten" (exemplarisch in Art. 5 Abs. 1 lit. e, Art. 10 DS-GVO) und „personenbezogene Daten" (Art. 50 Abs. 1 lit. b DS-GVO). Regelungstechnisch knüpfen das Datenschutzrecht sowie die DS-GVO jeweils bei Daten bzw. konkreter bei personenbezogenen Daten an.

**Personenbezogene Daten** sind gemäß Art. 4 Nr. 1 DS-GVO definiert als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ,betroffene Person') beziehen".<sup>2</sup> Im Schulkontext eröffnet bereits die Nutzung ei-

---

<sup>2</sup> Gem. Art. 4 Nr. 1 DS-GVO ist eine natürliche Person identifizierbar, wenn sie „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren

ner Lernplattform Einblicke in personale Aspekte (Fähigkeiten, Bewertungsdispositionen, Verhalten und Umstände). So können z. B. Namensangaben, personalisierte Profile, Angaben zur Schule wie Schulform, Schulname, Bundesland und Jahrgang, sowie Nutzungsdaten in Form von IP-Adresse, Daten bezogen auf Art und Umfang der Nutzung, Daten durch Verwendung von Social-Networks- oder Webanalyse-Diensten und pädagogische Prozessdaten erhoben werden (vgl. Nebel, 2021: S. 199 f.). Kritisiert werden kann jedoch, dass sich aus Daten ohne Personenbezug personenbezogene Daten bzw. Informationen ableiten lassen können (vgl. Steinebach, Krempel, Jung & Hoffmann, 2016: S. 441; vgl. Finck & Pallas, 2019). Zugespitzt lässt sich formulieren: „Es gibt keine neutrale (zweck- und benutzerunabhängige) Information“ (Steinmüller, 1971: S. 85).

Für den föderal geregelten Schulbereich in Deutschland sind mit Blick auf die Verarbeitung von Schüler\*innendaten von zentraler Bedeutung: das bundeslandspezifische Schulgesetz (gegebenenfalls mit weiteren Verordnungen), zudem das Landesdatenschutzgesetz und auch die DS-GVO (vgl. Hansen, 2021: S. 317). Letztgenannte enthält gem. Art. 5 DS-GVO Grundsätze für die Verarbeitung personenbezogener Daten: Eine solche muss auf rechtmäßige Weise, d. h. vorausgesetzt wird eine Rechtsgrundlage (vgl. Hansen, 2021: S. 316) nach Treu und Glauben und transparent, d. h. für die betroffene Person in einer nachvollziehbaren Weise erfolgen („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Der Grundsatz der Zweckbindung bedeutet, dass Daten gem. Art. 5 Abs. 1 lit. b DS-GVO nur „für zuvor festgelegte, eindeutige und legitime Zwecke erhoben“ oder weiterverarbeitet werden dürfen („Zweckbindung“). Datenminimierung im Sinne von Art. 5 Abs. 1 lit. c DS-GVO bedeutet, dass Daten für den nach Art. 5 Abs. 1 lit. b DS-GVO bestimmten Zweck angemessen und erheblich sein müssen („Datenminimierung“). Kann der Zweck auf andere Weise erfüllt werden, sind andere Mittel zu wählen. Zudem sollen die Daten richtig und in ihrer Speicherdauer begrenzt sein („Richtigkeit; Speicherbegrenzung“). Weiterhin ist die Einhaltung der Grundsätze Integrität und Vertraulichkeit zu gewährleisten, so sollen u. a. Unbefugte keinen Zugang zu den personenbezogenen Daten erhalten („Integrität und Vertraulichkeit“). Die DS-GVO stellt an die Verarbeitung personenbezogener Daten von Kindern, die im Sinne des Erwägungsgrundes 38 S. 1 DS-GVO besonderen Schutz verdienen, da sie „sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind“, punktuell besondere Anforderungen. Diese betreffen nach Roßnagel (2021) u. a. Einwilligungen von Kindern, Abwägungen mit ihren schutzwürdigen Interessen, Informationen für Kinder und Löschung ihrer personenbezogenen Daten gem. Art. 17 Abs. 1 DS-GVO.<sup>3</sup>

---

besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

<sup>3</sup> Problematisch ist in dem Kontext, dass der aktuell bestehende Schutz – insbesondere mit Blick auf automatisierte Entscheidungen (u. a. Profiling) und eine Nicht-Implementation des Erwägungsgrundes 71 in den Normtext der DS-GVO – nicht ausreicht bzw. „kein Gesamtkonzept eines Kinderdatenschutzes sichtbar“ wird (Roßnagel, 2021: S. 190).

Unter dem Begriff der **Datensicherheit** werden vor allem technische und organisatorische Schutzmaßnahmen diskutiert, um die Sicherheit der Datenverarbeitung zu gewährleisten. Die technisch-organisatorischen Maßnahmen reichen von Beachtung der Gefahren im technischen Umfeld (z. B. Gestaltung des Serverraums in der Schule) über Maßnahmen der IT-Sicherheit zur Verschlüsselung (z. B. bei Instant-Messenger-Diensten) bis hin zur Qualifikationsangeboten von Mitarbeiter\*innen (vgl. Lenhard, 2020). Datensicherheit betrifft die Verarbeitung aller Daten und ist nicht auf personenbezogene Daten beschränkt. Zugleich kann Datenschutz nicht ohne Datensicherheit realisiert werden (vgl. Lenhard, 2020: S. 3) und ist eine Anforderung an eine rechtmäßige Verarbeitung personenbezogener Daten. In der DS-GVO findet diese Anforderung mit Nennung der Grundsätze Vertraulichkeit, Integrität und Verfügbarkeit Erwähnung (vgl. Hansen, 2021; vgl. Art. 32 DS-GVO). Die (Design-)Ziele und Anforderungen durch die Datensicherheit und Datenschutz an Informationssysteme können sich auch entgegenstehen, da beispielsweise Anonymität Vertraulichkeit ermöglichen und gefährden kann.<sup>4</sup>

Der Begriff **Privatsphäre** wurde im Zuge von Eingriffen in allgemeine Persönlichkeitsrechte vom Bundesverfassungsgericht im Rahmen der Sphärentheorie verwendet und wird dabei abgegrenzt von der Intim- bzw. der Sozialsphäre (vgl. Nebel, 2020: S. 41). Durch das sog. Volkszählungsurteil 1983 wurde mit dem Recht auf informationelle Selbstbestimmung eine Abkehr von der von außen definierten „Sphäre“ gewählt: Schutzgut ist seitdem die Selbstbestimmung des Einzelnen bzw. die „Befugnis des Einzelnen, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“ (BVerfGE 65, 1 (42)). Das Grundrecht auf informationelle Selbstbestimmung wird im Grundgesetz (GG) nicht genannt, sondern durch das Bundesverfassungsgericht (BVerfG) in ständiger Rechtsprechung aus Art. 2 Abs. 1 i. V. m. Art 1 Abs. 1 GG abgeleitet und ist – ebenso wie das Recht am eigenen Bild, das Recht am eigenen Namen und das Recht am eigenen Wort – vom Schutzzumfang des allgemeinen Persönlichkeitsrechts gedeckt. Es kann an dieser Stelle festgehalten werden, dass zwischen dem Schutz der Privatsphäre und dem Datenschutz zu differenzieren ist, auch wenn Überschneidungen existieren (vgl. Kokott & Sobotta, 2013).

#### 4. Datenschutz in der Schulpraxis: Herausforderungen und Spannungsfelder

Wie bereits skizziert, zeigen sich Herausforderungen und Spannungsfelder bei Realisierung des Datenschutzes in der Unterrichts- und Schulentwicklung (z. B. Kammerl et al., 2016; Gerick et al., 2019; Gerick & Eickelmann, 2020; Rau et al., 2021; Reichwein, 2021). Diese Herausforderungen und Spannungsfelder für Lehrpersonen werden im Folgenden

---

<sup>4</sup> Von Lewinski (2014) verweist darauf, dass Datensicherheit, verstanden als Schutz von Daten, zu „vollmundige Versprechungen v.a. u.s.-amerikanischer Internet-Unternehmen zum Datenschutz“ geführt habe, da Interessen von Betroffenen und Verarbeitern an Datensicherheit „eher deckungsgleich sind“ (von Lewinski, 2014: S. 4 f.). Datenschutz und Datensicherheit sind aber mitnichten gleichzusetzen.

vertiefend betrachtet und diskutiert, um potenzielle Gestaltungsmöglichkeiten für die Lehrer\*innenbildung zu identifizieren.

#### 4.1 Zwischen Lebenswelt, Medienkompetenz und Datenschutz

Lehrpersonen sollen sich „mit der von Digitalisierung und Mediatisierung gekennzeichneten Lebenswelt und den daraus resultierenden Lernvoraussetzungen“ (KMK, 2017: S. 25) ihrer Lernenden auseinandersetzen und zur Medienkompetenzentwicklung beitragen. Die Daten der JIM-Studie zeigen, dass die Lebenswelt der Lernenden heutzutage geprägt ist von digitalen Geräten und Medien. 94% der befragten Jugendlichen besitzen ein Smartphone und neun von zehn Jugendlichen nutzen täglich das Internet in ihrer Freizeit (MPFS, 2020: S. 8, 14). Anknüpfend an die Forderung der KMK lassen sich Gründe identifizieren, lebensweltlich verankerte Apps von Jugendlichen im Unterricht zu thematisieren und einzusetzen (Rummler, Müller, Kamin, Richter, Kammerl, Potzel, Grabensteiner & Schneider Stingelin, 2021) sowie den Ansatz „Bring Your Own Device“ (BYOD) zur Ergänzung der schulischen Infrastruktur zu nutzen (Döbeli Honegger, 2017: S. 121 ff.). Als eine solche Möglichkeit sehen Rummler et al. (2021) aus einer medienpädagogischen Perspektive die Nutzung von „Instant-Messenger-Kommunikation als Ressource für die Bewältigung von schulischen Aufgaben“ in einer durch digitale Medien (mit-)geprägten häuslichen und schulischen Lernumgebung (Rummler et al., 2021: S. 80). Auf Basis verschiedener Projekte skizzieren sie ein pädagogisches Potenzial von Instant-Messenger-Diensten „zur Optimierung des Lernprozesses und insbesondere der Selbstorganisationsfunktion im Sinne einer explorativen und selbstgesteuerten Gestaltung von Lern- und Kommunikationsprozessen“ (ebd.). Diese Möglichkeiten bleiben nach Rummler et al. (2021) jedoch in der schulischen Praxis weitestgehend unausgeschöpft.

Bei den von Rummler et al. (2021) skizzierten Projekten sowie bei BYOD-Ansätzen im Allgemeinen werden private mobile Endgeräte Teil der schulisch genutzten IT-Infrastruktur. Die Nutzung der Geräte der Lernenden haben dabei sowohl didaktische, finanzielle als auch technisch-organisatorische Implikationen. Dadurch bewegen sich Schulen bzw. Lehrpersonen bei der Thematisierung und Nutzung der Geräte der Lernenden zwischen zwei unterschiedlichen Zielperspektiven. Während die Nutzung eigener Geräte und eigener Apps im Unterricht einerseits zur Medienkompetenzentwicklung der Jugendlichen beitragen kann, stellen sich verschiedene Fragen zum Schutz vor Datenverarbeitungsprozessen entsprechender Apps. Eine durchaus umstrittene Frage lautet, inwiefern die sogenannte „verantwortliche Stelle“ nach Art. 4 Nr. 7 DS-GVO auch dann für die ordnungsgemäße Verarbeitung von personenbezogenen Daten verantwortlich ist, wenn die Verarbeitung auf privaten Endgeräten der Lehrer\*innen bzw. Schüler\*innen stattfindet (vgl. LDI NRW, 2021: S. 8). Private Anwendungen auf Endgeräten können ggf. Zugriff auf Daten, welche zu schulischen Zwecken erhoben wurden, erlangen und so personenbeziehbare Daten an Dritte weitergeben (z. B. durch umfangreiche Freigabe von App-Berechtigungen). Aber anders als bei schuleigenen Geräten hat die Schule nur berechtigter-

weise eingeschränkte Möglichkeiten, technische und organisatorische Vorgaben hinsichtlich der sicheren Datenverarbeitung auf privaten Endgeräten zu treffen und durchzusetzen.

In diesem Zusammenhang werden kaum lösbare Spannungsfelder sichtbar, weil die verschiedenen Zielperspektiven nicht vereinbar sind. Für die Schaffung eines sicheren bzw. datenschutzkonformen digitalen Raumes sind viele lebensweltlich relevante Apps der Lernenden nicht geeignet. Es erscheint in diesem Zusammenhang nachvollziehbar, dass sich Lehrpersonen gegen die Nutzung eigener Geräte im Unterricht einsetzen bzw. spezifische Apps nicht nutzen. In den von Rummler et al. (2021) beschriebenen Projekten wird dies u. a. daran deutlich, dass sich Lehrer\*innen explizit gegen „Klassenchats aussprechen“ (vgl. Rummler et al., 2021: S. 80). Eine entsprechende Umgangsweise führt jedoch dazu, dass Lehrpersonen dem Anspruch, an die Lebenswelt der Jugendlichen anzuknüpfen und ihr Medienhandeln gemeinsam zu reflektieren, kaum gerecht werden können. Die in der JIM-Studie 2020 (MPFS, 2020: S. 38) benannten wichtigsten Apps der Lernenden sind aus der Perspektive des Datenschutzes zu kritisieren. Durch die Nicht-Thematisierung der eigenen Apps werden Lernende mit diesem Problem alleingelassen bzw. kann festgestellt werden, dass es nicht als schulisches Problem wahrgenommen wird.

## 4.2 Herausforderungen zur Gestaltung sicherer Lernumgebungen

Zur Unterrichtsentwicklung sollten Lehrer\*innen systematisch digitale Medien bzw. digitale Lernumgebungen einsetzen und durch Wissen über Datenschutz und Datensicherheit einen sicheren digitalen Raum für Schüler\*innen gestalten können (vgl. KMK, 2017: S. 27 f.). Wie bereits im vorherigen Kontext gezeigt wurde, können sich diese Zielperspektiven widersprechen und sind in der Realisierung keinesfalls trivial. In verschiedenen Modellschulprojekten der letzten Jahre beschreiben Lehrpersonen die datenschutzkonforme Auswahl digitaler Anwendungen als herausfordernd bzw. überfordernd (vgl. Rau et al., 2021; vgl. Kammerl et al., 2016; vgl. Gerrick & Eickelmann, 2020).

Die mit diesen Anforderungen verbundenen Schwierigkeiten lassen sich exemplarisch am Beispiel der Plattform „Padlet“ konkretisieren. Die von einem US-Unternehmen betriebene Plattform „Padlet“ stellt Funktionen zur synchronen Kollaboration in Form einer digitalen Pinnwand bereit. Auf der digitalen Pinnwand können Texte, Bilder, Videos, Links, Sprachaufnahmen, Bildschirmaufnahmen und Zeichnungen abgelegt werden. Eine Nutzung ist ausschließlich über einen Browser wie auch über Apps für Tablets und Smartphones mit einem Internet-Zugang möglich. „Padlet“ wurde auf verschiedene Weise didaktisch in Unterrichtssettings eingebunden: von der Bereitstellung multimedialer Ressourcen bis zur Einbindung der Lernenden in Form eigener multimedialer Beiträge (z. B. Anders, 2020; Robert Bosch Stiftung & Die Deutsche Schulakademie, 2020; ebd., 2021).

Fragen zur Realisierung des Datenschutzes werden – blendet man die Debatte um den Datentransfer in Drittländer nach dem "Schrems II"-Urteil erstmal aus – insbesondere bei der interaktiven Nutzung relevant. Wird die Plattform „Padlet“ ausschließlich über das schulische WLAN auf schulischen Endgeräten genutzt, ohne einen persönlichen Ac-

count auf dem Endgerät für die jeweilige Schüler\*in anzulegen oder gleichzeitig an anderen Online-Plattformen bzw. -diensten eingeloggt zu sein, können die Daten laut Einschätzung des HBDI (2021b) technisch keiner Person zugeordnet werden. Wenn kein Personenbezug bei den Daten vorliegt, ist der sachliche Anwendungsbereich der DS-GVO nicht gegeben. Wie bereits in der Begriffsdiskussion skizziert, wird der Personenbezug durchaus kritisch gesehen. Ungeklärt ist bei „Padlet“ hingegen, welche Daten vom Plattformbetreibenden erhoben werden, wenn mit einem schulischen Endgerät über den privaten Internetanschluss auf „Padlet“ zugegriffen wird. Sobald Schüler\*innen, Lehrpersonen oder Eltern ihre privaten Endgeräte einsetzen, sind sie möglicherweise als Personen identifizierbar, weil durch den Plattformbetreibenden Cookies und Trackingmechanismen zur Erbringung des Dienstes eingesetzt werden, welche auf Personen beziehbare technische Informationen (z. B. IP-Adresse, Browsertyp, Betriebssystemtyp, Bewegungsprofile etc.) verarbeiten könnten (vgl. Ruhestroth & Baulig, 2020; vgl. Thiede, 2021). Die genauen Inhalte dieser Daten sind dabei bislang weitgehend unbekannt. Auch die Datenschutzbestimmungen, die der Plattform zugrunde liegen, entsprechen nicht den Vorgaben der DS-GVO, u. a. da diese in ihren Angaben unpräzise sind (vgl. Thiede, 2021; vgl. HBDI, 2021b). Entsprechend bleiben zentrale Fragen offen und die tatsächliche Einhaltung der vertraglichen Zusagen im „Data Processing Addendum“ schwierig überprüfbar. Zugleich ist anzumerken, dass eine Prüfung der allgemeinen Geschäftsbedingungen sowie der Datenschutzbestimmungen aufgrund möglicher Aktualisierungen nur zeitlich eingeschränkt gültig ist. Unter Berücksichtigung der Debatte um den Datentransfer in Drittländer betreffen Fragen zur Realisierung des Datenschutzes bei der Verwendung von „Padlet“ letztlich die Problematiken der Datenübertragungen in ein Drittland und die Einbindung von Drittanbietern:

Die Plattform Padlet wird von einem US-Unternehmen betrieben. Da in den Vereinigten Staaten die Datenschutz-Grundverordnung (DS-GVO) nicht gilt, können personenbeziehbare Daten durch das Unternehmen selbst oder Drittanbieter gespeichert und verarbeitet werden. Das können neben den geteilten Inhalten auch die IP-Adressen der Nutzer\*Innen sein oder auch Bewegungsprofile, da Padlet bei der Benutzung Daten mit Drittanbietern wie z. B. Google teilt (HBDI, 2021b, c).

Der von der KMK geforderte systematische Einsatz digitaler Medien bedeutet in diesem Zusammenhang auch eine regelmäßige Prüfung der Datenverarbeitungsprozesse entsprechender digitaler Medien. Am Beispiel von Padlet zeigte sich im Rahmen der pandemiebedingten Schulschließungen auch, dass unterschiedliche Institutionen hinsichtlich des Umgangs mit Datenschutzfragen durchaus unterschiedliche Empfehlungen geben. Beispielsweise unterscheiden sich die Empfehlungen vom Hessischen Kultusministeriums (HKM) und des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) hinsichtlich der Nutzung bzw. Duldung für den Übergang (Vorabinformation des HKM vom 05.02.2021; HBDI, 2021b; HBDI, 2021c) und den darauf bezogenen Reaktionen (Untersagung der Nutzung mit sofortiger Wirkung) von denen einzelner staatlicher Schulämter. Anstatt konsistente Rahmenvorgaben für eine einzelne Anwendung zu bieten, dokumentieren die unterschiedlichen Empfehlungen vielmehr die Komplexität der Aufgabe.

Die Ausführungen veranschaulichen, dass die von der KMK geforderte Kompetenz von Lehrpersonen, digital sichere Umgebungen gestalten zu können, an Voraussetzungen und konkreten Rahmenbedingungen geknüpft ist. Aufgrund der Abhängigkeit vom jeweiligen Einsatzszenario sowie der zeitlich befristeten Gültigkeit einer Einschätzung lässt sich zudem erahnen, dass die Auseinandersetzung mit Fragen des Datenschutzes nicht einmal abgearbeitet werden kann, sondern eine regelmäßige Aufgabe darstellt. Jenseits der formulierten Leitbilder zeigt die Praxis, dass die begründete Einschätzung und Auswahl von datenschutzkonformen digitalen Anwendungen zur Interaktion mit Schüler\*innen für Lehrpersonen eine zentrale Herausforderung darstellt (vgl. Gerick & Eickelmann, 2020; vgl. Reichwein, 2021). Am Beispiel der unterschiedlichen Empfehlungen zeigt sich zudem, dass die Herausforderungen zur Ermöglichung eines Datenschutzes in der Schule auch die äußere Schulentwicklung betreffen. Die vielfältigen Schwierigkeiten, mit der Offenheit und Unbestimmtheit verschiedenen Datenpraktiken als Lehrpersonen angemessen umgehen zu können, werden in bestehenden Leitbildern bisher kaum aufgegriffen.

### 4.3 Schulische Datenschutzbeauftragte mit geringen Ressourcen

Verantwortliche und Auftragsverarbeiter\*innen sind gem. Art. 37 DS-GVO angehalten, eine\*n Datenschutzbeauftragte\*n und Vertreter\*innen zu benennen – für hessische öffentliche Schulen ergibt sich diesbezüglich eine Verpflichtung aus § 11 der Verordnung zur Verarbeitung personenbezogener Daten an Schulen sowie aus § 5 des Hessischen Datenschutz- und Informationsfreiheitsgesetz (HDSIG). Zentrale Aufgaben des\*der schulischen Datenschutzbeauftragten (schDSB) sind Unterrichtung und Beratung von Verantwortlichen, Auftragsverarbeiter\*innen und Beschäftigten, die Verarbeitungen durchführen, auf Anfrage Beratung der Schulleitung mit Blick auf Datenschutzfolgeabschätzungen (DSFA), Sensibilisierung und Schulung der Verantwortlichen und Auftragsverarbeiter\*innen, Zusammenarbeit mit der Aufsichtsbehörde und Überwachung der Einhaltung des Datenschutzrechts und der Datenschutz-Strategie der Schule. Die schDSB sind für die skizzierten Aufgabenbereiche zum Datenschutz (zumindest theoretisch) nicht weisungsgebunden (Art. 38 Abs. 3 DS-GVO). In Hessen informiert der HBDI, die Schulleitung habe „zu gewährleisten, dass der schDSB ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängender Fragen eingebunden wird. Dies gilt insbesondere bei der Einführung neuer Software an der Schule, mit der personenbezogene Daten verarbeitet werden“ (HBDI, o. J.). In der Praxis gestaltet sich die Erfüllung der benannten Aufgaben und die Umsetzung als höchst schwierig, was nicht nur an der Zunahme der Risiken für die Grundrechte, für die sich schDSB einsetzen sollen, oder an bestimmten Entwicklungen (z. B. Gestaltung zeitgemäßer Bildung), die im Schulleben ankommen und umzusetzen sind, liegt. Die schDSB stehen partiell vor ähnlichen Herausforderungen, wie sie auch von Landesbeauftragten für Datenschutz skizziert werden.

Im Rahmen der Arbeit mit Modellschulen zeigt sich, dass Lehrpersonen – sofern Schulleitungen darum bemüht sind, einen schDSB zu benennen – nicht notwendigerweise

über die erforderliche Qualifikation insbesondere Fachwissen auf dem Gebiet des Datenschutzrechtes und der Datenschutzpraxis verfügen. Die A29WP-Fachgruppe (2017) benennt diesbezüglich:

Fachkompetenz auf dem Gebiet des nationalen und europäischen Datenschutzrechts und der Datenschutzpraxis, einschließlich eines umfassenden Verständnisses der DS-GVO, Verständnis der jeweils durchgeführten Verarbeitungsvorgänge, Kenntnisse in den Bereichen IT und Datensicherheit, Kenntnis der jeweiligen Branche und Einrichtung, die Fähigkeit, eine Datenschutzkultur innerhalb der Einrichtung zu fördern (A29WP-Fachgruppe, 2017: 27).

Zeitliche Ressourcen sind nicht nur mit Blick auf die Erfüllung der benannten Aufgaben nicht vorhanden, sondern fehlen schon vorab bei der Vorbereitung auf und Einarbeitung in diese. So heißt es auch an anderer Stelle: „Datenschutzbeauftragte: Die Lehrkraft, die durch die Schulleitung zur bzw. zum Datenschutzbeauftragten bestellt ist, erhält nach Bestellung genau eine Anrechnungsstunde für die Ausübung dieser Tätigkeit“ (Realschule, BayMBL 2019 Nr. 141). Ferner konstatiert beispielsweise die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI):

Zum anderen aber sind Schulen mit diesen Prüfungen regelmäßig komplett überfordert, weil es hier nicht um eine rein pädagogische Beurteilung digitaler Lehrmittel geht, sondern weit darüber hinaus um die Prüfung und Bewertung höchst komplexer rechtlicher und technischer Sachverhalte, für die Lehrkräfte normalerweise nicht ausgebildet sind und wofür sie auch nicht über die notwendigen zeitlichen Ressourcen verfügen. (BlnBDI, 2021b: S. 1 f.)

Der Schulleitung obliegt als Behördenleitung die Verantwortung für die Einhaltung des Datenschutzes und zur Sicherstellung geeigneter und organisatorischer Maßnahmen. In diesem Zusammenhang lässt sich mit Schulz (2021) darauf hinweisen, dass die Unabhängigkeit der schDSB bestehe, aber eine Rollendiffusion existiere: So sei eine Lehrperson gegenüber der Schulleitung zugleich unabhängig in ihrer Funktion als schDSB und weisungsgebunden in ihrer Funktion als Lehrkraft (vgl. Schulz, 2021: S. 290). Fraglich ist ferner, ob aufgrund der komplexen Herausforderungen, eine Berufung externer schDSB tatsächlich eine Lösung darstellt. Bei der Berufung eines externen schDSB besteht die Gefahr, dass diese Person nicht genügend Einblick in tatsächliche schulische Abläufe und Organisationsstrukturen erhält, auch wenn dadurch zumindest ein innerschulisches Problem gelöst werden könnte. Eine Entschärfung des Ressourcenproblems durch eine zeitgleiche Zuständigkeit für mehrere Schulen oder den Einsatz externer schDSB kann an dieser Stelle nicht erkannt werden.

Anknüpfend an die Ausführungen zu zentralen Herausforderungen auf der Ebene der Unterrichtsgestaltung (Kap. 4.2) veranschaulicht die Darstellung, dass die vielfältigen Aufgaben, welche schulischen Datenschutzbeauftragten obliegen auf Basis völlig unzureichender zeitlicher Ressourcen und fehlender Qualifizierungsangebote nicht in einzelnen Verantwortlichkeiten hinreichend bearbeitet werden können. Für die Schaffung eines datenschutzkonformen digitalen Raums ist es unter den aktuellen Rahmenbedingungen erforderlich, dass alle Lehrpersonen über notwendiges Fachwissen auf dem Gebiet des



Datenschutzrechtliches und der Datenschutzpraxis verfügen sowie Handlungskompetenzen entwickeln können, um digital sichere Umgebungen zu gestalten.

## 5. Datenschutz als Aufgabe für die Lehrer\*innenbildung

Datenschutz ist ein Bestandteil aktueller Leitbilder zur Bildung in einer digital geprägten Welt. Diese Position ist im bildungspolitischen Diskurs unstrittig und als Absichtserklärung in diversen Dokumenten sichtbar (vgl. KMK, 2012, 2017; vgl. Bundesregierung, 2021). Mit diesen Leitbildern werden komplexe Aufgaben und Anforderungen an Lehrpersonen gerichtet. Aufgrund der Dynamik technischer und rechtlicher Entwicklungen können diese als voraussetzungsvoll und zeitintensiv beschrieben werden. Zudem sind Lehrer\*innen in der aktuellen schulischen Praxis mit konkurrierenden Leitbildern konfrontiert. Um Lehrpersonen einen souveränen Umgang mit diesen komplexen und partiell unbestimmten Situationen zu ermöglichen, muss sich die Lehrer\*innenbildung dem Thema Digitale Bildung und Datenschutz aktiver stellen.

Ein erster Beitrag zur Sensibilisierung für Fragen einer Digitalen Bildung und des Datenschutzes als Unterrichtsgegenstand und Gestaltungsmerkmal digitaler Lernumgebungen eröffnet eine kritische Auseinandersetzung mit unserer Sprache über digitale Medien.<sup>5</sup> In vielfältigen bildungsrelevanten Diskursen werden digitale Medien vor allem als Werkzeuge, Hilfsmittel und Tools metaphorisiert (z. B. KMK, 2017). Auch bei Lehramtsstudierenden ist die Beschreibung von digitalen Medien als Werkzeuge bzw. Hilfsmittel eine verbreitete Metapher (vgl. Rau & Kosubski, 2019). Das Problem dieser Metapher besteht darin, dass komplexe Datenverarbeitungsprozesse ausgeblendet werden.<sup>6</sup> Gemäß der KMK (2017) sollen Lernende beispielsweise die Kompetenz entwickeln, „Digitale Werkzeuge bei der gemeinsamen Erarbeitung von Dokumenten [zu] nutzen“ (KMK, 2017: S. 16). Im Fokus dieser Beschreibung steht die Fähigkeit, mit digitalen Medien kollaborative Texte zu schreiben. Kollaborative „Schreibwerkzeuge“ lassen sich jedoch zugleich als Informationssysteme verstehen, da die Erhebung, Verarbeitung und Speicherung von (personenbezogenen) Daten gemeinsame Schreibprojekte technisch erst möglich machen. Während der Begriff des Informationssystems auf Informations- und Datenverarbeitungsprozesse hinweist, rücken Datenverarbeitungsprozesse beim Werkzeugbegriff in den Hintergrund. Die Problematik des Werkzeugbegriffs für das Handlungsfeld Schule wurde von Kraut (2012) bereits im Kontext der Web 2.0 Debatte markiert. Neben der Ausblendung von Datenverarbeitungsprozessen ist der Werkzeugbegriff nicht hilfreich,

---

<sup>5</sup> Sprache und Metaphern können einen Zugang zu (individuellen und kollektiven) Orientierungen eröffnen (vgl. Schmitt, 2017) und rahmen zugleich die Möglichkeiten, in denen wir in konkreten Situationen sprechen, denken und handeln können (vgl. Lakoff & Johnson, 2014; vgl. Schmitt, 2017).

<sup>6</sup> In einer alltagsnahen Deutung des Begriffs kann ein Werkzeug als ein konkretes Objekt oder Gerät verstanden werden, das für die Bearbeitung eines spezifischen Problems zweckdienlich ist. Ein Schraubendreher erfüllt beispielsweise den Zweck, Schrauben in ein Material hinein- bzw. herauszudrehen. Übertragen auf digitale Medien werden mit dem Werkzeugbegriff häufig konkrete Zielsetzungen an die Nutzung digitaler Medien geknüpft.

um auf Fragen zu allgemeinen Geschäftsbedingungen und Lizenzfragen aufmerksam zu machen (vgl. Kraut, 2012). Auf individueller Ebene bietet die Auseinandersetzung mit entsprechenden Sprachphänomenen und Metaphern das Potenzial, zur Erweiterung der eigenen Ausdrucks- und Reflexionsmöglichkeiten beizutragen (vgl. Gropengießer, 2004: S. 22). Neben den Potenzialen für individuelle Entwicklungsprozesse von Personen in der Lehrer\*innenbildung und (angehenden) Lehrer\*innen kann eine entsprechende begriffliche Vielfalt auch dazu beitragen, dass Fragen der Digitalen Bildung nicht auf die Betrachtung von digitalen Medien als neue Werkzeuge und technische Geräte verkürzt werden.

Die Perspektive, dass sich Schule und explizit die Lehrer\*innenbildung mit Fragen der Digitalisierung auseinandersetzen müssen, ist nicht neu (vgl. Arbeitsgruppe Erziehungswissenschaft, 1997). Zugleich zeigt sich auch in der Betrachtung der letzten zehn Jahre, dass medienpädagogische Themen und Module, die Digitalisierungs- und Mediatisierungsprozesse umfassen, nur in Ansätzen verankert sind (vgl. Kammerl & Mayrberger, 2011; vgl. Ackeren, Aufenanger, Eickelmann, Friedrich, Kammerl, Knopf, Mayrberger, Scheika, Scheiter & Schiefner-Rohs, 2019). Mit Blick auf Fragen des Datenschutzes innerhalb der Schule und unbestimmte Datenpraktiken außerhalb der Schule offenbaren sich weitere Leerstellen auf bildungsorganisatorischer Ebene. Wenngleich das Thema ‚Datenschutz‘ zumindest in Kompetenzdimensionen der „Standards für die Lehrerbildung: Bildungswissenschaften“ (vgl. KMK, 2019b) benannt wird, ist der Begriff „Datenschutz“ in den Anforderungen an die Fachwissenschaften und Fachdidaktiken lediglich bei drei Fächern verankert (KMK, 2019a). Datenschutz im Kontext der Digitalisierung ist insofern bisher kein fächerintergratives Thema in der Lehrer\*innenbildung. Anknüpfend an die Argumentation von Livingstone, Stoilova und Nandagiri (2021) stellt sich die Frage, wie Schulen Datenschutz als Unterrichtsthema etablieren und Lehrkräfte ihrer Vermittlungsaufgabe gerecht werden sollen, wenn sie mit dem Thema im Rahmen der Lehrer\*innenbildung nicht konfrontiert werden.

Auch in der theoretischen Diskussion zur Modellierung entsprechender Kompetenzen wird der Handlungsbedarf sichtbar. Lorenz und Endberg (2019) markieren in vergleichender Betrachtung unterschiedlicher medienpädagogischer Kompetenzmodelle, dass „rechtliche Fragestellungen rund um Datenschutz und Urheberrecht [...] unberücksichtigt bleiben“ (Lorenz & Endberg, 2019: S. 76). Die Relevanz zur Diskussion der übergreifenden Frage, wie „data literacy“ modelliert werden kann bzw. welche (medienpädagogischen) Kompetenzen in einer datengetriebenen Medienlandschaft benötigt werden, wird auch international betont (vgl. Audenhove et al. 2020). Während sich der Einsatz von datenbasierter Lernsoftware international verbreitet, existiert zugleich eine Forschungslücke zur Analyse ethischer Fragen und sozialer Implikationen bei der Verwendung entsprechend generierter Daten bei Kindern im (Vor-)Schulalter (Hakimi, Eynon & Murphy, 2021). Diese Erkenntnisse sind zugleich notwendig, um eine fundierte Kompetenzmodellierung einer „data literacy“ für Lehrpersonen überhaupt entwickeln zu können. Hier werden nicht nur Potenziale, sondern zentrale Aufgabenbereiche sichtbar, um Datenschutz als Facette von Medienkompetenz bzw. Datenkompetenz in einer digital geprägten Welt wissenschaftlich sowie bildungspraktisch in den Blick zu nehmen.

Neben der Erweiterung individueller Kompetenzen zum Datenschutz im Spezifischen und aktueller Datenpraktiken im Allgemeinen, darf das Thema Datenschutz nicht auf den Selbstschutz beschränkt bleiben. Zur strukturellen Verankerung von Datenschutz in Bildungseinrichtungen in einer digital geprägten Welt und der Ermöglichung einer Digitalen Bildung bedarf es mehr zeitlicher und finanzieller Ressourcen. Dies betrifft den systematischen Aufbau technischer Infrastruktur und den Ausbau von Stellen, die zum Datenschutz und zum Recht auf informationelle Selbstbestimmung beratend tätig sind (z. B. Institutionen wie die Aufsichtsbehörden der Länder). Über die Beschaffung von Endgeräten hinaus müssen insbesondere Lösungen entwickelt werden, um datenschutzkonforme Lehr-Lernplattformen und Webdienste als OpenSource-Lösungen in sämtlichen Institutionen entlang der Lehrer\*innenbildungskette von den jeweiligen Bundesländern systematisch anzubieten. Das Netzwerk „Freie Schulsoftware“ zeigt bereits Möglichkeiten und Ansprechpersonen, um offene und freie Software zum Schutz von Daten und Grundrechten für alle beteiligten Personen im Schulkontext zu nutzen.<sup>7</sup> Über Einzelinitiativen hinaus bedarf es jedoch systematischen Wissens über Datenschutz bei Personen der inneren und äußeren Schulentwicklung, um die Relevanz einer verantwortungsvollen und datenschutzkonformen schulischen Infrastrukturentwicklung zu kennen, einschätzen und mitgestalten zu können. Lehrer\*innenbildung kann durch die Reflexion und Entwicklung der eigenen Praxis dazu einen relevanten Beitrag leisten.

## Literatur

- Artikel-29-Datenschutzgruppe (A29WP-Fachgruppe). (2016). Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“). <[https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/wp243rev01\\_de.pdf](https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/wp243rev01_de.pdf)> (zuletzt aufgerufen am 12.11.21).
- Ackeren, Isabell van; Aufenanger, Stefan; Eickelmann, Birgit; Friedrich, Steffen; Kammerl, Rudolf; Knopf, Julia; Mayrberger, Kerstin; Scheika, Heike; Scheiter, Katharina & Schiefner-Rohs, Mandy (2019). Digitalisierung in der Lehrerbildung. Herausforderungen, Entwicklungsfelder und Förderung von Gesamtkonzepten. In *Die deutsche Schule*, 111(1), S. 103–119.
- Anders, Florentine (2020). Digitale Beziehungsarbeit in der Primarstufe. *Das Deutsche Schulportal*, 22. September 2020 <<https://deutsches-schulportal.de/unterricht/digitale-beziehungsarbeit-in-der-primarstufe>> (zuletzt aufgerufen am 12.11.2021).
- Audenhove, Leo van; Broeck, Wendy van den; & Mariën, Ilse (2020). Data literacy and education: Introduction and the challenges for our field. In *Journal of Media Literacy Education*, 12(3), S. 1-5.
- Bayerische Staatskanzlei (Hg.) (2019). Bayerisches Ministerialblatt 2019 Nr. 14 (BayMBL). Unterrichtspflichtzeit, Stundenermächtigungen und Anrechnungstunden der Lehr-

---

<sup>7</sup> Das „Netzwerk Freie Schulsoftware – Schulen helfen Schulen“ ist eine Initiative des Vereins „digitalcourage e.V.“ und ermöglicht einen Austausch zu Fragen offener und freier Software: <https://digitalcourage.de/netzwerk-freie-schulsoftware>

- kräfte an staatlichen Realschulen. Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus. <<https://www.verkuendung-bayern.de/files/baymbl/2019/141/baymbl-2019-141.pdf>> (zuletzt aufgerufen am 12.11.2021).
- Berliner Beauftragte für Datenschutz und Informationssicherheit (BInBDI) (2021a). Datenschutz und Informationsfreiheit. Jahresbericht 2020. <[https://www.datenschutz-berlin.de/fileadmin/user\\_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2020-Web.pdf](https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2020-Web.pdf)> (zuletzt aufgerufen am 12.11.2021).
- (2021b). Digitaler Unterricht—Misstände müssen so schnell wie möglich behoben werden. <[https://www.datenschutz-berlin.de/fileadmin/user\\_upload/pdf/pressemitteilungen/2021/20210122-PM-Digitaler Unterricht Misstaende beheben.pdf](https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210122-PM-Digitaler_Unterricht_Misstaende_beheben.pdf)> (zuletzt aufgerufen am 12.11.2021).
- Bundeskanzleramt (Hg.) (2021). Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum. <<https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632>> (zitiert als Bundesregierung (2021), zuletzt aufgerufen am 12.11.2021).
- Bundesministerium für Bildung und Forschung (BMBF) (2016). Bildungsoffensive für die digitale Wissensgesellschaft. Strategie des Bundesministeriums für Bildung und Forschung. <[https://www.kmk.org/fileadmin/pdf/Themen/Digitale-Welt/Bildungsoffensive fuer die digitale Wissensgesellschaft.pdf](https://www.kmk.org/fileadmin/pdf/Themen/Digitale-Welt/Bildungsoffensive_fuer_die_digitale_Wissensgesellschaft.pdf)> (zuletzt aufgerufen am 12.11.2021).
- Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) (2013). Medienkompetenzförderung für Kinder und Jugendliche. Eine Bestandsaufnahme. <<http://docplayer.org/8007329-Medienkompetenzfoerderung-fuer-kinder-und-jugendliche-eine-bestandsaufnahme.html>> (zuletzt aufgerufen am 12.11.2021).
- Bundesverfassungsgericht (BVerfG) (1983). Volkszählungsurteil, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 15. Dezember 1983. <[https://www.bundesverfassungsgericht.de/Shared\\_Docs/Downloads/DE/1983/12/rs19831215\\_1bvr020983.pdf?blob=publicationFile&v=1](https://www.bundesverfassungsgericht.de/Shared_Docs/Downloads/DE/1983/12/rs19831215_1bvr020983.pdf?blob=publicationFile&v=1)> (zuletzt aufgerufen am 12.11.2021).
- Dehnert, Henning; Glahe, Annika; Kunze, Sina-Marie & Schulze, Ulrike (2019). Ein Jahr DSGVO in Schulen. In *Recht der Jugend und des Bildungswesens* 67(3), S. 292-297. <<https://doi.org/10.5771/0034-1312-2019-3>>.
- Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. (HBDI) (o. J.). Hinweise zum schulischen Datenschutzbeauftragten nach Art. 37-39 DS-GVO“. <<https://datenschutz.hessen.de/hinweise-zum-schulischen-datenschutzbeauftragten-nach-art-37-39-ds-gvo>> (zuletzt aufgerufen am 18.11.2021).
- (2021a). Neunundvierzigster Tätigkeitsbericht zum Datenschutz und Dritter Tätigkeitsbericht zur Informationsfreiheit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit Professor Dr. Michael Ronellenfitsch, vorgelegt zum 31. Dezember 2020 <<https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files>

- [/HBDI\\_49\\_Ta%CC%88tigkeitsbericht\\_2020.pdf](#)> (zuletzt aufgerufen am 18.11.2021).
- (2021b, Februar 1). Kein ausreichender Datenschutz bei der Nutzung von Padlet. <<https://web.archive.org/web/20210201182138/https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/kein-ausreichender-datenschutz-bei-der-nutzung-von>> (zuletzt aufgerufen am 18.11.2021).
- (2021c, Februar 8). Kein ausreichender Datenschutz bei der Nutzung von Padlet. <<https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/kein-ausreichender-datenschutz-bei-der-nutzung-von>> (zuletzt aufgerufen am 18.11.2021).
- Deutscher Bundestag (2011). Zweiter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft“ Medienkompetenz, BT-Drs. 17/7286. <<https://dserver.bundestag.de/btd/17/072/1707286.pdf>> (zuletzt aufgerufen am 12.11.2021).
- Döbeli Honegger, Beat (2020). Warum sich der Covid-19-Notfallfernunterricht nicht als Diskussionsgrundlage für zeitgemässe Bildung in einer Kultur der Digitalität eignet. Pädagogische Hochschule Schwyz: Goldau. <<https://www.lernentrotzcorona.ch/pub/Lernentrotzcorona/VorsichtBeiVergleichen/2020-beat-doebeli-honegger-warum-sich-der-notfallfernunterricht-nicht-als-diskussionsgrundlage-eignet.pdf>> (zuletzt aufgerufen am 18.11.2021).
- Drackert, Stefan (2014). *Die Risiken der Verarbeitung personenbezogener Daten: Eine Untersuchung zu den Grundlagen des Datenschutzrechts*. Berlin: Duncker & Humblot.
- Eder, Sabine; Mikat, Claudia & Tillmann, Angela (Hg.) (2017). *Software takes command: Herausforderungen der „Datafizierung“ für die Medienpädagogik in Theorie und Praxis*. München: Kopaed.
- Eickelmann, Birgit; Bos, Wilfried; Gerick, Julia; Goldhammer, Frank; Schaumburg, Heike; Schwippert, Knut; Senkbeil, Martin & Vahrenhold, Jan (2019). *ICILS 2018 #Deutschland Computer- und informationsbezogene Kompetenzen von Schülerinnen und Schülern im zweiten internationalen Vergleich und Kompetenzen im Bereich Computational Thinking*. Münster, New York: Waxmann. <<https://www.waxmann.com/index.php?eID=download&buchnr=4000>> (zuletzt aufgerufen am 18.11.2021).
- Feustl, Alina (2021). Informationen zum digitalen Unterricht in Zusammenarbeit mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. In Reichwein, Wilko (Hg.), *Unterricht digital gestalten—Rahmenbedingungen und Beispiele für digitales Lernen mit iPads*. Universität Hamburg. <<https://doi.org/10.25592/UHHFDM.8405>>.
- Finck, Michèle & Pallas, Frank (2019). They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR (October 1, 2019). Forthcoming, *International Data Privacy Law*, 2020, Max Planck Institute for Innovation & Competition Research Paper No. 19-14, <<https://dx.doi.org/10.2139/ssrn.3462948>>
- Fischer, Claudia; Wawrzyniak, Jessica & Simon, Leena (2020). BigBrotherAward 2020 in der Kategorie Digitalisierung. Big Brother Awards. <<https://bigbrotherawards.de/>

- [2020/digitalisierung-bildungsministerin-baden-wuerttemberg-susanne-eisenmann](#)> (zuletzt aufgerufen am 18.11.2021).
- Friedrichs, Henrike; Junge, Thorsten & Sander, Uwe (Hg.) (2013). *Jugendmedienschutz in Deutschland*. Wiesbaden: Springer VS Verlag für Sozialwissenschaften. <<https://doi.org/10.1007/978-3-531-18905-5>>.
- Gapski, Harald (2015). *Big Data und Medienbildung. Zwischen Kontrollverlust, Selbstverteidigung und Souveränität in der digitalen Welt*. Düsseldorf, München: Kopaed.
- Gerick, Julia & Eickelmann, Birgit (2020). *Ergebnisse der vertiefenden Untersuchung der Modellschulen ‚Lernen mit digitalen Medien‘ (Phase III) in Schleswig-Holstein mit Fokus auf der Gestaltung von Schule in der Zeit der Corona-Pandemie*. Universität Hamburg, Universität Paderborn.
- Gerick, Julia; Eickelmann, Birgit & Steglich, Emilie (2019). *Abschlussbericht zur prozessbegleitenden Evaluation der Einführung von LOGINEO NRW an Pilotschulen*. Universität Hamburg, Universität Paderborn.
- Gropengießer, Harald (2004). Denkfiguren im Lehr-Lernprozess. In Gropengießer, Harald, Janßen-Bartels, Anne & Sander, Elke (Hg.), *Lehren fürs Leben: Didaktische Rekonstruktion in der Biologie*. Köln: Aulis Verlag Deubner, S. 8-24.
- Hakimi, Laura; Eynon, Rebecca & Murphy, Victoria A. (2021). The Ethics of Using Digital Trace Data in Education: A Thematic Review of the Research Landscape. In *Review of Educational Research* 91(5), S. 671-717. <<https://doi.org/10.3102/00346543211020116>>.
- Hansen, Marit (2021). Digitalisierung in der Schule – Datenschutz mitdenken. In Stapf, Ingrid, Ammicht Quinn, Regina, Friedewald, Michael, Heesen, Jessica & Krämer, Nicole (Hg.) *Aufwachsen in überwachten Umgebungen. Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend*, Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, S. 313-330. <<https://doi.org/10.5771/9783748921639-313>>.
- Heckmann, Dirk (2019). *Digitale Bildung. Lösungsvorschläge zum Datenschutz im Schulverhältnis*. vbw Vereinigung der Bayerischen Wirtschaft e. V. <[https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Bildung/2019/Downloads/Bi-0161-001\\_Digitale-Bildung.-L%C3%B6sungsvorschl%C3%A4ge-zum-Datenschutz-im-Schulverh%C3%A4ltnis.pdf](https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Bildung/2019/Downloads/Bi-0161-001_Digitale-Bildung.-L%C3%B6sungsvorschl%C3%A4ge-zum-Datenschutz-im-Schulverh%C3%A4ltnis.pdf)> (zuletzt aufgerufen am 18.11.2021).
- Heidrich, Jens; Bauer, Pascal & Krupka, Daniel (2018). Future Skills: Ansätze zur Vermittlung von Data Literacy in der Hochschulbildung. (Hochschulforum Digitalisierung, Arbeitspapier Nr. 37, S. 114). <[https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Aktionen/Data\\_Literacy/HFD\\_AP37\\_DALI\\_Studie\\_2018-09.pdf](https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Aktionen/Data_Literacy/HFD_AP37_DALI_Studie_2018-09.pdf)> (zuletzt aufgerufen am 18.11.2021).
- Hof, Simone van der (2017). I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World. *Wisconsin International Law Journal*, 34(2), S. 409–445.

- Iske, Stefan (2016). Medienbildung im Kontext digitaler Personenprofile. In Verständig, Dan; Holze, Jens & Biermann, Ralf (Hg.), *Von der Bildung zur Medienbildung*. Wiesbaden: Springer VS, S. 257–280. <[https://doi.org/10.1007/978-3-658-10007-0\\_13](https://doi.org/10.1007/978-3-658-10007-0_13)>
- Kammerl, Rudolf & Mayrberger, Kerstin (2011). Medienpädagogik in der Lehrerinnen- und Lehrerbildung in Deutschland: Aktuelle Situation und Desiderata. In *Beiträge zur Lehrerinnen- und Lehrerbildung* 29(2), S. 172–184.
- Kammerl, Rudolf; Unger, Alexander; Günther, Silke & Schwedler, Anja (2016). *BYOD – Start in die nächste Generation. Abschlussbericht der wissenschaftlichen Evaluation des Pilotprojekts*. Universität Hamburg.
- Kokott, Juliane & Sobotta, Christoph (2013). The distinction between privacy and dataprotection in the jurisprudence of the CJEU and the ECtHR. In *International Data Privacy Law* 3 (4), S. 222–228. <<https://doi.org/10.1093/idpl/ipt017>>.
- Kraut, Boris (2012). Freie Bildung: Web 2.0-Tools als Türöffner für die Wirtschaft. In Apostolopoulos, Nicolas; Mußmann, Ulrike; Coy, Wolfgang & Schwill, Andreas (Hg.), *Grundfragen Multimedialen Lehrens und Lernens: Von der Innovation zur Nachhaltigkeit*. Münster: Waxmann, S. 275–280. <[http://www.gml-2012.de/tagungsband/Tagungsband\\_GML2012\\_web.pdf](http://www.gml-2012.de/tagungsband/Tagungsband_GML2012_web.pdf)> (zuletzt aufgerufen am 18.11.2021).
- Kultusministerkonferenz (KMK) (2012). Medienbildung in der Schule. Beschluss der Kultusministerkonferenz vom 8. März 2012. <[https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen\\_beschluesse/2012/2012\\_03\\_08\\_Medienbildung.pdf](https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2012/2012_03_08_Medienbildung.pdf)> (zuletzt aufgerufen am 18.11.2021).
- \_\_\_ (2017). Bildung in der digitalen Welt. Strategie der Kultusministerkonferenz. <[https://www.kmk.org/fileadmin/pdf/PresseUndAktuelles/2018/Digitalstrategie\\_2017\\_mit>Weiterbildung.pdf](https://www.kmk.org/fileadmin/pdf/PresseUndAktuelles/2018/Digitalstrategie_2017_mit>Weiterbildung.pdf)> (zuletzt aufgerufen am 18.11.2021).
- \_\_\_ (2019a). Ländergemeinsame inhaltliche Anforderungen für die Fachwissenschaften und Fachdidaktiken in der Lehrerbildung. Kultusministerkonferenz. <[http://www.kmk.org/fileadmin/Dateien/veroeffentlichungen\\_beschluesse/2008/2008\\_10\\_16-Fachprofile-Lehrerbildung.pdf](http://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2008/2008_10_16-Fachprofile-Lehrerbildung.pdf)> (zuletzt aufgerufen am 18.11.2021).
- \_\_\_ (2019b). Standards der Lehrerbildung: Bildungswissenschaften. Kultusministerkonferenz. <[http://www.kmk.org/fileadmin/Dateien/veroeffentlichungen\\_beschluesse/2004/2004\\_12\\_16-Standards-Lehrerbildung-Bildungswissenschaften.pdf](http://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2004/2004_12_16-Standards-Lehrerbildung-Bildungswissenschaften.pdf)> (zuletzt aufgerufen am 18.11.2021).
- Lakoff, Georg & Johnson, Mark (2014). *Leben in Metaphern: Konstruktion und Gebrauch von Sprachbildern* (8. Aufl.). Heidelberg: Carl-Auer-Verlag.
- Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) (2021b). Pandemie und Schule – Datenschutz mit Augenmaß. <<https://www.lds.nrw.de/mainmenu/Aktuelles/Inhalt/Schule-Videokonferenzsysteme-und-Messenger-Dienste-waehrend-der-Corona-Pandemie/LDI-NRW---Pandemie-und-Schule--Datenschutz-mit-Augenmass-2021-05.pdf>> (zuletzt aufgerufen am 18.11.2021).

- Livingstone, Sonia; Stoilova, Mariya & Nandagiri, Rishita (2021). Data and privacy literacy: the role of the school in educating children in a datafied society. In Stapf et al. (Hg.), S. 219-236.
- Lenhard, Thomas H. (2020). *Datensicherheit: Technische und organisatorische Schutzmaßnahmen gegen Datenverlust und Computerkriminalität*. Wiesbaden: Springer Vieweg. <<https://doi.org/10.1007/978-3-658-29866-1>>.
- Lorenz, Ramona; Bos, Wilfried; Endberg, Manuela; Eickelmann, Birgit, Grafe, Silke & Vahrenhold, Jan (Hg.) (2017). *Schule digital. Der Länderindikator 2017. Schulische Medienbildung in der Sekundarstufe I mit besonderem Fokus auf MINT-Fächer im Bundesländervergleich und Trends von 2015 bis 2017*. Münster: Waxmann.
- Lorenz, Ramona & Endberg, Manuela (2019). Welche professionellen Handlungskompetenzen benötigen Lehrpersonen im Kontext der Digitalisierung in der Schule? Theoretische Diskussion unter Berücksichtigung der Perspektive Lehramtsstudierender. In *MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung*, 2019 (Occasional Papers), S. 61–81. <<https://doi.org/10.21240/mpaed/00/2019.10.16.X>>.
- Medienpädagogischer Forschungsverbund Südwest (MPFS) (2020). *JIM-Studie 2019. Jugend, Information, Medien. Basisuntersuchung zum Umgang 12- bis 19-Jähriger*. <[https://www.mpfs.de/fileadmin/files/Studien/JIM/2020/JIM-Studie-2020\\_Web\\_final.pdf](https://www.mpfs.de/fileadmin/files/Studien/JIM/2020/JIM-Studie-2020_Web_final.pdf)> (zuletzt aufgerufen am 18.11.2021).
- Meyer-Scholten, Jörg (2021, Februar 5). Vorabinformation zur Nutzung von Padlet [Persönliche Kommunikation].
- Nebel, Maxi (2020). *Persönlichkeitsschutz in Social Networks: Technische Unterstützung eines grundrechtskonformen Angebots von Social Networks*. Wiesbaden: Springer Vieweg. <<https://doi.org/10.1007/978-3-658-31786-7>>.
- Nebel, Maxi (2021). Digitales Lernen – Datenschutzrechtliche Rechtsgrundlagen von Lernplattformen für Kinder und Erwachsene. In Stapf et al. (Hg.), S. 197–218.
- Petric, Ronald & Sorge, Christoph (2017). *Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie*. Wiesbaden: Springer Vieweg. <<https://doi.org/10.1007/978-3-658-16839-1>>.
- Pohle, Jörg & Hölzel, Julian (2020). Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts. Berlin: Alexander von Humboldt Institut für Internet und Gesellschaft <[https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1\\_Anonymisierung/Stellungnahmen/Alexander-von-Humboldt-Institut.pdf?blob=publicationFile&v=3](https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellungnahmen/Alexander-von-Humboldt-Institut.pdf?blob=publicationFile&v=3)> (zuletzt aufgerufen am 18.11.2021)
- Rau, Franco; Grell, Petra; Geritan, Anna; Galanamatis, Britta & Gerber, Lars (2021). *Bildung in der digitalen Welt „Darmstädter Modellschulen“. Zwischenbericht zur Begleitung von drei Modellschulen unter Pandemiebedingungen*. TU Darmstadt. <<https://tuprints.ulb.tu-darmstadt.de/17655/>> (zuletzt aufgerufen am 18.11.2021).



- Rau, Franco & Kosubski, Ilaria (2019). «Digitale Medien sind wie Pilze»: Eine Analyse studentischer Metaphern zu digitalen Medien. In *MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung* 36 (Teilhabe), S. 81–96. <<https://doi.org/10.21240/mpaed/36/2019.11.14.X>>.
- Reichwein, Wilko (2021). *Unterricht digital gestalten—Rahmenbedingungen und Beispiele für digitales Lernen mit iPads*. Universität Hamburg. <<https://doi.org/10.25592/UHHFDM.8405>>.
- Robert Bosch Stiftung, & Die Deutsche Schulakademie. (2020). Konzept: Zwischen Chance und Herausforderung. Deutsches Schulportal vom 13. Juli 2020. <<https://deutsches-schulportal.de/konzepte/zwischen-chance-und-herausforderung/>> (zuletzt aufgerufen am 18.11.2021).
- Robert Bosch Stiftung, & Die Deutsche Schulakademie. (2021). Sendepläne und tägliche Lernreflexionen geben Halt. Deutsches Schulportal vom 12. April 2021. <<https://deutsches-schulportal.de/konzepte/sendeplaene-und-taegliche-lernreflexionen-geben-halt/>> (zuletzt aufgerufen am 18.11.2021).
- Roßnagel, Alexander (2021). Privatheit und Selbstbestimmung von Kindern in der digitalisierten Welt: Ein juristischer Blick auf die Datenschutz-Grundverordnung. In Stapf et al. (Hg), S. 165–196.
- Ruhenstroth, Miriam & Baulig, Thorsten (2020). Interaktions-App Padlet im Test. Mobil-sicher. Das Infoportal für sichere Handynutzung. Eintrag vom 15. September 2020. <<https://mobilsicher.de/ratgeber/interaktions-app-padlet-im-test>> (zuletzt aufgerufen am 18.11.2021).
- Rummler, Klaus; Müller, Jane; Kamin, Anna-Maria; Richter, Lea; Kammerl, Rudolf; Potzel, Katrin; Grabensteiner, Caroline & Schneider Stingelin, Colette (2021). Medienhandeln Heranwachsender im Spannungsfeld schulischer und familialer Lernumgebungen. In *MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung* 42 (Optimierung), S. 63–84. <<https://doi.org/10.21240/mpaed/42/2021.03.10.X>>.
- Stapf, Ingrid; Ammicht Quinn, Regina; Friedewald, Michael; Heesen, Jessica; Krämer, Nicole (Hg.) (2021). *Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend* (1. Aufl., Bd. 14). Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG. <<https://doi.org/10.5771/9783748921639>>.
- Sassenberg, Elke (2019). Datenschutz in Schule und Schulverwaltung. In Specht, Louisa & Mantz, Reto (Hg.) *Handbuch Europäisches und deutsches Datenschutzrecht. Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor*, München: C.H. Beck oHG.
- Scheppler, René, & Wampfler, Philippe (2021). Von Datenschutz, Pragmatismus und zeitgemäßer Bildung. Bundeszentrale für politische Bildung. <<https://www.bpb.de/lernen/digitale-bildung/werkstatt/328594/von-datenschutz-pragmatismus-und-zeitgemaesser-bildung>> (zuletzt aufgerufen am 18.11.2021).

- Schmitt, Rudolf (2017). *Systematische Metaphernanalyse als Methode der qualitativen Sozialforschung*. Wiesbaden: Springer VS. <<https://doi.org/10.1007/978-3-658-13464-8>>.
- Schüller, Katharina (2019). Ein Framework für Data Literacy. In *AStA Wirtschafts- und Sozialstatistisches Archiv* 13(3–4), S. 297–317. <<https://doi.org/10.1007/s11943-019-00261-9>>.
- Schulz, Andreas D. (2021). Datenschutz und Medienbildung – Chancen und Barrieren in der schulischen Praxis. In Stapf et al. (Hg), S. 279–292.
- Smolczyk, Maja & Kugelmann, Dieter (2021). Standpunkt: Schluss mit den Attacken auf den Datenschutz! Berliner Beauftragte für Datenschutz und Informationssicherheit. <[https://www.datenschutz-berlin.de/fileadmin/user\\_upload/pdf/pressemitteilungen/2021/2021-BlnBDI-LfdRLP-Standpunkt\\_Attacke\\_auf\\_Datenschutz.pdf](https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/2021-BlnBDI-LfdRLP-Standpunkt_Attacke_auf_Datenschutz.pdf)> (zuletzt abgerufen am 18.11.2021).
- Steinebach, Martin; Krempel, Erik; Jung, Christian & Hoffmann, Mario (2016). Datenschutz und Datenanalyse. Herausforderungen und Lösungsansätze. In *Datenschutz und Datensicherheit - DuD*, 40 (7), S. 440–445. <<https://doi.org/10.1007/s11623-016-0633-7>>.
- Steinmüller, Wilhelm; Lutterbeck, Bernd; Mallmann, Christoph, Harbort, Uwe; Kolb, Gerhard & Schneider, Jochen (1971). Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern (VI/3826 Anlage 1). <<http://dipbt.bundestag.de/doc/btd/06/038/0603826.pdf>> (zuletzt aufgerufen am 18.11.2021).
- Thiede, Dirk (2021). Padlet—Digitale Pinnwand. Datenschutz-schule.info. Datenschutz ist ein Grundrecht - auch in der Schule. Eintrag Februar 2021. <<https://datenschutz-schule.info/datenschutz-check/padlet-digitale-pinnwand/>> (zuletzt aufgerufen am 18.11.2021).
- von Lewinski, Kai (2014). *Die Matrix des Datenschutzes - Besichtigung und Ordnung eines Begriffsfeldes* (Bd. 1). Tübingen: Mohr Siebeck.
- Zorn, Isabel; Murmann, Jule & Harrach-Lasfaghi, Asmae (2021). Kriterien für die Auswahl privatsphäreschützender Messenger-Dienste für Einrichtungen der Sozialen Arbeit. In Stapf et al. (Hg), S. 331–350.

## Über die Autor\*innen

**Prof. Dr. Franco Rau** ist Juniorprofessor für Mediendidaktik an der Universität Vechta. Im Kontext aktueller Digitalisierungs- und Mediatisierungsprozesse bearbeitet er Fragen zur Unterrichts- und Schulentwicklung sowie der Lehrer\*innenbildung. In seiner Dissertation untersuchte Franco Rau Entwicklungspotenzialen einer integrativen Medienbildung in der Lehrer\*innenbildung. Als Mitglied der „Werkstatt Digitalisierung in inklusiven Settings“ (Bridges, BMBF) arbeitet er derzeit der Erforschung neuer Strukturen und Strategien im Umgang mit Digitalisierung in inklusiven Kontexten. Im Kooperationsprojekt „Bildung in der digitalen Welt. Darmstädter Modellschulen“ untersucht er Schulentwicklungsprozesse in einem gestaltungsorientierten Forschungsansatz.

Korrespondenzadresse: [franco.rau@uni-vechta.de](mailto:franco.rau@uni-vechta.de)

**Britta Galanamatis**, M.A. ist wissenschaftliche Mitarbeiterin am Arbeitsbereich für Allgemeine Pädagogik mit dem Schwerpunkt Medienpädagogik an der Technischen Universität Darmstadt. Dort ist sie unter anderem für das Forschungs- und Entwicklungsprojekt „Bildung in der digitalen Welt: Darmstädter Modellschulen“ tätig. Sie hat Erziehungswissenschaft an der Goethe-Universität Frankfurt und Bildungswissenschaften an der Technischen Universität Darmstadt studiert. Korrespondenzadresse: [britta.galanamatis@tu-darmstadt.de](mailto:britta.galanamatis@tu-darmstadt.de)

**Lars Gerber**, M.A. ist wissenschaftlicher Mitarbeiter am Arbeitsbereich für Allgemeine Pädagogik mit dem Schwerpunkt Medienpädagogik an der Technischen Universität Darmstadt. Er arbeitet unter anderem im Forschungs- und Entwicklungsprojekt „Bildung in der digitalen Welt: Darmstädter Modellschulen“. Lars Gerber hat Pädagogik an der Technischen Universität Darmstadt und Erziehungs- und Bildungswissenschaften mit dem Schwerpunkt Außerschulische Jugend- und Erwachsenenbildung an der Philipps Universität Marburg studiert. Korrespondenzadresse: [lars.gerber@tu-darmstadt.de](mailto:lars.gerber@tu-darmstadt.de)

**Anna Geritan**, M.A. ist wissenschaftliche Mitarbeiterin am Arbeitsbereich für Allgemeine Pädagogik mit dem Schwerpunkt Medienpädagogik an der Technischen Universität Darmstadt. Dort ist sie unter anderem für das Forschungs- und Entwicklungsprojekt „Bildung in der digitalen Welt: Darmstädter Modellschulen“ tätig. Sie hat Erziehungswissenschaft mit dem Schwerpunkt Lebenslanges Lernen und Medienbildung an der Johannes-Gutenberg-Universität Mainz sowie Pädagogik mit dem Schwerpunkt Kinder- und Jugendhilfe an der Universität Koblenz-Landau studiert. Korrespondenzadresse: [anna.geritan@tu-darmstadt.de](mailto:anna.geritan@tu-darmstadt.de)