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).