forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

White Paper

PRIVATHEIT UND KINDERRECHTE

IMPRESSUM

Autoren:
Ingrid Stapf, Judith Meinert, Jessica Heesen, Nicole Krämer, Regina Ammicht Quinn, Felix Bieker, Michael Friedewald, Christian Geminn, Nicholas Martin, Maxi Nebel, Carsten Ochs

Kontakt:
Michael Friedewald

Telefon +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage, Mai 2020

Einleitung

Die Jahrestagung des Forum Privatheit im November 2019 hat das Thema „Aufwachsen in überwachten Umgebungen" in Deutschland erstmals interdisziplinär aufgegriffen. Dabei zeigte sich eine Diskrepanz zwischen dem gesellschaftlichen und politischen Orientierungs- und Steuerungsbedarf einerseits und der wissenschaftlichen Forschung an der Schnittstelle von Theorie und Praxis andererseits.

Mit dem Aufkommen überwachungsbasierter Medientechnologien von Smart Toys, Babysitter-Kameras im Teddy-Bär bis hin zu Sprachassistenzsystemen wie Alexa, individualisierte Lernsoftware, Tracking-Apps oder Videoüberwachung in der Kita, stellt sich die Frage, was Privatheit von Kindern heute ausmacht: Bedarf es bei Kindern anderer Konzepte als bei Erwachsenen? Wie können sie den Schutz ihrer Daten im Altersverlauf steuern? Und wer trägt die Verantwortung?

Dieses White Paper analysiert das Recht von Kindern auf Privatheit mit Blick auf digitale Umwelten, bezieht sich auf aktuelle empirische Daten und leitet daraus aktuelle Forderungen an Politik, die Medienregulierung, den Bildungsbereich sowie mediale Anbieter ab. **Unsere Kernthese ist: Die Rechte von Kindern in digitalen Handlungswelten müssen stärker durchgesetzt und berücksichtigt werden. Dazu gehören explizit das Recht auf informationelle Selbstbestimmung, der Datenschutz, die freie Entfaltung der Persönlichkeit und ein geschützter Privatbereich.** Ziel des White Papers ist es, einen gesellschaftlich-politischen Diskurs anzustoßen, erste Anforderungen für die Praxis zu formulieren sowie den Forschungsbedarf aufzuzeigen.

Demokratische Freiheits- und Gleichheitsrechte sollen Kindern das Recht auf eine offene Zukunft ermöglichen. Da Kindheit eine besonders verletzliche Entwicklungsphase ist und sich wichtige Fähigkeiten erst noch ausbilden, bedürfen Kinder eines umfassenden Schutzes durch Fürsorgetragende und den Staat. Sie sollen gleichzeitig aber auch als handelnde Subjekte ihre Selbstbestimmung erproben können. Hierzu werden Befähigungsmaßnahmen wesentlich, welche die Mündigkeit von Kindern in der Demokratie (und im „digitalen Gemeinwesen") zum Ziel haben. Das Thema Privatheit von Kindern weist dabei eine Dualität auf: einerseits als fürsorglicher Schutz im Interesse des Kindes, andererseits aber auch als paternalistische Überwachungspraktiken, die kindliche Selbstbestimmungsansprüche in Frage stellen.

Aus der fortschreitenden „Mediatisierung von Kindheit" resultiert Handlungsbedarf mit Blick auf damit verbundene Risiken. Denn Kinder und Jugendliche bis 18 Jahren machen rund ein Drittel der weltweiten Internetznutzer*innen aus. Dieses White Paper füllt eine bestehende Lücke, da das Zusammenspiel von Privatheit und Kinderrechten bislang noch kaum wissenschaftlich differenziert untersucht wurde.

Kinderrechte wurden – ergänzend zu den allgemeinen Menschenrechten – 1989 völkerrechtlich in der UN-Kinderrechtskonvention (UN-KRK) verankert und gelten seit 1992 als einfaches Recht in Deutschland. Die Rechte von Kindern werden zudem in Artikel 24 der EU-Grundrechtecharta verbrieft. Die UN-KRK betont die Rolle von Kindern als subjektive Handlungsträger mit eigenen Rechten und etabliert in 54 Artikeln das beste Interesse von Kindern als leitendes Prinzip im Zusammenspiel von Schutz-, Förderungs- und Beteiligungsrechten. In Artikel 16 UN-KRK ist das Recht auf „Schutz der Privatsphäre und Ehre" formuliert.

Aktuelle Entwicklungen zur Aufnahme von Kinderrechten ins Grundgesetz bedürfen einer rechtzeitigen Auseinandersetzung mit der Bedeutung der spezifischen Problemlagen rund um ein Recht auf Privatheit von Kindern in digitalen Kontexten. Diese Auseinandersetzung möchte das Paper anstoßen und erste Forderungen kurz vor dem 2. Jahrestag der Geltung der DSGVO herausarbeiten.

Privatheit im Kontext der Digitalisierung

Kindheit ist nicht nur eine biologische Lebensphase, sondern wird auch gesellschaftlich-kulturell konstruiert. In Deutschland herrscht ein stark schutzbetonter Blick auf Kinder vor, der im Recht den Ausdruck in der Redensart vom Kind als der „Heiligen Kuh des BGB" gefunden hat. Dahinter steht die Idee, dass Kinder geschützte Räume brauchen, um ihre Persönlichkeit und auch ihre Selbstbestimmung erproben und erlernen zu können. Das Kinderzimmer galt lange als Raum des Rückzugs, in dem sich der im Kindheitsverlauf wachsende Wunsch von Kindern nach eigenen Bereichen, Erfahrungen und Beziehungen entwickelt.

Im Zuge der zunehmenden Digitalisierung haben Kinder und Jugendliche heute jedoch im Internet nicht nur einen umfassenden Zugriff auf mediale Inhalte, globale Plattformen und eine Vielfalt an Informationen, sondern geben dabei gleichzeitig viele ihrer persönlichen Daten preis. Das geschieht nicht nur im Rahmen einer aktiven, selbstinitiierten Weitergabe, beispielsweise, wenn ein Social Media Profil mit persönlichen Daten gefüllt wird und in Interaktionen mit anderen Nutzer*innen Fotos, Daten und Informationen ausgetauscht werden. Neben der aktiven Preisgabe von Daten und persönlichen Informationen und der damit einhergehenden Gefahr, dass Gleichaltrige diese zum Beispiel für Cybermobbing-Angriffe nutzen (horizontale Privatheitsbedrohung), ist auch die passive Sammlung, Analyse und der Verkauf von Daten durch Unternehmen eine Gefahr, der sich Kinder und Jugendliche nicht vollständig bewusst sind (vertikale Privatheitsbedrohung).

Der Begriff Privatheit in digitalen Kontexten

Privatheit ist eine wesentliche Bedingung für Demokratie und Rechtsstaatlichkeit. Als Sammelbegriff für bestimmte zu schützende Positionen ist Privatheit jedoch keine rein rechtliche Kategorie. Der Begriff der Privatheit umfasst zahlreiche Teilaspekte. Dazu gehören auch Rechte, wie das Recht auf informationelle Selbstbestimmung, das Recht auf Schutz des Privaten und das Recht auf Datenschutz sowie das Persönlichkeitsrecht, das Post- und Fernmeldegeheimnis, die Unverletzlichkeit der Wohnung und das sogenannte IT-Grundrecht, das die Vertraulichkeit und Integrität informationstechnischer Systeme zum Schutzzweck hat.

Für den digitalen Bereich ist das Recht auf informationelle Selbstbestimmung eine zentrale Kategorie. Es unterscheidet sich jedoch strukturell stark vom paternalistischen Ansatz der Bestimmung eines schützenswerten Bereiches von außen („Privatsphäre"), indem die Selbstbestimmung des Einzelnen zum Maßstab erhoben wird (Geminn & Roßnagel, 2015; Nebel, 2015). Bei einem schutzbetonten Ansatz legen Dritte, nämlich staatliche Behörden, die Justiz und auch die Rechtswissenschaften fest, was „privat" und damit geschützt ist. Diese fremdbestimmte Vorstellung wird dem Einzelnen gleichsam aufoktroyiert. Ausgangspunkt des Ansatzes ist mithin der Staat; er legt die Grenzen der „Privatheit" fest. Demgegenüber steht hinter der informationellen Selbstbestimmung ein freiheitsorientierter Ansatz, der die autonome Entscheidungsfähigkeit der Akteure in den Vordergrund stellt. Für Erwachsene wird diese Selbstbestimmung im Grundsatz voll angenommen, bei Kindern müssen die Grenzen jedoch individuell ausgelotet werden.

Aktuelle Herausforderungen mit Blick auf Medien und Kinder

Die aktuellen Nutzungszahlen belegen nicht nur, dass bereits sehr junge Kinder über ein eigenes Smartphone verfügen und Zugang zum Internet haben, sondern auch, dass sie täglich Apps wie WhatsApp und YouTube sowie digitale Spiele nutzen (Hajok, 2019; Rathgeb & Behrens, 2018b). Weiterhin steigt die Nutzung mit dem Alter stark

an, sodass unter den 12- bis 19- Jährigen bereits 97 Prozent ein eigenes Smartphone besitzen und 89 Prozent täglich online sind (Engels, 2018, Rathgeb & Behrens, 2018a).

Die beliebtesten Apps von Kindern und Jugendlichen sind momentan WhatsApp, Instagram, YouTube und Snapchat (Rathgeb & Behrens, 2018a). Auch die chinesische App TikTok gewinnt zunehmend an Popularität (Monllos, 2019). In einer Studie, die Jugendliche zu ihrem Datenschutzverhalten befragte, gaben 67 Prozent an, die Speicherung ihrer persönlichen Daten durch diese Apps abzulehnen (Engels, 2018). Das hatte jedoch überwiegend keinen Einfluss auf ihr Nutzungsverhalten. Dieses Phänomen wird in der Forschung als „privacy paradox" (Barnes, 2006; Norberg, Horne & Horne, 2007) bezeichnet und diskutiert (Baruh, Secinti & Cemalcilar, 2017). Den Grund für das scheinbar widersprüchliche Verhalten vermuten Wissenschaftlerinnen (Livingstone, Stoilova & Nandagiri, 2019) darin, dass Kinder im Internet einerseits freiwillig persönliche Informationen online teilen und dabei Risiken für ihre Sicherheit und ihre Privatheit in Kauf nehmen, obwohl sie andererseits ihre Privatheit schützen wollen. Der Widerspruch besteht dann darin, dass soziale Teilhabe nur bei Aufgabe herkömmlicher Privatheitsvorstellungen zu haben ist. Studien mit erwachsenen Teilnehmer*innen betonen darüber hinaus, dass ein Gefühl von Machtlosigkeit und Resignation sowie mangelnde Wahlmöglichkeiten ein Grund für das privacy paradox sind (Matzner, Masur, Ochs & von Pape, 2016; Stoycheff 2016). Andere wiederum betonen, dass es in Bezug auf das scheinbar widersprüchliche Nutzungsverhalten um eine Abwägung verschiedener Wertvorstellungen geht, die eher mit Konzepten zur Risikoanalyse anstelle von Paradoxien treffend beschrieben werden können. Ferner wurde nachgewiesen, dass es sich tatsächlich nur scheinbar um eine Paradoxie handelt, da eine genauere Analyse auf Basis der psychologischen „Theory of Planned Behavior" aufzeigt, dass bei Erfragen von spezifischen Einstellungen und Intentionen sehr wohl eine Deckungsgleichheit von Einstellungen und privatheitsbezogenem Verhalten nachweisbar ist (Dienlin & Trepte, 2015). Gerade bei jüngeren Kindern kommt das Problem hinzu, wieviel Wissen und Erfahrungen schon vorausgesetzt werden können, um derartige Abwägungen überhaupt treffen zu können.

Die gängigen Anwendungen wie Facebook, Instagram, TikTok und Snapchat berufen sich auf eine Altersbeschränkung ab 13 Jahren, bei WhatsApp beispielsweise wurde diese im Zuge des Geltungsbeginns der DSGVO im Mai 2018 auf 16 Jahre angehoben. Allerdings handelt es sich dabei um eine Formalität ohne praktische Bedeutung, da sich die Apps ohne Altersüberprüfung herunterladen und nutzen lassen. Dies wirft insgesamt die Frage auf, ob eine solche Form der Selbstkontrolle ein valides Instrument ist, um Kinder und Jugendliche von der Nutzung datenschutzkritischer Anwendungen abzuhalten. Vor dem Hintergrund des hohen Belohnungswertes, den diese Anwendungen mit sich bringen, erscheint es zudem weder erwartbar noch vertretbar, Heranwachsende davon fernhalten zu wollen, auf eine Benutzung zu verzichten, weil der Verzicht mit weniger Gefahren einhergeht.

Mit der zunehmenden Mediatisierung von Kindheit (Kutscher, 2012; Tillmann & Hugger, 2014) nutzen Kinder also schon sehr früh eigene digitale Geräte. Damit erhalten sie nicht nur Zugang zu Inhalten, Netzwerken und Plattformen, die ihre Rechte auf Information, medialen Zugang und Teilhabe neuartig und umfassend ermöglichen, sondern gleichzeitig auch ihre Persönlichkeitsrechte beeinträchtigen. Da digital vernetzte Medien mobil und abseits elterlicher Kontrolle genutzt werden und der rechtliche Jugendmedienschutz aktuell durch den digitalen Wandel grundlegend herausgefordert ist, sind schon jüngere Kinder erhöhten Risiken ausgesetzt, die sich auf ihre Entwicklung auswirken können (Brüggen et al., 2019).

Der Prozess intensiver Datensammlung, Beobachtung und Überwachung wird als Bestandteil der „Datafizierung" bezeichnet (Lupton & Williamson, 2017). Auch Daten von Kindern werden hier zu „Gütern", die mit Vermarktungsinteressen verbunden sind. Gerade Spiele-Apps mit Captology-Technik, einer Computertechnologie, welche das

Beurteilungs- und Entscheidungsverhalten von Menschen zu beeinflussen versucht (z.B. Pokémon-Go, Candy-Crush Saga), personalisierte Werbung mit Aufforderungscharakter bis hin zu rein kommerziellen Zwecken (z.B. Instagram, TikTok), im kindlichen Spiel eingesetzte Smart Toys, die systematisch Daten auswerten und speichern (z.B. der Roboter i-Que, Cloud Pets, Hello Barbie), die Verwendung von Klassenchats, die Daten systematisch abgreifen (z.B. WhatsApp), das Preisgeben des Standorts von Kindern in sozialen Medien (z.B. TikTok) oder die von Fürsorgetragenden gewollte Überwachung im familiären oder schulischen Umfeld durch Tracking-Apps (z.B. Little Nanny GPS Tracker) sowie individualisierte und Profile erstellende Lernsoftware (z.B. Quizlet) beschneiden die Rechte von Kindern auf eine offene Zukunft und das Erproben von Selbstbestimmung in einem für Kinder oft nicht einschätzbaren öffentlichen und kommerziell durchdrungenen Raum (Fahlquist, 2015; Forum Privatheit 2018). Um bestimmte Apps und Dienste kostenlos nutzen zu können sind Kinder und Jugendliche häufig bereit, bestimmte persönliche Daten preiszugeben – ohne dabei die volle Tragweite der vermeintlichen harmlosen Informationsweitergabe überschauen zu können (Engels, 2018).

In digitalen Kontexten werden die Entscheidungen und Praktiken von Kindern und Jugendlichen durch die soziale Umgebung, allem voran durch das vorgelebte Verhalten ihrer Eltern und der Peer-Group beeinflusst (vgl. Kapitel Einfluss- und Schutzfaktoren bei der Internetnutzung durch Kinder und Jugendliche, S. 11). Ob Kinder persönliche Daten teilen oder zurückhalten, verhandeln sie in einem Kontext vernetzter Kommunikation und damit verknüpfter Praktiken. Eine aktuelle Studie (Livingstone et al., 2019) differenziert hierbei zwischen einer relationalen (das Daten-Ich, das über das eigene Sozialverhalten online geschaffen wird), einer institutionellen (durch das Sammeln und Auswerten persönlicher Daten durch Regierung, Bildungs- oder Gesundheitseinrichtungen) und einer kommerziellen Privatheit (persönliche Daten, die für Unternehmen wirtschaftlich verwendet werden). Hinsichtlich letzterer fühlen sich Kinder am wenigsten handlungsmächtig.

Kinder als besonders vulnerable Gruppe

Kinder und Jugendliche werden immer wieder als besonders vulnerable Gruppe bezeichnet. Diese Vulnerabilität gründet darin, dass sich Kinder und Jugendliche hinsichtlich ihrer kognitiven Voraussetzungen von Erwachsenen unterscheiden, dass sie weniger Vorwissen und Erfahrungen zu bestimmten gesellschaftlichen Prozessen haben sowie, dass sie eine für ihre Altersgruppe spezifische Herangehensweise an Medien pflegen.

Kognitive Voraussetzungen

Wie Studien etwa von Sonia Livingstone zeigen, sind Kinder unter 11 Jahren typischerweise in ihrer Entwicklung noch nicht weit genug vorangeschritten, um Konzepte wie „Privatheit" vollumfänglich zu begreifen. Auch sind Kinder weniger in der Lage, das monetäre Potenzial von Daten und deren Nutzung für Profiling einzuschätzen (Livingstone et al., 2019). Erst beginnend im Jugendalter wird die Fähigkeit zum abstrakteren Denken ausgebildet, was auch das Erkennen von (intransparenten) Zusammenhängen umfasst, dem sogenannten formal-operationalen Denken (vgl. Piaget, 1972). Insbesondere bei Kindern in der Pubertät wurde nachgewiesen, dass verschiedene neuronale Verschaltungen temporär eingeschränkter funktionieren als in der Kindheit oder im Erwachsenenalter (Powell, 2006). Dies kann das Verständnis – zum Beispiel der potenziellen Konsequenzen der Online-Selbstoffenbarung – zusätzlich erschweren.

Vor dem Hintergrund ihrer noch nicht vollständig abgeschlossenen Entwicklung sind Kinder und Jugendliche somit auch besonders anfällig für Online-Dienste, die auf kurzfristige Erfolgserlebnisse, Belohnungsanreize und soziale Honorierung setzen und im Gegenzug Datenprofile der Nutzenden sammeln – sowohl aus aktiv veröffentlichten Daten als auch durch die passive und intransparente Speicherung von Klicks, Webseitenbesuchen und Likes. Prominente Beispiele dafür sind – neben WhatsApp, Instagram, Facebook, Reddit und Snapchat, die über soziale Belohnungssysteme arbeiten – digitale Spiele-Apps wie Pokémon-Go oder die chinesische Video- und Musik-App TikTok. Die Mechanismen dieser Applikationen basieren auf einer Bindung der Nutzenden durch wiederholte Push-Nachrichten, Belohnungen für erreichte Ziele, soziale Vernetzung mit anderen Nutzenden oder Spieler*innen und der Möglichkeit einer Bühne zur Selbstdarstellung. Diese sind für die jüngeren Nutzer*innen schwer zu durchschauen und – sofern die Nutzungsdynamik einmal begonnen hat – zu durchbrechen.

Fehlender Erfahrungshintergrund

Zahlreiche Publikationen weisen darauf hin, dass Kinder und Jugendliche sich der Gefahren für Privatheit und Datenschutz und den potenziellen Folgen eher wenig bewusst sind (Heeg et al., 2018; Naplavova, Ludik, Hruza & Bozek, 2014). Werden Kinder direkter befragt, welche Gefahren sie im Internet vermuten, lässt sich ein deutlicher Effekt der Medienberichterstattung der vergangenen Jahre feststellen: Befürchtungen von Kindern und Jugendlichen in Bezug auf eine Verletzung ihrer Online-Privatheit beziehen sich vor allem auf andere Nutzer*innen und somit vertikale Privatheitsbedrohungen. Eine häufig artikulierte Gefahr ist zum Beispiel Online-Mobbing bzw. Cyberbullying, welches durch die Beschränkung der Sichtbarkeit einzelner Fotos oder Beiträge oder des gesamten Profils zu verhindern versucht wird (Borgstedt, Roden, Borchard, Rätz & Ernst, 2014). Ebenso sind die Gefahren des Cybergrooming eher präsent, die in einer qualitativen Studie in neun europäischen Ländern als Gefahr der Kontaktanbahnung durch Fremde detailliert beschrieben wird (Mascheroni, Jorge & Farrugia, 2014). Über die Hintergründe und potenziellen Gefahren der Datenökonomie besteht dagegen kaum Bewusstsein (Livingstone et al., 2019).

Kinder als besonders vulnerable Gruppe

Altersgruppenspezifische Herangehensweise an Medien

Kinder und Jugendlichen gelten oft als „Digital Natives“, da sie von frühester Kindheit an mit dem Internet aufgewachsen sind. Auch wenn sie mit digitalen Medien aufwachsen, heißt dies aber nicht, dass eine kritische Reflexion der Effekte und Nebenfolgen der Nutzung von Informations- und Medientechniken nicht gelernt werden müsste (kritisch zum Begriff „Digital Natives“; vgl. Genner & Süss, 2017; Prinzing, 2019). Neben positiven Konsequenzen wie einer hohen technischen Affinität führt die quasi selbstverständliche Nutzung auch dazu, dass bestimmte Persuasionsmechanismen wie die Aufforderung Inhalte zu abonnieren und die Existenz personalisierter Werbung nicht (mehr) hinterfragt als selbstverständliche Bestandteile der Funktionsweise des modernen Internets empfunden werden (Wang et al., 2019).

Auf der anderen Seite nähern sich Kinder den neuen digitalen Angeboten vor allem aus ihrer Erfahrungswelt heraus: Hier kann besonders die Tatsache problematisch sein, dass sich Kinder neue Spiele durch einfaches Ausprobieren aneignen – ohne vorab Informationen oder Warnungen zu beachten und Gefahren dadurch erst retrospektiv überhaupt erkannt werden können (Borgstedt et al., 2014). Generell zeigt sich dabei, dass der Grad der Sichtbarkeit der eigenen Aktivitäten in Online-Applikationen nur schwer eingeschätzt werden kann. Das geht sogar so weit, dass die „Öffentlichkeit“ einer Interaktion an den jeweils beteiligten Akteur*innen festgemacht wird, wodurch ein WhatsApp Chat zwischen zwei Personen als vollkommen privat empfunden wird (Borgstedt et al., 2014), obwohl trotz der Ende-zu-Ende-Verschlüsselungen private Inhalte durch andere Nutzer*innen geteilt werden können, Metadaten transparent sind oder Sicherheitsrisiken durch die Speicherung von Fotos bestehen. Ein Verständnis der Datenverarbeitung wird dadurch erschwert, dass sich die Nutzungsbedingungen, die oftmals sowohl für Kinder als auch deren Eltern kaum verständlich sind, primär an Eltern als Sorgeberechtigte wenden, die aber nicht notwendigerweise an der Nutzung beteiligt sind. Folglich kann keine informierte Entscheidung angenommen werden.

Dies ist jedoch aus datenschutzrechtlicher Sicht problematisch, da eine ausreichende Informationsgrundlage eine zentrale Voraussetzung einer wirksamen Einwilligung in die Datenverarbeitung nach Artikel 7 Abs. 1 DSGVO – bei Kindern in Verbindung mit Artikel 8 DSGVO – ist. Nur bei Kenntnis aller entscheidungsrelevanten Informationen können die Nutzer*innen Risiken und Vorteile abschätzen und dann sachgerecht über die Einwilligung entscheiden. In der Praxis zeichnet sich jedoch ein gegenteiliges Bild ab, da diese in den seltensten Fällen über alle nötigen Informationen verfügen, um die Risiken und Nachteile einer Einwilligung in ein angemessenes Verhältnis zu setzen. Häufig überwiegt aufgrund dieser Informationsasymmetrie für die Nutzenden der Vorteil, der mit „kostenlosen“ Spielen und Apps verbunden ist, die potenziellen und vom Anbieter nicht transparent dargestellten Risiken der Datenverarbeitung (ausführlich zur Einwilligung Forum Privatheit, 2020 i. E.).

Kinder wollen in ihrem medialen Handeln oft einfach bestimmte Angebote nutzen und pflegen ihre Freundschaften ohne noch zwischen „analog“ und „digital“ zu unterscheiden, wie das noch bei vorherigen Generationen der Fall war. Damit ist Privatheit von Kindern – noch stärker als bei Erwachsenen – als kontextbezogen und relational zu sehen. Je jünger und unerfahrener sie sind, desto schwieriger ist es folglich für Kinder, ihre Daten und ihre Privatsphäre selbst zu schützen und dies auch im Wissen um mögliche Folgen für sie und andere informiert und selbstbestimmt zu tun.

Einfluss- und Schutzfaktoren bei der Internetnutzung durch Kinder und Jugendliche

Wie bereits beschrieben, wird die Art und Weise, wie Kinder und Jugendliche das Internet und Soziale Medien nutzen, durch den (sozialen) Kontext beeinflusst. Hervorzuheben sind dabei Fürsorgetragende wie die Eltern (oder auch andere Erwachsene wie Lehrer*innen und Erzieher*innen) sowie die gleichaltrigen Bezugspersonen. Ein weiterer bestimmender Kontext sind die so genannten Affordances, d.h. der Angebotscharakter der Anwendungen selbst. Im Folgenden wird für jeden Bereich diskutiert, inwieweit die einzelnen Aspekte die Problematik verstärken oder auch hemmen können.

Fürsorgetragende als Einflussfaktoren

Ein starker Treiber für die generelle Internetnutzung, aber auch die Verwendung bestimmter Apps ist die Orientierung an Anderen. Im jüngeren Alter richten sich Kinder besonders an ihren Eltern und älteren Geschwistern aus. Das bedeutet, dass nicht nur das eigene Internetverhalten am Modell der Eltern und deren Umgang mit Apps wie zum Beispiel Instagram und der unbeschränkten Veröffentlichung von Familienfotos (Sharenting) ausgerichtet wird, sondern auch, dass darüber hinaus eine Habitualisierung der Anwesenheit und Nutzung von Technologien stattfindet, die notwendigerweise die Weitergabe von Daten erfordern. Das kann sich auf die Nutzung von Smart-Home-Steuerungs-Apps, den Einsatz von virtuellen Assistenten wie Alexa oder Siri sowie die Verwendung von Online-Diensten zur Strukturierung des Familienalltags (z.B. die Aufräum-App Highscore House) beziehen.

Besonders bei konkreten Verhaltensweisen haben Eltern einen hohen Einfluss: Im Sinne des Modelllernens übernehmen Kinder und Jugendliche das Verhalten der Eltern, die oft über ein umfangreicheres Wissen über Zusammenhänge und potenzielle Gefahren verfügen, das sie an die Kinder und Jugendliche vermitteln können. Allerdings ist auch von Seiten der Eltern eine Überforderung zu beobachten und eine adäquate Risikoeinschätzung der Nutzung von Apps oder Spielen und der damit verbundenen Datenverarbeitung ist aufgrund der hohen Komplexität oftmals erschwert (Kutscher & Bouillon, 2018; Manske & Knobloch, 2017). Hinzu kommt, dass auch Unterschiede im Wissensstand und Umgehen der Eltern mit dem Schutz persönlicher Daten (z.B. basierend auf sozioökonomischen Unterschieden) bedacht werden müssen, die sich dann nachfolgend auch nachteilig auf die Kompetenz der Kinder und Jugendlichen auswirken und zur Verschärfung sozialer Ungleichheiten im Rahmen einer Wissenskluft beitragen können (Paus-Hasebrink, Sinner, Prochazka & Kulterer, 2018). Generell zeigt sich, dass zum Beispiel Altersnutzungsbeschränkungen von Online-Apps und digitalen Spielen lediglich als „pädagogische Empfehlung" verstanden werden (vgl. Hajok, 2019). Das betrifft weiterführend auch die Ausdifferenzierung von Kommunikationsräumen als privat oder öffentlich; so wird beispielsweise WhatsApp im Vergleich zu Facebook häufig als stärker geschützter privater Raum wahrgenommen, obwohl auch hier Metadaten und Kontaktinformationen abfließen.

Insgesamt sind Kinder und Jugendliche heute mit omnipräsenten und vielschichtigen Medienangeboten und Technologien konfrontiert. Um diese chancenorientiert und selbstbestimmt nutzen zu können, müssen sie mit Kompetenzen und Wissen (z. B. über komplexe Trackingverfahren von Webseiten und Apps) sowie kritischer Urteilskraft zu einem reflektierten Umgang mit einhergehenden Risiken für Datensicherheit und den Schutz von persönlichen Informationen befähigt werden. Da dieses Wissen auch über Erfahrungen vertieft wird, sind Maßnahmen der Befähigung möglichst auf konkrete Kontexte ihrer Lebenswelt zu beziehen und sollten über Selbstbefähigung das Ziel selbstbestimmten Handelns verfolgen (Stapf, 2019; 2020). Ein solches Wissen sollte –

auf Basis der beschriebenen Überforderung vieler Eltern – vorrangig in den Bildungsinstitutionen, also durch Schule und Lehrer*innen, vermittelt und im familiären Kontext vertieft werden. Für diesen Bildungsauftrag sind ausreichende Ressourcen vorzusehen und die Implementierung entsprechender Kompetenzen im Bereich von Lehrerbildung und Fortbildungen sowie eine Anpassung der schulischen Curricula zu ermöglichen.

Peers als Einflussfaktoren

Weiterhin orientieren sich Kinder und vor allem Jugendliche an Gleichaltrigen. Teil der Gruppe zu sein, wird dabei als wichtiger wahrgenommen als der Schutz der eigenen Daten. Die Vorteile mit anderen online zu kommunizieren (und daraus resultierend eigene Daten zu veröffentlichen) werden direkter wahrgenommen, wohingegen Risiken wie z. B. die Vorfilterung von Informationen und Produkten, Cybermobbing oder auch ein Identitätsdiebstahl oftmals erst verspätet wahrgenommen werden (können).

Die besondere Wichtigkeit, Gruppendynamiken zu folgen und beispielsweise genauso wie Gleichaltrige bestimmte Apps (über die durch vernetzte Profile auch Verbindungen untereinander bestehen, z. B. Instagram, TikTok) zu nutzen, um Teil der Gemeinschaft als auch der online stattfindenden Interaktionen und Dialoge zu sein, stellt ein zentrales Motiv jugendlicher Mediennutzung dar. Da sich Kinder und Jugendliche noch in der Phase der Identitätsbildung befinden, hat sowohl der Einfluss anderer als auch die Relevanz sozialer Interaktionsprozesse eine höhere Wichtigkeit. Es ist zum Beispiel gemeinhin üblich, WhatsApp-Gruppen für die Kommunikation im Klassenverband zu nutzen (Rathgeb & Behrens, 2018a).

Datenschutzkritischen Applikationen stehen Kinder und Jugendliche demnach machtlos gegenüber, da eine Nichtnutzung für sie aufgrund impliziter Kommunikationsnormen im Klassenverband, Freundeskreis oder Sportverein nicht in Frage kommt und mit einer sozialen und kommunikativen Abgeschnittenheit einhergehen würde (Engels, 2018).

Gerade die noch nicht abgeschlossene Persönlichkeitsentwicklung, einhergehend mit der Festigung des Selbstkonzepts, die individuell unterschiedlich und nicht an feste Altersschritte geknüpft stattfindet, macht Kinder und Jugendliche sehr beeinflussbar, wodurch sie leicht, auf impulsive Weise und ohne kritische Reflexion von dem Nutzungsverhalten ihrer Peergroups angesteckt werden können.

In Kombination mit der alters- und erfahrungsbedingten Unwissenheit der Heranwachsenden (z. B. in Bezug auf mögliche zukünftige Konsequenzen ihrer heutigen Handlungen als auch der Langfristigkeit einiger Nutzungsentscheidungen) ist es wichtig, dass Kinder und Jugendliche in besondere Weise geschützt werden (Dreyer 2018; 2020). In diesem Kontext kommt den Prinzipen der datenschutzgerechten Gestaltung (Datenschutz by Design) und der Auswahl datenschutzfreundlicher Voreinstellungen (Datenschutz by Default) eine besondere Bedeutung zu (Bieker & Hansen, 2017). Datenschutz muss bei Anwendungen, die sich an Kinder und Jugendliche richten, vom Beginn der Entwicklung an umgesetzt werden. Zudem müssen Apps in einer Art und Weise vorkonfiguriert sein, dass nicht mehr Daten als die, die zur Erreichung des Zwecks erforderlich sind, verarbeitet werden und nur Grundfunktionen aktiviert sind. Für jede Erweiterung sollte dann eine eigene informierte Einwilligung der Nutzenden oder ihrer gesetzlichen Vertreter*innen erforderlich werden.

„Affordances" der Anwendungen als Einflussfaktor

Wie bereits angesprochen, führt der Angebotscharakter der medialen Anwendungen dazu, dass Kinder und Jugendliche geradezu zu einer ungeschützten Nutzung aufgefordert werden. So stellen die Anwendungen die Vorteile und den Belohnungswert im Sinne einer Teilhabe am sozialen Leben und der Verfügbarkeit von Information über gesellschaftlich relevante Themen durch die Art und Weise ihrer Gestaltung klar in den

Einfluss- und Schutzfaktoren bei der Internetnutzung durch Kinder und Jugendliche

Vordergrund, während potenzielle Risiken der Nutzung in den Hintergrund treten. Dies erhöht die Bereitschaft der Kinder und Jugendlichen, private Informationen zu teilen. So sind Kinder und Jugendliche gerade im Austausch gegen eine kostenlose Nutzung bestimmter Apps und Dienste bereit, persönliche Daten preiszugeben – oftmals ohne die volle Tragweite der vermeintlich harmlosen Informationsweitergabe übersehen zu können (Engels, 2018). Dies entspricht dem empirisch gut belegten Ansatz des „privacy calculus" (Culnan & Armstrong, 1999), der zeigt, dass ein kurzfristiger Nutzen häufig über langfristige (weniger überblickbare) Folgen gestellt wird. Die entsprechenden Studien beziehen sich allerdings ausschließlich auf Erwachsene und fokussieren dabei stark auf rationale Überlegungen, was dem Ansatz Kritik entgegengebracht hat. So gilt es bislang als ungeklärt und muss hinterfragt werden, ob und in welcher Weise diese rationalen Überlegungen bei Kindern überhaupt stattfinden. Hinzu kommt, dass die Anwendungen nahelegen, dass sie eigentlich privat sind (etwa ein Austausch mit Freunden auf Instagram).

Um diesen Einflussfaktor zu einem Schutzfaktor machen zu können, müssten die Anwendungen folglich so verändert werden, dass die Gefahren unmittelbar sichtbarer und damit für die Nutzer*innen einschätzbarer werden – was nicht im Sinne von Anbietern sein dürfte, deren Geschäftsmodell auf dem Sammeln und Auswerten von Daten beruht. Bereits nach der DSGVO müssen Anbieter von Anwendungen, die personenbezogene Daten verarbeiten, ohnehin über die Weitergabe von Daten transparent und in einer für die Nutzenden verständlichen Weise etwa auf die Weitergabe von Daten hinweisen. Dies kann durch so genannte Privacy Icons (Holtz, Nocun & Hansen, 2011) erreicht werden, die mit Symbolen einen Überblick über die Datenverarbeitung bieten können (Artikel 12 Abs. 7 DSGVO). In jedem Fall müssen die Anbieter im Sinne des Datenschutzes durch datenschutzfreundliche Voreinstellungen, d. h. by Default (Artikel 25 Abs. 2 DSGVO), auch sicherstellen, dass Daten der Nutzenden nicht standardmäßig mit Dritten geteilt werden oder gar öffentlich einsehbar sind. Diese Datenschutzanforderungen werden zurzeit generell häufig ignoriert, was exemplarisch in der Studie „Deceived by Design" (Kaldestad, 2018) herausgearbeitet wurde. Auf der einen Seite müssen daher die Sanktionierungsmöglichkeiten verbessert werden, auf der anderen Seite sollten der Staat und diejenigen Akteure, bei denen Anwendungen zum Einsatz kommen, auch positive Anreize dafür schaffen, dass Hersteller und Anbieter von Anfang in ihren Systemen die Datenschutz-Grundsätze, und damit auch die Transparenz über die Verarbeitung und die Risiken, einbauen (Bieker & Hansen, 2017; Datenethikkommission, 2019).

Der kinderrechtliche Ansatz mit Blick auf Privatheit

Selbst bestimmen zu können, welche persönlichen Räume andere betreten oder welche Informationen sie einsehen oder verwenden dürfen, ist ein zentrales Menschenrecht. So ist in Artikel 16 der UN-KRK verbrieft, dass „kein Kind (…) willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden" darf. Die UN-KRK verbrieft Kindern seit 1989 ausdrücklich grundlegende Rechte als Subjekte. Seit dieser völkerrechtliche Vertrag 1992 von Deutschland ratifiziert und umgesetzt wurde, gilt er als einfaches Recht. Die UN-KRK hat damit den Rang eines Bundesgesetzes und ist von allen staatlichen Stellen zu beachten. Kommt es zu einer Kollision mit einer anderen gesetzlichen Vorschrift, kommt der UN-KRK, anders als etwa den Grundrechten des Grundgesetzes, kein Vorrang zu. Allerdings können die relevanten Grundrechte – wie das Recht auf informationelle Selbstbestimmung – völkerrechtsfreundlich dahingehend ausgelegt werden, dass das kollidierende nationale Recht im Sinne der UN-KRK ausgelegt wird. Damit kommt völkerrechtlichen Verträgen, obwohl sie „nur" gleichrangig mit anderen Gesetzen gelten und keinen Vorrang genießen, in der Praxis eine erhöhte Bedeutung zu.

Im Zuge der aktuellen Diskussion einer Aufnahme von Kinderrechten ins Grundgesetz ist die Frage nach Privatheit auch in digitalen Kontexten ein zentrales politisches Thema, das Auswirkungen in unterschiedliche Lebensbereiche (von Schule bis Familie und die mediale Regulierung) haben könnte.

Daher erscheint eine kinderrechtliche Perspektive für die informationelle Selbstbestimmung von Kindern und Jugendlichen weiterführend. Entscheidend ist hierbei der Blick auf Heranwachsende als handelnde Subjekte und nicht nur Objekte des Schutzes von Fürsorgetragenden. Dies wird über die vier Grundprinzipien Recht auf Gleichbehandlung bzw. Nicht-Diskriminierung, Vorrang des Kindeswohls, Recht auf Leben und Entwicklung und Achtung vor der Meinung des Kindes angestrebt (Maywald, 2012). Den 54 Artikeln der UN-KRK ist das Kindeswohl in Artikel 3 übergeordnet: „Bei allen Maßnahmen, die Kinder betreffen, gleichviel ob sie von öffentlichen oder privaten Einrichtungen der sozialen Fürsorge, Gerichten, Verwaltungsbehörden oder Gesetzgebungsorganen getroffen werden, ist das Wohl des Kindes ein Gesichtspunkt, der vorrangig zu berücksichtigen ist."

Rechte gleichen Gehalts enthält auch das Grundgesetz, dort jedoch implizit. Sie aktivieren umfangreiche Schutzpflichten. Explizite Rechte des Kindes enthält auch die EU-Grundrechtecharta, zwar nicht in dem Umfang der UN-KRK, dafür aber auf verfassungsrechtlicher Ebene und nicht bloß im Rang eines einfachen Gesetzes. Nach Artikel 24 Abs. 1 Satz 1 GRCh haben Kinder „Anspruch auf den Schutz und die Fürsorge, die für ihr Wohlergehen notwendig sind". Außerdem gelten für Kinder auch alle anderen Grundrechte, wie das Recht auf Privatleben nach Artikel 7 GRCh und auf Datenschutz nach Artikel 8 GRCh.

Aus Sicht der Kinderrechte sind auch Fragen der Privatheit auf das Wohlergehen von Kindern ausgelegt. Kindern soll eine gute und gelingende Kindheit sowie gute Chancen und wichtige Fähigkeiten mit Blick auf ihr Erwachsenenleben eröffnet werden. Hierzu braucht es ein auf die kindlichen Fähigkeiten zugeschnittenes Zusammenspiel von Schutz-, Förderungs- und Beteiligungsrechten (Stapf, 2020).

Woran ist dieses Wohl dann auszurichten, wenn man bedenkt, dass Kindheit eine Entwicklungsphase ist? Mit Blick auf Kinder geht es darum, ihr Wohlergehen sowohl in ihrer Gegenwart, aber immer auch mit Blick auf die Entwicklungsdimension ihrer „evolving capacities" (Lansdown, 2005), auf ihre überhaupt mögliche Zukunft auszurichten. Joel Feinberg (1980) spricht hierbei von „the child's right to an open future".

Der kinderrechtliche Ansatz mit Blick auf Privatheit

Eine offene Zukunft mit Blick auf Privatheit impliziert beispielsweise eine besondere Sorgfalt im Umgang mit kindlichen Daten, ein Recht Heranwachsender auf Vergessenwerden im Netz sowie auf Datensparsamkeit mit Blick auf Datenspuren, die Kinder im Netz hinterlassen. Denn die auf Verhaltensvorhersage und -formung (predictive analytics, nudging usw.) angelegten Geschäftsmodelle der meisten kommerziell erfolgreichen Internet-Plattformen stehen dem Prinzip der offenen Zukunft diametral entgegen (Van Dijck, Poell & De Waal, 2018; Forum Privatheit 2018; Zuboff, 2019). Dies bedeutet ein erhöhtes Schutzbedürfnis von Kindern im Netz. Und es erfordert, zusammen mit den kindlichen Rechten auf Informations- und Meinungsfreiheit (Artikel 13 UN-KRK), dass Kinder aufgrund für sie verständlicher Informationen eigene Entscheidungen zum Schutz ihrer Privatheit treffen lernen können. Um dies zu ermöglichen, sind Bildungsrechte für Kinder (Artikel 28/29 UN-KRK) verbrieft. Hierzu erforderlich werden Befähigungsmaßnahmen im Elternhaus sowie systematisch in der Schule und in schulischen Einrichtungen. Dazu wird ein ebenfalls verbriefter Kinder- und Jugendschutz (Artikel 17 UN-KRK) auch in digitalen Kontexten notwendig, der den heutigen Nutzungsbedingungen wie Mobilität und Medienkonvergenz entspricht. All dies erfordert ein Spektrum positiver Angebote für Kinder im Netz. Denn Kinder sind nicht nur bereits immer früher schon im Netz unterwegs, man kann sie aufgrund der Bedingungen „mediatisierter Welten“ (Krotz & Hepp, 2012) auch weder praktisch noch sinnvoll von allen digitalen Angeboten ausschließen, bis sie selbst rechtlich einwilligen können.

Ein weiteres Querschnittsrecht von Kindern ist ihr Recht auf Beteiligung (Artikel 12 UN-KRK). Das Wohl des Kindes als Treuhänder seiner Interessen zu vertreten, ist die Aufgabe seiner Eltern (vgl. auch Artikel 24 Abs. 3 GRCh). Dem Wohl des Kindes entspricht es auch, seine Persönlichkeit zu entwickeln und zu entfalten. Dieses erfordert eine angemessene Beteiligung bezogen auf den kindlichen Entwicklungsstand: „Die Vertragsstaaten sichern dem Kind, das fähig ist, sich eine eigene Meinung zu bilden, das Recht zu, diese Meinung in allen das Kind berührenden Angelegenheiten frei zu äußern, und berücksichtigen die Meinung des Kindes angemessen und entsprechend seinem Alter und seiner Reife“ (vgl. auch Artikel 24 Abs. 1 Satz 2 und 3 GRCh, dazu mit weiteren Nachweisen Roßnagel, 2020).

Dieses Recht im Kontext des Digitalen ernst zu nehmen, umfasst Anforderungen an die Medienbildung, die Medienregulierung sowie die universitäre Forschung. Evidenzbasierte Medienforschung über Kinder, aber auch mit Kindern kann Maßnahmen ermöglichen, welche Entscheidungskompetenzen von Kindern und ihr sicheres Erlernen von Selbstschutzmechanismen fördern. Angesichts aktueller Diskussionen zur Aufnahme von Kinderrechten ins Grundgesetz darf hier ein dringender gesellschaftlicher Reflexions- und Diskussionsbedarf angenommen werden.

Spannungsfelder: Privatheit von Kindern in digitalen Kontexten

Die Privatheit von Kindern in digitalen Umwelten zu stärken und optimale Bedingungen für ihren Schutz, ihre Befähigung und ihre Teilhabe zu ermöglichen, bedarf einer Berücksichtigung der damit verbundenen Spannungsfelder und Herausforderungen in Abwägung mit möglichen Potenzialen. Über die gesetzlichen Regelungen und die unverzichtbaren Maßnahmen zur Medienbildung hinaus sollten weitere technische Voraussetzungen zum Schutz von Kindern getroffen werden. Hier werden neben neuen theoretischen Konzepten technische Innovationen ebenso notwendig wie interdisziplinäre Forschung als Grundlage von Politikgestaltung. Darüber hinaus sollten dringend auch rechtliche und technische Schutzmaßnahmen vorangetrieben werden, die insbesondere die intransparente Speicherung und Weiterverbreitung von Nutzerdaten im nationalen wie internationalen Rahmen adressieren.

- **Damit eine Einwilligung wirksam ist, müssen die relevanten Informationen verständlich dargestellt werden, es bedarf daher einer Anpassung an die Fähigkeiten und Interessen von Kindern:** Wie ist beispielsweise damit umzugehen, dass sich in der frühen Kindheit wichtige Fähigkeiten, die Voraussetzung für das Treffen selbstbestimmter Entscheidungen sind, erst entwickeln? Wie müssten Informationen zum Schutz von Daten für Kinder formuliert und visualisiert sein, um sicherzustellen, dass Kinder eine Einwilligung geben können? Wie verhält sich dies im Altersverlauf, z.B. bei noch sehr kleinen Kindern im Vergleich zu Jugendlichen kurz vor dem Erwachsenenalter?
- **Eltern- und Kinderrechte sollten im Zusammenspiel gedacht werden:** Kinderrechte umfassen auch die Pflicht zur Fürsorge durch die Eltern. Sorgeberechtigte haben die erzieherische Vermittlung zentraler Kompetenzen zu übernehmen und dabei gleichzeitig das Kind zur Wahrnehmung seiner Freiheitsrechte im digitalen Raum zu befähigen (Croll, 2019). Welche Befähigungsmaßnahmen werden dann auch für Eltern, Erziehende und Lehrende notwendig? Inwieweit können Institutionen, die Fürsorgepflichten wahrnehmen, wie z.B. Schulen datenschutzfreundliche Infrastrukturen zur Verfügung stellen? Wie lässt sich die Pflicht zur Fürsorge der Eltern mit der wachsenden Selbstbestimmung von Kindern vereinbaren mit Blick auf den dafür notwendigen Erwerb von Kompetenzen und Fähigkeiten? Inwieweit wirkt sich dies auf schulische Aufgaben und Lehrpläne oder auf die Umsetzung der Anforderungen von Datenschutz insgesamt und von speziell von Datenschutz by Design & by Default aus?
- **Schutz-, Beteiligungs- und Befähigungsrechte greifen ineinander, können aber auch zu Spannungsfeldern führen:** Alle Kinderrechte gelten grundsätzlich gleichwertig. Grundsätzlich könnten anzustrebende Schutzmaßnahmen sinnvoll mit Befähigungs-, aber auch mit Beteiligungsmaßnahmen verbunden werden, da dies vor allem für ältere Kinder zu Selbstschutzmaßnahmen führen kann und Kinder dies auch als Wunsch artikulieren (Frense, 2020). Verschiedene Kinderrechte stehen aber oft auch im Widerspruch zueinander. So führen erhöhte Beteiligung (Artikel 12 UN-KRK) oder Meinungsäußerung (Artikel 13 UN-KRK) auch zu erhöhten Gefahren mit Blick auf kindliche Schutzrechte, wie bei Hate Speech, Cybermobbing oder der erhöhten Preisgabe von Daten. Im rechtlichen Konfliktfall kommen hier auf grundrechtlicher Ebene Verfahren der praktischen Konkordanz zum Tragen. Wie können solche Konfliktlinien jedoch schon präventiv im Jugendmedienschutz sinnvoll aufgegriffen werden? Wie lässt sich dies in der Regulierungspraxis ausgestalten und in der Medienbildung zugrunde legen?

Spannungsfelder: Privatheit von Kindern in digitalen Kontexten

- **Spannungsfelder zwischen den Generationen:** Kinder, die aktuell in mediatisierten Lebenswelten aufwachsen, entwickeln in ihrer gelebten Praxis ein anderes und sich wandelndes Verständnis von Privatheit. Wie kann Privatheit als wichtiger Wert für die freiheitliche Demokratie an die jetzt aufwachsende Generation vermittelt werden? Wie ist damit umzugehen, dass Kinder oft kompetenter in der Techniknutzung und nicht selten auch bezogen auf das Technikverständnis sind als ihre Eltern? Wie sind beispielsweise Klassenchats mittels Messenger-Diensten in der Schule zu bewerten, die unter der DSGVO-Altersgrenze von 16 liegen und der Einwilligung der Eltern bedürften? Und was folgt daraus für die Verantwortungsübernahme hinsichtlich der Beurteilung möglicher Konsequenzen der Techniknutzung und des Handelns im digitalen Umfeld?
- **Herausforderungen im Kontext der Kommerzialisierung von Kindheit:** Wie lassen sich Forderungen an positive Angebote stellen und Anreizsysteme auf einem zunehmend kommerziell durchdrungenen globalen Markt etablieren? Die Nichtnutzung digitalisierter Technologien ist keine wirkliche Alternative, vielmehr sollten Ansätze zur Befähigung von Kindern, Jugendlichen und den für sie verantwortlichen Personen dazu führen, dass informierte Entscheidungen zur Wahrung der informationellen Selbstbestimmung getroffen werden können. Um eine Überforderung zu vermeiden und Schutzansprüche nicht zu individualisieren (Karaboga et al., 2014), ist es gleichzeitig ebenso wichtig, Kindern ein sicheres digitales Kommunikationsumfeld zu bieten, in dem Einschränkungen - bis hin zum Verbot - der kommerziellen Verwertung der Daten von Kindern und restriktive Löschungsvorgaben Standard sind. Und wie könnte eine auf der Analyse von Nutzungsdaten von Kindern basierende Produktentwicklung so reguliert werden, dass der Schutz vor wirtschaftlicher Ausbeutung über Artikel 32 der UN-KRK über gezielt auf die kindlichen Bedürfnisse ausgerichtete Kauf- und Nutzungsanreize gewährleistet wird?

Fazit und Empfehlungen

Die folgenden Empfehlungen verstehen sich als ein erster Impuls, um die politische und gesellschaftliche Diskussion zum Thema Privatheit und Kinder voranzutreiben:

1. Die Privatheit von Kindern ist auch im Digitalen ein verbrieftes Kinderrecht

Selbst bestimmen zu dürfen, welche Räume andere betreten oder welche Informationen sie einsehen oder verwenden dürfen, ist ein Menschenrecht. So ist auch in Artikel 16 der UN-KRK verbrieft, dass „kein Kind (…) willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden" darf. Die UN-Kinderrechtskonvention als völkerrechtlicher Vertrag garantiert Kindern seit 1989 grundlegende Rechte als Subjekte. Seit sie 1992 von Deutschland ratifiziert und umgesetzt wurde, muss sie auch hier bei der Auslegung nationalen Rechts Berücksichtigung finden. Den durch das Grundgesetz, die EU-Grundrechtecharta und die Europäische Menschenrechtskonvention verbrieften Rechten von Kindern muss zu stärkerer Durchsetzung und praktischer Relevanz im Bereich der Nutzung digitaler Technik verholfen werden. Auch im Zuge der aktuellen Diskussion über eine Aufnahme von Kinderrechten ins Grundgesetz ist dies ein zentrales politisches Thema. Dem Grundgesetz fehlt in seiner derzeitigen Fassung die explizite Aussage, dass der Schutz der in seinen Katalog von Grundrechten aufgenommenen Rechte bei Kindern andere Dimensionen haben kann als dies bei Erwachsenen der Fall ist, wenngleich dies allgemein akzeptiert ist. Dem stehen aktuelle Durchsetzungsdefizite bezogen auf grundrechtlich geforderten Schutz im Rahmen der Digitalisierung gegenüber, die zwar allgemein auch für Erwachsene gelten, für Kinder aufgrund erhöhter Vulnerabilität allerdings stärker wirksam werden könnten.

2. Mit der Sicherung kindlicher Privatheit ist das Recht des Kindes auf eine offene Zukunft verbunden

Aus Sicht der Kinderrechte sind Fragen der informationellen Selbstbestimmung und Privatheit auf das Wohlergehen von Kindern ausgelegt. Es geht darum, Kindern eine gute und gelingende Kindheit und gute Chancen und wichtige Fähigkeiten mit Blick auf ihr Erwachsenenleben zu eröffnen. Darunter fällt es auch, Kindern ein Recht auf eine offene Zukunft zu gewährleisten. Anbieter sollten verpflichten werden, neu zu schaffende rechtliche und technische Standards einzuhalten. Dazu könnten Vorschriften gehören, dass Kinder grundsätzlich von personalisierter Werbung und Tracking ausgenommen werden müssen; oder ein Verbot von Profilbildung bei Kindern. Ein weiterer Vorschlag ist die Auflage, in sensiblen Kontexten gewonnene Daten über Kinder regelmäßig zu löschen, sofern dem nicht Kindeswohlinteressen entgegenstehen. Damit verbunden wären verschärfte Anforderungen an die Datenminimierung und ein deutlich über Artikel 17 DSGVO hinausgehendes, echtes Recht Heranwachsender auf Vergessenwerden im Netz, so auch z. B. alle im Rahmen einer Bildungs-App gewonnenen Daten, sobald das Kind die Schule verlässt, kombiniert mit einem Weitergabeverbot während der Nutzungsdauer. Entgegenstehende Kindeswohlinteressen, die für eine andauernde Speicherung auch sensibler Daten von Kindern sprechen, können etwa am Erhalt von Untersuchungsergebnissen bestehen, die Missbrauch dokumentieren.

Die Berücksichtigung der besonderen Schutzinteressen im Umgang mit kindlichen Daten impliziert außerdem den grundsätzlichen Ausschluss der Einwilligung durch Kinder in die Verarbeitung besonderer Kategorien personenbezogener Daten. Ausnahmen sind nur in solchen Fällen denkbar, in denen es um höchstpersönliche Sachverhalte, etwa die Intim- und Geheimsphäre des Kindes, geht, die auch gegenüber den Sorgeberechtigten geschützt ist. Dies gilt etwa im Rahmen der Beratung in einer Not- oder Konfliktlage gemäß § 8 Abs. 3 SGB VIII, bei der sensible Daten ohne Kenntnis der Per-

sonensorgeberechtigten erhoben, sowie überdies die Aufnahme einer Verpflichtung zur Berücksichtigung des Verständnisvermögens und der Hilfsbedürftigkeit von Kindern bezogen auf Form und Inhalt der Benachrichtigung nach einer Schutzverletzung und auch die Berücksichtigung der Grundrechte und Interessen von Kindern bei der Risikoanalyse und bei der Festlegung von Schutzmaßnahmen in der Datenschutz-Folgenabschätzung (ausführlich Roßnagel, 2020; s. zu konkreten Vorschlägen Roßnagel & Geminn, 2020).

3. Maßnahmen zum Schutz von Kindern müssen stets von Befähigungsmaßnahmen begleitet werden

Sowohl Staat, Schule als auch Eltern sollten Medienerziehung und Medienbildung vorantreiben, indem sie Kinder über ihre Privatheitsrechte informieren. Dazu sollten Kinder zunächst die verschiedenen Formen von Privatheit in digitalen Kontexten kennen und auch lernen, diese selbst anzupassen. Bereits in jungen Jahren brauchen Kinder Eltern, Erziehende und Lehrende, die im Bereich Medienbildung kompetent sind. Der Digitalpakt der Bundesregierung sollte daher neben der Anschaffung datenschutzkonformer Hard- und Software (Datenschutz by Design & Default) und der Bereitstellung entsprechender Infrastrukturen auch die didaktische und pädagogische Förderung digitaler Kompetenzen in Erziehungs- und Bildungseinrichtungen im Blick haben. Ziel dabei wäre es, dass Kinder selbst informierte Entscheidungen treffen können und für sie verständliche, transparente Informationen erhalten.

4. Anreizsysteme für Datenschutz by Design & by Default bei Plattformbetreibern, Unternehmen und Bildungseinrichtungen sollten staatlich gefördert werden

Selbstbestimmung im Digitalen sollte der Standard sein - und nicht erst von Seiten der Nutzenden aktiv über Privacy-Einstellungen aktiviert werden müssen. Dies ist besonders wichtig, wenn sich Angebote auch an Kinder richten oder von Kindern genutzt werden. Es muss für Kinder selbst zumindest verständlich und anpassbar sein, in welchem Kontext von Privatheit und Öffentlichkeit sie sich jeweils befinden und dies muss für sie einfach während der Benutzung einfach erkennbar sein, z. B. über auditive Mitteilungen oder Rückmeldungen („Wenn Du das abschickst, können es alle Menschen sehen, die das gleiche Angebot nutzen) oder über visuelle Gestaltung. Bei den Inhalten und der Art und Weise der Hinweise ist aber darauf zu achten, dass sie nicht verstörend wirken oder zu anderen negativen Effekten führen, etwa, weil die Kinder davon ausgehen, dass in jeder Risikosituation eine Mitteilung erscheint. Die Selbstbestimmung von Kindern im Digitalen sollte bereits bei der Konzeption digitaler Angebote berücksichtigt werden. Unternehmen sollten staatliche Anreizsysteme vorfinden, sodass für sie der Einbau von Datenschutz by Design & by Default am Ende Wettbewerbsvorteil und nicht -nachteil ist.

5. Die Digitalisierung entwickelt sich rasant. Privatheit und Datenschutz als die Demokratie sichernde Menschenrechte zu gewährleisten, bedarf gesamtgesellschaftlicher, interdisziplinärer und kontextsensibler Ansätze

Die Möglichkeit zu entscheiden, welche Informationen in bestimmten Kontexten oder mit bestimmten Personen geteilt werden und welche nicht, ist mit weiteren kindlichen Grundrechten verknüpft. Sie ist grundlegend für persönliche Autonomie und Menschenwürde. Damit ermöglicht Privatheit erst viele Aktivitäten und Strukturen einer demokratischen Gesellschaft. Sie ist ein Kernthema freiheitlicher Demokratien im Zuge der Digitalisierung. Zu erkennen, wie Heranwachsende Privatheit heute im Digitalen erleben, verstehen und wie sich dies im Altersverlauf entwickelt ist ein Desiderat aktueller und zukünftiger Forschung.

Notwendig hierzu ist ein „holistic child-rights-oriented approach“ (Milkaite & Lievens, 2019), in dem beispielsweise neue rechtliche oder Regulierungsmaßnahmen mit Blick auf ihre Auswirkung auf das gesamte Spektrum von Kinderrechten beurteilt und diese

systematisch mitgedacht werden. Um dies voranzubringen, braucht es interdisziplinär ansetzende Langzeitstudien, auch unter Beteiligung von Kindern und Jugendlichen, inklusive Partizipationsformen für Kinder auch bei der Gestaltung von Maßnahmen, innovative technische Ansätze, gesellschaftliche Diskurse und einen zukunftsfähigen und flexiblen Kinder- und Jugendmedienschutz.

Literatur und Ressourcen

Literatur

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

Baruh, L., Secinti, E. & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication, 67(1), 26-53.

Bieker, F. & Hansen, M. (2017). Datenschutz "by Design" und "by Default" nach der neuen europäischen Datenschutz-Grundverordnung, RDV, 4, 165-170.

Borgstedt, S., Roden, I., Borchard, I., Rätz, B. & Ernst, S. (2014). DIVSI U25-Studie: Kinder, Jugendliche und junge Erwachsene in der digitalen Welt. SINUS Institut Heidelberg. 1-175.

Brüggen, N., Dreyer, S., Gebel, C., Lauber, A., Müller, R. & Stecher, S. (2019). Gefährdungsatlas. Digitales Aufwachsen. Vom Kind aus denken. Zukunftssicher handeln. Bundesprüfstelle für jugendgefährdende Medien.

Croll, J. (2019). Das Recht des Kindes auf Privatsphäre in einer digitalisierten Lebenswelt. Frühe Kindheit, 2(19), 24-31.

Culnan, M. J. & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science, 10(1), 104-115.

Datenethikkommission der Bundesregierung (2019). Gutachten der Datenethikkommission. Oktober 2019. datenethikkommission. https://datenethikkommission.de/

Dienlin, T. & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European journal of social psychology, 45(3), 285-297.

Dreyer, S. (2018). On the Internet, nobody knows you're a kid. Zur (Nicht-)Erkennbarkeit Minderjähriger in digitalen Medienumgebungen. merzWissenschaft. 65-78.

Dreyer, S. (2020). Recht auf mein Selbst – Schutzräume kindlicher Entwicklungsphasen in der digitalen Gesellschaft. Aufwachsen in überwachten Umgebungen. Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend.

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

Fahlquist, J. N. (2015). Responsibility and privacy - ethical aspects of using GPS to track children. Children & Society, 29(1), 38-47.

Feinberg, J. (1980). The child's right to an open future in whose child. Childrens' rights, parental authority, and state power, 123-153.

Forum Privatheit (2018). Tracking. Beschreibung und Bewertung neuer Methoden. White Paper, hg. v. Michael Friedewald, Regina Ammicht Quinn, Thilo Hagendorff, Marit Hansen, Jessica Heesen, Thomas Hess, Nicole Krämer, Jörn Lamla, Christian Matt, Alexander Roßnagel, Michael Waidner, Schriftenreihe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Creative Commons 2018.

Forum Privatheit (2020): Einwilligung. Ein Forschungsbericht. Karlsruhe, im Erscheinen.

Frense, E. (2020). Partizipativer Jugendmedienschutz. Anforderungen an einen zeitgemäßen Jugendmedienschutz aus Perspektive von Kindern und Jugendlichen. Wochenschau Verlag.

Geminn, C. & Roßnagel, A. (2015). „Privatheit" und, „Privatsphäre" aus der Perspektive des Rechts - ein Überblick. JuristenZeitung, 70(14), 703-708.

Genner, S. & Süss, D. (2017). Socialization as media effect. The international encyclopedia of media effects, 1-15.

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

Heeg, R., Genner, S., Steiner, O., Schmid, M., Suter, L. & Süss, D. (2018). Generation Smartphone. Ein partizipatives Forschungsprojekt mit Jugendlichen. Generation Smartphone. http://www.generationsmartphone.ch./

Holtz, L. E., Nocun, K. & Hansen, M. (2010). Towards displaying privacy information with icons. IFIP PrimeLife International Summer School on Privacy and Identity Management for Life, 338-348.

Kaldestad, Ø., H. (2018). Report: Deceived by Design. Forbrukerrådet. https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

Karaboga, M., Schütz, P., Friedewald, M., Zoche, P., Matzner, T., Mothes, C., Nebel, M., Ochs, C. & Simo Fhom, H. (2014). Selbstdatenschutz. White Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forum-privatheit.de/download/selbstdatenschutz-2-auflage-2014/

Krotz, F. & Hepp, A. (2012). Mediatisierte Welten: Forschungsfelder und Beschreibungsansätze. Springer-Verlag.

Kutscher, N. (2012). Medienbildung in der Kindheit. MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung, 22, 1-16.

Kutscher, N. & Bouillon, R. (2018). Kinder. Bilder. Rechte. Persönlichkeitsrechte von Kindern im Kontext der digitalen Mediennutzung in der Familie. Schriftenreihe des Deutschen Kinderhilfswerkes e. V., 4. 1-97.

Lansdown, G. (2005). The evolving capacities of the child. Innocentil Insights, 5(18).

Livingstone, S., Stoilova, M. & Nandagiri, R. (2019). Children's data and privacy online: growing up in a digital age: an evidence review. London School of Economics and Political Science: London, UK, 2019.

Lupton, D. & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. New Media & Society, 19(5), 780-794.

Manske, J. & Knobloch, T. (2017). Datenpolitik jenseits von Datenschutz. Stiftung Neue Verantwortung. 1-97

Mascheroni, G., Jorge, A. & Farrugia, L. (2014). Media representations and children's discourses on online risks: Findings from qualitative research in nine European countries. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8(2).

Matzner, T., Masur, P. K., Ochs, C. & von Pape, T. (2016). Do-It-Yourself Data Protection—Empowerment or Burden?. Data protection on the move, 277-305.

Maywald, J. (2012). Kinder haben Rechte!: Kinderrechte kennen-umsetzen-wahren. Für Kindergarten, Schule und Jugendhilfe (0-18 Jahre). Weinheim: Beltz.

Milkaite, I. & Lievens, E. (2019). Children's rights to privacy and data protecton around the world: challenges in the digital realm. European Journal of Law and Technology, 10(1).

Monllos, K. (2019). As TikTok's popularity rises, buyers say the ad team needs to grow to keep up. DIGIDAY. https://digiday.com/marketing/tiktok-popularity-rises-buyers-say-ad-team-needs-grow-keep/

Naplavova, M., Ludik, T., Hruza, P. & Bozek, F. (2014). General Awareness of Teenagers in Information Security. International Journal of Information and Communication Engineering, 8(11), 3552-3555.

Nebel, M. (2015). Schutz der Persönlichkeit - Privatheit oder Selbstbestimmung, Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht. Zeitschrift für Datenschutz, 517-522.

Norberg, P. A., Horne, D. R. & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs, 41(1), 100-126.

Paus-Hasebrink, I., Sinner, P., Prochazka, F. & Kulterer, J. (2018). Auswertungsstrategien für qualitative Langzeitdaten: Das Beispiel einer Langzeitstudie zur Rolle von Medien in der Sozialisation Heranwachsender. Auswertung qualitativer Daten, 209-225.

Piaget, J. (1972). Intellectual evolution from adolescence to adulthood. Human development, 15(1), 1-12.

Powell, K. (2006). Neurodevelopment: How does the teenage brain work? Nature, 442, 865–867.

Prinzing, M. (2019). Eingeboren? Oder nur eingewandert ins Digitale? Warum die Abkehr vom Mythos einer Generation von Digital Natives Voraussetzung einer verantwortungsorientierten Bildungs- und Gesellschaftspolitik ist. Aufwachsen mit Medien. Zur Ethik mediatisierter Kindheit und Jugend, 283-295.

Rathgeb, T. & Behrens, P. (2018a). JIM-Studie 2018. Jugendliche, Information, Medien. Basisuntersuchung zum Medienumgang Zwölf-bis 19-Jähriger. Medienpädagogischer Forschungsverbund Südwest.

Rathgeb, T. & Behrens, P. (2018b). KIM-Studie 2018. Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang Sechs-bis 13-Jähriger. Medienpädagogischer Forschungsverbund Südwest.

Roßnagel, A. (2020). Der Datenschutz von Kindern in der DS-GVO. Zeitschrift für Datenschutz, 88-92.

Roßnagel, A. & Geminn, C. (2020). Datenschutz-Grundverordnung verbessern! –

Änderungsvorschläge aus Sicht der Verbraucher. Datenschutz und Datensicherheit-DuD. 44, 287-292.

Stapf, I. (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. frühe Kindheit, 2(19), 12-25.

Stapf, I. (2020). Aufwachsen in überwachten Umgebungen: Medienethische Überlegungen zum Kinderrecht auf Privatsphäre im Zeitalter des Digitalen. Aufwachsen in überwachten Umgebungen – Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. Journalism & Mass Communication Quarterly, 93(2), 296-311.

Tillmann, A. & Hugger, K. U. (2014). Mediatisierte Kindheit–Aufwachsen in mediatisierten Lebenswelten. Handbuch Kinder und Medien, 31-45.

Van Dijck, J., Poell, T. & De Waal, M. (2018). The platform society: Public values in a connective world. Oxford University Press.

Wang, X., Shi, W., Kim, R., Oh, Y., Yang, S., Zhang, J. & Yu, Z. (2019). Persuasion for Good: Towards a Personalized Persuasive Dialogue System for Social Good. arXiv preprint arXiv:1906.06725.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.

Exemplarische Ressourcen und Initiativen

Im deutschsprachigen Raum

- https://www.forum-privatheit.de/jahreskonferenz-2019/
- Dokumentation der Jahrestagung des Forum Privatheit 2019: https://www.forum-privatheit.de/jahreskonferenz-2019/g des Forum Privatheit 2019
- https://www.klicksafe.de/ speziell zur Privatheit: https://www.klicksafe.de/themen/datenschutz/privatsphaere/ und Datenschutz: https://www.klicksafe.de/themen/datenschutz/

Im internationalen Raum

- Richtlinien des Europarats zu Kinderrechten in digitalen Umwelten: http://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a
- Aktuelle Studien zu Privatheit von Kindern: http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline
- Ein Toolkit für Kinder, Erziehende, Eltern und Policy Maker: http://www.lse.ac.uk/my-privacy-uk
- Plattform für ein besseres Internet für Kinder zum Austausch von Wissen, Expertise und Best Practice: https://www.betterinternetforkids.eu/
- Non-Profit-Organisation zur Stärkung der Sicherheit von Kindern im Internet: https://www.childnet.com/
- Industry Toolkit von UNICEF (2018): https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein