Der SIKID-Kompass:

Sicherheit von Kindern in der digitalen Welt im Akteursnetzwerk ermöglichen

Arbeitspapier des BMBF-Projekts SIKID – Sicherheit für Kinder in der digitalen Welt

November 2024

SIKID
Sicherheit für Kinder in der digitalen Welt

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Der SIKID-Kompass wurde auf Grundlage der Projektergebnisse entwickelt, die in der interdisziplinären Zusammenarbeit seit 2021 entstanden sind. Er zeigt Handlungsfelder und -optionen für die Steigerung der Sicherheit im Zusammenspiel von Schutz, Teilhabe und Befähigung von Kindern in digitalen Umwelten auf. Sicherheit wird als ein Kinderrecht auch in digitalen Umgebungen verstanden, für die ein breites Akteursnetzwerk Verantwortung trägt. Im Zentrum stehen Interaktionsrisiken wie Cybergrooming, Cybermobbing, Hate Speech und non-konsensuales Sexting.

SIKID ist ein Verbundprojekt der Universität Tübingen, der TU Berlin und des Leibniz-Instituts für Medienforschung | Hans-Bredow-Institut, gefördert vom Bundesministerium für Bildung und Forschung unter der Fördernummer 13N15884.

Förderzeitraum: September 2021 – Dezember 2024

Autorinnen und Autoren: Ingrid Stapf, Laura Schelenz, Stephan Dreyer, Jan Pfetsch, Claudia Lampert, Sünje Andresen, Felix Paschel, Kira Thiel, Neda Wysocki, Sonja Pfisterer, Jessica Heesen

Layout und grafische Gestaltung: Sonja Pfisterer

Materialien zur Ethik in den Wissenschaften
Band 25

Herausgegeben vom
Internationalen Zentrum für Ethik in den Wissenschaften (IZEW)
Universität Tübingen 2024

ISBN: 978-3-935933-22-3

Inhaltsverzeichnis

TEIL I: Grundlagen und Ergebnisse

1. Einführung: Hintergrund und Ziele des Projekts SIKID

Das Projekt „SIKID – Sicherheit für Kinder in der digitalen Welt" hat das Ziel, die Sicherheit von Kindern im digitalen Raum zu erhöhen, indem es Akteure vernetzt, Regulierung verbessert und Kinderrechte stärkt. Das BMBF-geförderte Forschungsprojekt setzt sich aus ethischer, rechtlicher, psychologischer und kommunikationswissenschaftlicher Perspektive interdisziplinär mit den Interaktionsrisiken für Kinder bei der Nutzung des Internets und digitaler Technologien auseinander. Wichtig ist neben dem Schutz auch die Befähigung von Kindern und Jugendlichen. Heranwachsende sollten über partizipative Methoden an ihrem eigenen Schutz und ihrer Befähigung aktiv mitwirken, etwa bei der Entwicklung und Gestaltung von Anbietermaßnahmen auf digitalen Plattformen. Zu den Arbeitsergebnissen des SIKID-Projekts gehören konzeptuelle Entwürfe, Fachpublikationen, Methoden und Leitfäden, empirische Studien und Handlungsoptionen sowie die Vernetzung und der Austausch mit Expert:innen aus Politik, Recht, Strafverfolgung, Regulierung, Wissenschaft, Zivilgesellschaft, dem Anbieter- und dem Medienbildungsbereich. Projektergebnisse und Publikationen finden sich auf der Webseite https://sikid.de/.

Der SIKID-Kompass wurde auf Grundlage der Projektergebnisse entwickelt, die im vorliegenden Papier vorgestellt werden. Er zeigt Handlungsfelder und Handlungsoptionen für die Steigerung der Sicherheit und Befähigung von Kindern in digitalen Umwelten auf. Dabei steht Sicherheit als Kinderrecht (im Kontext von Teilhabe und Befähigung) im Vordergrund (Teil I). Die Handlungsoptionen basieren auf drei Jahren der interdisziplinären Forschung (siehe Teil II und III), der Konsultation von ausgewiesenen Expert:innen im Kinder- und Jugendmedienschutz sowie weiteren Stakeholdern aus Wirtschaft, Recht und Politik in zwei Workshops (2022 und 2024). Sie adressieren die Breite und Komplexität des Akteursnetzwerks, bestehend aus Politik und Recht, Sicherheitsbehörden, Forschung und Wissenschaft, der Zivilgesellschaft, den Anbietern, aber auch dem Bildungsbereich, welches modellhaft für die Sicherheit von Kindern in der digitalen Welt integriert und als Schaubild veranschaulicht wird (siehe Kapitel 5).[1] Leitend war dabei die Maxime, Maßnahmen zur Verbesserung der Sicherheit und Befähigung von Kindern in digitalen Kontexten inter- und transdisziplinär und im Netzwerk zu denken. Dies kennzeichnet das SIKID-Projekt als Forschungsansatz und eigenen Multiplikator für die Praxis, der stets im Austausch mit und als Teil des Akteursnetzwerks für die Sicherheit von Kindern im Digitalen agiert. Über die hier dargelegten Konzepte, Modelle und Vorschläge zur Verbesserung von Sicherheit für Kinder in der digitalen Welt sollen Impulse für weiterführende Diskurse und insbesondere für praktische Maßnahmen gesetzt werden.

[1] Im Kompass finden sich verschiedene Kategorisierungen relevanter Akteursgruppen. So hat die Netzwerkanalyse der Projektpartner am Leibniz-Institut für Medienforschung | Hans-Bredow-Institut auf den bestehenden Rechtsrahmen und dort angelegte Stakeholdergruppen und Kooperationsbeziehungen rekurriert. Im ethischen Zugang wurde darauf geblickt, wo sich Akteure darüber hinaus als verantwortlich wahrnehmen bzw. welche Kooperationen im Themenfeld bestehen sollten. Das Akteursnetz wurde stetig und insbesondere im Zuge der Erkenntnisse aus den zwei Workshops 2022 und 2024 erweitert.

2. Grundlagen: Sicherheit als ein Kinderrecht auch im Digitalen

Der Blick auf Sicherheit führt aus kinderrechtlicher Perspektive zu neuen Fragestellungen, Zugangsweisen zu Problemlagen, aber auch einer differenzierten Konzeptionalisierung des Sicherheitsbegriffs. In einem ersten Schritt wird daher zusammengefasst herausgearbeitet, was einen kinderrechtlichen Ansatz ausmachen kann und welche normativen Dimensionen sich daraus ergeben.

Sicherheit als ein Recht von Kindern gilt auch im Digitalen. Zwar ist Sicherheit kein eigenes Kinderrecht, aber es wird von verschiedenen Schutzrechten in der Kinderrechtskonvention der Vereinten Nationen (UN-KRK) umfasst. Sicherheit für Individuen sowie die Gesellschaft zu ermöglichen, ist kein „Luxusgut", sondern ein Kernziel freiheitlicher Demokratien. Nicht nur ist Sicherheit – und das Gefühl von Sicherheit – wesentlich für die Lebensqualität und das (mögliche) Handeln der Bürger:innen in Freiheit und Autonomie. Sicherheit ist darüber hinaus auch die Grundlage zur Verwirklichung vieler anderer Menschen- und Grundrechte. Und das bereits in der Lebensphase Kindheit.

Im Projekt SIKID wurde daher erstmals ein **kinderrechtlicher Ansatz im Forschungskontext der zivilen Sicherheitsforschung** zugrunde gelegt. Erarbeitet wurde, dass Sicherheit ein grundlegendes „Basis-Kinderrecht" ist und eine kinderrechtliche Perspektive auf Sicherheit viele Potenziale im Sicherheitsbereich insgesamt bietet. Denn in einem hochdynamischen Feld Sicherheit zu gewährleisten impliziert, den Fokus weg von bewahrpädagogischen Verhinderungsmaßnahmen hin zur Frage einer schützenden Befähigung zu erweitern. Gerade bei Sicherheitsrisiken im digitalen Umfeld werden neben einem **umfassenden Schutz** daher auch Beteiligung und vor allem Befähigungsmaßnahmen wesentlich. **Befähigung** kann bei den hier fokussierten Interaktionsrisiken als eine **„Sicherheitsressource"** verstanden werden. **Beteiligung** impliziert, Kinder als Expert:innen ihrer Lebenswelt angemessen auch in die Forschung, Regulierung, Technikgestaltung und Entwicklung von Maßnahmen einzubeziehen.

Im **Kontext mediatisierter Kindheit** (Tillmann & Hugger 2014) oder gar der **Digitalität** (Stalder 2016) **verschränken sich nicht nur die Lebenswelten online und offline, sondern auch die zivilen Sicherheitsgefährdungen.** Dies betrifft nicht nur Erwachsene, sondern zunehmend auch Minderjährige und zeigt sich vor allem bei Interaktionsrisiken in Online-Umgebungen.

Online-Risiken umfassen verschiedene Formen von Gefährdungen. Differenziert werden die sogenannten *4Cs of online risks of harm* (Livingstone & Stoilova 2021), d.h. „content, contact, conduct and contract risks". Es bestehen also Risiken in Bezug auf Inhalte und Vertragsabschlüsse, insbesondere bestehen aber auch Risiken, die unmittelbar aus den Kontakten und dem Verhalten von jungen Menschen online resultieren. Diese Interaktionsrisiken werden als relational verstanden, indem sie aus der „dynamic interaction between the child's agency and the agency of others operating in the digital environment" erwachsen (Livingstone & Stoilova 2021, S. 10). Mit dem Aufkommen interaktiver Online-Angebote haben sich die Nutzungsmöglichkeiten digitaler Medien für Heranwachsende deutlich erweitert und ausdifferenziert (Hasebrink, Lampert & Thiel 2019; Thiel & Lampert 2023). Neben Unterhaltungsangeboten sind es vor allem Online-Dienste wie Messenger-Apps und Social-Media-Plattformen, die junge User faszinieren. Bereits im Grundschulalter zählt das Verschicken von WhatsApp-Nachrichten zu den häufigsten Tätigkeiten im Internet bzw. am Smartphone (Feierabend et

al. 2023a, S. 40-42). Im Medienalltag schon jüngerer Kinder gewinnen zunehmend auch soziale Netzwerke, voran Instagram, Snapchat und TikTok an Bedeutung (Feierabend et al. 2023a; Cousseran et al. 2021).

Interaktive Online-Angebote wie diese bieten Heranwachsenden allerdings nicht nur Teilhabemöglichkeiten und individuelle Entfaltungsmöglichkeiten (Livingstone & Haddon 2009), sondern gehen auch mit neuen Risiken einher, die eine unbeeinträchtigte Persönlichkeitsentwicklung und -entfaltung im Sinne des Jugendschutzgesetzes gefährden können. Das betrifft insbesondere sogenannte **Online-Interaktionsrisiken**. Diese umfassen Phänomene wie Cybermobbing, Grooming oder Hate Speech und können verstanden werden als „Potenziale für negative Folgen, die sich aus digital vermittelter sozialer Interaktion ergeben" (Dreyer et al. 2022, S. 2).

Cybergrooming

Aktuelle Zahlen belegen, dass die Sicherheit von Kindern in digitalen Umgebungen keine Selbstverständlichkeit ist: Die aktuelle Polizeiliche Kriminalstatistik (PKS) 2023 (BMI 2024) belegt, dass Missbrauchsdarstellungen von Kindern und Jugendpornografie (im Hellfeld) im Vergleich zum Vorjahr von 48.821 um 5.221 auf 54.042 Fälle gestiegen sind. Gleichzeitig besaßen immer mehr Kinder und Jugendliche selbst Missbrauchsdarstellungen von Kindern und jugendpornografische Inhalte. So ermittelte die Polizei insgesamt 5.581 Kinder als Tatverdächtige, die im Verdacht standen, Missbrauchsdarstellungen zu besitzen, herzustellen, zu erwerben oder über Soziale Medien weiterzuverbreiten. Bei jugendpornografischen Inhalten wurden insgesamt 516 verdächtige Kinder ermittelt.[2] Laut der JIM-Studie 2023 (Feierabend et al. 2023b) wurden 30% der Jugendlichen im Netz schon sexuell belästigt (vorwiegend auf Plattformen wie Instagram, TikTok und Snapchat), teilweise sogar regelmäßig. Und weitere Interaktionsrisiken, wie Hate Speech, Cybermobbing und non-konsensuales Sexting sind Teil der Alltagserfahrungen. Aktuelle Zahlen einer Befragung der Landesanstalt für Medien NRW (2024) betonen überdies, dass es gerade die Anonymität des Internets potenziellen Täter:innen leicht macht, sich Kindern und Jugendlichen unbemerkt zu nähern und ihr Vertrauen zu erschleichen. Dabei ist es eine verbreitete Strategie von Täter:innen, dass sie ihr wahres Alter erst zu erkennen geben, wenn sie bereits das Vertrauen des Kindes gewonnen haben. Jedes vierte Kind (25 %) hält den Kontakt aufrecht, nachdem es herausfindet, dass sein Chatpartner bereits erwachsen ist. Als Motive dafür werden vor allem die entgegengebrachte Wertschätzung (45 %), die Freude über das Interesse von Älteren an der eigenen Person (38 %) und die Neugierde, schauen zu wollen, was passieren würde (31 %), angegeben. Viele Kinder (31 %) haben noch nie über Cybergrooming gesprochen. Besonders jüngere Kinder haben sich bisher weder mit Eltern oder Lehrkräften, noch mit Gleichaltrigen über die Gefahren durch Cybergrooming ausgetauscht. Unter den 8- bis 9-Jährigen sind dies mit 45 Prozent beinahe die Hälfte der Befragten.

Cybergrooming als ein beispielhaftes **Gefährdungsszenario** zeigt die starke Verflechtung kindlicher Lebenswelten mit digitalem Handeln und Erleben. So kann digital vermittelte Sexualität einerseits Entwicklungspotenziale und Erprobungsmöglichkeiten in der Adoleszenz

[2] Anzumerken ist, dass die polizeiliche Kriminalstatistik in ihrer Aussagekraft begrenzt ist. Sie kann hier trotz dessen zeigen, welche Brisanz das Thema der Missbrauchsdarstellungen unter Minderjährigen hat (zur Aussagekraft der PKS siehe Cramer & Mischkowitz 2013).

bieten. Denn sexuelle Selbstbestimmung und sozio-moralische Kompetenzen in Beziehungen entfalten sich im Zuge sich noch entwickelnder Fähigkeiten und brauchen dafür auch digitale Erfahrungs- und Erprobungsräume. Andererseits führen die Entwicklungsverletzlichkeiten (d.h. die Tatsache, dass Fähigkeiten und Möglichkeiten zum Selbstschutz noch nicht ausgebildet sind oder zugeschrieben werden) dazu, dass Kinder Risiken nicht als solche erkennen oder sie anders einschätzen. Gerade bei Erfahrungen, die schambesetzt sind oder wenn kein Vertrauen etabliert ist, kann daraus folgen, dass Hilfesysteme nicht in Anspruch genommen werden oder z.B. bei strafrechtlich relevanten Vorgängen keine polizeiliche Unterstützung gesucht wird. Dies gilt insbesondere für digitale Plattformen und soziale Medien, die von Kindern genutzt werden. Gerade der Angebotscharakter (*media affordances)* berücksichtigt vielmals nicht die besonderen Interessen von Kindern, insoweit sie von Erwachsenen bzw. für Erwachsene konzipiert wurden. Adressieren digitale Angebote die Verletzlichkeiten junger Menschen nicht angemessen, können Sicherheitsgefährdungen begünstigt werden. Dies kann dazu führen, dass Kinder nicht nur gegenwärtig geschädigt oder traumatisiert werden, sondern dass ihr „Recht auf eine offene Zukunft" (Feinberg 1980; Stapf 2022) dadurch beeinträchtigt wird.

Überdies zeigen die Herausforderungen für die Sicherheit von Kindern[3] online die **Verwobenheit der verschiedenen Rechte**, die Kindern zustehen. Denn Menschen haben mit der seit 1989 geltenden und in Deutschland seit 1992 ratifizierten **UN-Kinderrechtskonvention** (UN 1989) vor der Volljährigkeit ganz **verschiedene Rechte**. Diese greifen mit dem General Comment Nr. 25 (UN 2021) gleichwertig in digitalen Umwelten. Neben Schutzrechten haben Kinder weitere Rechte, z.B. auf Bildung, Teilhabe oder Spiel, die in digitalen Welten erfüllt werden und dabei Potenziale und Chancen für sie ermöglichen können. Insofern Kinder viele verschiedene Rechte auch in digitalen Umwelten haben, geht es bei Fragen der Sicherheit immer auch um **Abwägungsprozesse** einzelner Rechte im Feld von Schutz, Teilhabe und Befähigung.

Sicherheit ist eine Grundbedingung für die freie Entfaltung von Persönlichkeitsrechten und eine unbelastete demokratische Teilhabe im Digitalen. Die konkreten Gefährdungen, denen Kinder psychisch und physisch ausgesetzt sind, können dazu führen, dass Kinder durch mangelnde Sicherheit – aber auch durch zu weitgehende Sicherheitsmaßnahmen – in ihrer personalen Integrität, ihren Partizipationschancen und ihren Möglichkeiten zur freien Entwicklung und Entfaltung eingeschränkt werden (Stapf & Heesen 2022). Sicherheit umfasst **intakte Infrastrukturen** und ein sicheres soziales Umfeld – auch im Digitalen. Solche Fragen der Lebensqualität haben einen Einfluss auf die subjektive wie objektive Sicherheitswahrnehmung: **Wer sich nicht sicher fühlt, partizipiert weniger** – aus Angst, Sorge, oder weil bereits Sicherheitsgefährdungen eingetreten sind, die zu Verstörung oder Traumata führen und die mögliche Zukunft von Kindern betreffen (HateAid 2024). Sicherheit ist demnach ein Kernziel von Kinderrechten sowie die Grundlage zur Umsetzung anderer Kinderrechte. Damit kann Sicherheit der Schaffung von Frei- und Handlungsspielräumen dienen.

[3] Der verwendete Begriff „Kinder" bezieht sich hier mit der UN-KRK auf junge Menschen bis zur Volljährigkeit. Wenn es spezifisch um Kinder in Abgrenzung zur Adoleszenz geht, werden diese auch als „Kinder" und „Jugendliche" bezeichnet.

Sicherheit

Sicherheit ist ein multidimensionaler Begriff. In der UN-KRK finden sich eine Vielzahl von Verbürgungen, die unmittelbar und mittelbar sicherheitsrelevante Schutzbereiche enthalten, darunter etwa Art. 6 (Recht auf Leben), Art. 24, 27 (Recht auf Gesundheit und gesunde Entwicklung), Art. 19, 32, 34, 36 (Recht auf Schutz vor Missbrauch und Ausbeutung). Die Gewährleistung von Online-Sicherheit von Kindern kann die Umsetzung dieser Rechte in der digitalen Welt unterstützen. **Sicherheitsethik** untersucht die Folgen und Implikationen der unterschiedlichen Begriffe von Sicherheit wie z.B. objektivierte und subjektive Sicherheitswahrnehmung, den erweiterten Sicherheitsbegriff (*Human Security)* sowie Angriffs- und Funktionssicherheit *(Security and Safety,* United Nations Trust Fund for Human Security). Aus normativer Perspektive erörtert die Sicherheitsethik, ob es ein Zuviel an Sicherheit geben kann und wann Sicherheitsmaßnahmen und -technologien andere Rechte beschneiden. Sicherheit wird vor diesem Hintergrund kritisch reflektiert in Hinsicht auf die Frage, welche Menschen in welcher Weise von welcher Form von Sicherheit profitieren, eingeschränkt oder sogar beschädigt werden (Ammicht Quinn 2014). Eine wichtige Rolle spielen im Zusammenhang dieser erweiterten Perspektive Präventionsangebote, der Resilienzbegriff und auch die Auseinandersetzung mit Machtverhältnissen im Zuge der Umsetzung von Sicherheitsinteressen.

Die drei Säulen der völkerrechtlich bindenden **Kinderrechte** verknüpfen Schutz-, Befähigungs- und Beteiligungsrechte. Diese sind als eine Einheit zu verstehen, für die das Kindeswohl (Art. 3 UN-KRK) als Brückenkonzept fungiert. Bezogen auf die **Sicherheitsrisiken** besteht dabei ein **Spannungsfeld:** Denn Grundlage der zukünftigen politischen Teilhabe und Mündigkeit von Kindern als Bürger:innen – aber auch in ihrer Gegenwart **als Kinder** – ist Sicherheit.

Aus kinderrechtlicher Sicht sollten Sicherheitsvorkehrungen und -maßnahmen daher – wann immer möglich – **handlungsfördernd bleiben.** Dies impliziert – da die Nutzung von digitalen Medien mit zunehmendem Alter immer häufiger mobil und oft ohne Beisein und Kontrolle durch die Eltern erfolgt –, dass Befähigung immer zentraler wird: Für Kinder sollte erfahrbar werden, was sie wie tun können, um sich selbst zu schützen oder die Hilfe zu bekommen, die sie in Problemsituationen brauchen. Dabei sollte die Grundlage, aber auch die Kommunikation der Maßnahmen nicht nur die Vermeidung von Risiken sein, sondern das Ziel unbeschwerter Teilhabe. Gerade in der Ansprache junger Menschen sollte stärker vom Ziel her gedacht und argumentiert werden, um dabei zu ergründen, welche Formate die Zielgruppe selbst erreichen und ihren Selbstschutz stärken. **Verantwortung** dafür, dass dies gelingen kann, trägt aus ethischer Sicht, gerade auch wegen der Relevanz und der Komplexität von Sicherheitsfragen, **nicht das minderjährige Individuum, sondern das gesamte Stakeholder-Netzwerk.**

Bestehende Regulierungsvorhaben, unterstützt durch z.B. die JuSchG-Novellierung, bestärken den Transformationsprozess hin dazu, den „Kinder- und Jugendmedienschutz vom Kind aus zu denken" (Brüggen et al. 2022, S. 19). Aber auch in der **technischen Gestaltung** lässt sich auf ***Support-by-Design***, ***Safety-by-Design***- **oder gar** ***Child Rights-by-Design***-**Ansätze** aufbauen. Es wird dadurch insgesamt stärker möglich, eine „*Positive Plattform Governance*" und „Kultur der Positiven Medien" (Süß 2009; Stapf 2012) zu etablieren.

Positive Medien

Ein für Kinder unbeschwerter Umgang mit (digitalen) Medien setzt **positive Medien** voraus. Kinder haben laut UN-Kinderrechtskonvention auch ein Recht auf entwicklungsförderliche mediale Angebote. Es kommt demnach nicht nur auf Medien an, die „nicht schaden", sondern es braucht auch mediale Angebote, welche Qualitätsanforderungen und pädagogische Kriterien erfüllen: Sie sollen beispielsweise Anregungen zur Auseinandersetzung mit Wertfragen enthalten und damit die Entwicklung der moralischen Urteilsfähigkeit fördern, sie sollten vielfältige Rollenmodelle und Identifikationsfiguren enthalten und Konfliktlösungsmodelle jenseits von Gewalt und Überanpassung bieten; altersgerechte Inhalte sollen Impulse zur Bewältigung von Entwicklungsaufgaben vermitteln, und der kulturelle Horizont der Kinder soll durch die Medienangebote erweitert werden. Kinder haben insgesamt nicht nur ein Recht auf Schutz, sondern auch ein Recht auf Spiel, Freizeit, Erholung und auf Teilhabe an den kulturellen Schöpfungen der Gesellschaft. Damit sind auch digitale Medien ein wichtiger Teil der zeitgenössischen Kultur, von Printmedien bis zu Computerspielen und digitalen Umgebungen (Süss 2012; S. 226; siehe auch Kapitel 3.1 Ergebnisse ethische Perspektive).

Damit dies auch strukturell gelingt, bedarf es einer **Förderkultur** für gute, d.h. kindgerechte und Kinderrechte stärkende Angebote für junge Menschen sowie den Ausbau von **Anreizsystemen für entwicklungsangemessene Angebote**. Hier sollten mit Blick auf Fragen sozialer Ungleichheit (und damit auch sozialer Ungerechtigkeit) möglichst **viele verschiedene – auch unterhaltsame – Angebote für Kinder in ihrer Diversität** auffindbar und nutzbar sein, die sicher sind, Kinder zur Sicherheit befähigen, die *Support-by-Design* anbieten oder sogar fähigkeitenbasiert (*asset-based*, Wong-Villacres et al. 2020) ansetzen.

Insoweit Sicherheit als Ermöglichung von Teilhabe und anderen Rechten gedacht wird, geht es aus kinderrechtlicher Sicht vor allem darum, Kinder sowohl als gesellschaftliche Gruppe als auch als einzelne Individuen zu stärken. Als gesellschaftliche Teilgruppe kann eine Befähigung beispielsweise als ein **Querschnittsthema in der schulischen Bildung** stattfinden und Kinder zum Selbstschutz in die Lage versetzen. Maßnahmen sollten es verschiedenen Kindern auch über **individualisierbare Ansätze** ermöglichen, selbstbestimmte Entscheidungen zu treffen und Sicherheitsrisiken kompetent begegnen zu lernen, ohne dabei Teilhabe aufgeben zu müssen.

Aktuelle Ansätze, die sich mit dem Thema ***Digital Wellbeing*** beschäftigen, weisen in eine wichtige Richtung.

Digital Wellbeing

Vor allem Plattformen bieten vermehrt Ressourcen und Anleitungen für *Digital Wellbeing* an, so der TikTok Guide for Digital Wellbeing oder Angebote von Google, Snapchat oder gar Consulting für Digital Wellbeing. Bestehende Definitionen umfassen unterschiedliche Aspekte, so „the enhancement and improvement of human well-being, in the intermediate and long term, through the use of digital media" (Israel National Commission for UNESCO 2024), „a state where subjective well-being is maintained in an environment characterized by digital communication overabundance" (Gui et al. 2017), „a subjective individual experience of optimal balance between the benefits and drawbacks obtained from mobile connectivity" (Vanden Abeele 2021). Der Begriff umfasst vor allem subjektives Wohlbefinden

in der Nutzung digitaler Medien oder die Nutzung digitaler Medien zur Realisierung eigener Potenziale oder eine Art Resilienz im Kontext einer überwältigenden Medienlandschaft. Auch damit angesprochen ist die Frage des guten Lebens (Burr et al. 2020) und wie sich digitale Medien auf das Wohlbefinden nicht nur von Individuen, sondern auch der Gesellschaft auswirken, so bei Burr & Floridi (2020): „the impact that digital technologies, such as social media, smartphones, and AI, have had on our well-being and our self-understanding of what it means to live a life that is good for us in an increasingly digital society". Aus kinderrechtlicher Sicht wird es zukünftig darauf ankommen, Fragen des *Digital Wellbeings* konzeptuell und auch aus Sicht von Kindern selbst zu klären, gerade insoweit Sicherheitsgefährdungen eine Rolle spielen.

Allerdings kann eine Verengung auf derartige Ansätze auch zu einem **Bumerang-Effekt** führen: Die Verantwortung für eine sichere und entwicklungsförderliche Internetnutzung **sollte nicht** auf die Individuen verlagert werden, da sie sie – zumal, wenn es junge Menschen in ihrer Entwicklung betrifft – überfordern kann. Fragen des gleichen Zugangs, intersektionale Diskriminierungsgefahren und sämtliche Benachteiligungen von Kindern dürfen, mit Blick auf das Gleichheitsprinzip und Diskriminierungsverbot, das Kinderrechten unterliegt, nicht ausgeblendet werden.

Insbesondere Fragen von digitalen Infrastrukturen, die Verfolgung von Hate Speech, Falschnachrichten oder diskriminierender Dienste, Manipulation durch Design (*Dark Patterns*) und Datentracking können nur durch institutionelle und gesetzliche Regelungen, Anreizsysteme und Strafverfolgung angegangen werden. Gesellschaft, Politik und Gesetzgeber stehen hier in der Verantwortung, sichere Rahmenbedingungen zu stellen, die die Risiken insbesondere auch für junge Menschen minimieren und die Grundlagen für Befähigung und Teilhabe auf überindividueller Ebene sichern (I-KiZ 2015).

Mit Blick auf die in den Kinderrechten angelegte Verwobenheit von Schutz, Teilhabe und Befähigung sollte **Sicherheit damit im digitalen (und sozialen) Ökosystem gedacht werden.** Daraus resultierende Ansätze sollten möglichst **inklusiv konzipiert sein.** Dies gelingt nur, wenn Lösungswege im Netzwerk angestrebt werden, und bedarf einer systematischen **Vernetzung aller relevanten Stakeholder**, voran Anbieter, Sicherheitsbehörden, Akteure des gesetzlichen Kinder- und Jugendmedienschutzes, Hilfe- und Unterstützungssysteme, Zivilgesellschaft, Bildungseinrichtungen, Erziehende, Recht und Medienregulierung und die Forschung und Wissenschaft. Hilfreich hierzu ist es, weitere gesellschaftliche und ethische Diskurse über Gelingensbedingungen darüber zu führen, wie mit bestehenden Spannungsfeldern umzugehen ist (Stapf & Dreyer, i.E.). All dies macht, so eine zentrale These des Kompasses, eine **angemessene Beteiligung junger (verschiedener) Menschen wesentlich** – nicht nur im Diskurs, sondern auch beim Design und der Gestaltung von Angeboten, im partizipativen Kinder- und Jugendmedienschutz und in der Forschung.

3. Ergebnisse: Erkenntnisse zur Online-Sicherheit von Kindern aus der Projektarbeit

Im SIKID-Projekt wurde interdisziplinär zu Online-Sicherheit von Kindern mit Blick auf Sicherheitsgefährdungen geforscht. Im Folgenden werden zentrale Ergebnisse aus den einzelnen

Teilprojekten dargestellt. Sie basieren auf disziplinären Perspektiven und legen unterschiedliche Methoden zugrunde, sind jedoch als Ergebnis des interdisziplinären Austausches mit allen Partner:innen im Projekt zu sehen.

3.1 Die ethische Perspektive

Die ethische Perspektive verbindet **sicherheits- und medienethische** mit **kinderrechtlichen Fragen im Kontext von Online-Interaktionsrisiken.** Sie kann dadurch Gefahren und bestehende Sicherheitslücken für Kinder und Jugendliche im digitalen Raum identifizieren und **mithilfe normativer Instrumente kindzentrierte Regulierungs- und Befähigungsansätze entwickeln.** Die ethische Forschung kann zudem über rechtliche Aspekte hinaus moralisch relevante Fragestellungen adressieren. Online-Interaktionsrisiken entstehen im Zuge von Kommunikation und Interaktion und sind stets mediiert durch technische Systeme und sozio-technische Prozesse. Diese wertgeladenen Kontexte sind bei der Bewertung von Risiken zu beachten und spielen mit Normen der Mediennutzung und der Ausgestaltung einer *Media Governance* zusammen. Bei der Bearbeitung von Online-Interaktionsrisiken für Heranwachsende gibt es daher keine klare ethische Richtungsweisung, die ungeachtet des Kontextes gilt. Im Gegenteil braucht es eine reflektierte Abwägung von Kontexten, von individuellen Faktoren und gesellschaftlichen Machtkonstellationen sowie eine kritische **Analyse, Reflexion und Steuerung** mit Blick auf die Verantwortung von Bildung, Erziehung und Regulierung. Zu den zentralen Ergebnissen aus dem Teilprojekt Ethik gehört die Etablierung einer kinderrechtlichen Perspektive für die zivile Sicherheitsforschung, die Förderung ethisch fundierter Forschung mit Kindern sowie die ethisch fundierte Herleitung bzw. Erarbeitung von Konzepten für mehr Sicherheit und Befähigung von Kindern durch eine *Positive Media Governance* für Plattformen und Politik sowie *Digital Street Work* für Jugendarbeiter:innen.

3.1.1 Die Entwicklung einer kinderrechtlichen Perspektive auf die zivile Sicherheitsforschung

Die bei SIKID erarbeitete **Verbindung der Themen Kinderrechte, Medien und Sicherheit ist neuartig** in dem Sinne, dass die Themen bislang nicht systematisch zusammengedacht wurden. Eine kinderrechtliche Perspektive auf Sicherheitsfragen in der Online-Kommunikation und Interaktion anzuwenden, ist jedoch aufgrund aktueller und steigender Risiken für Kinder und Jugendliche in digitalen Räumen (sexuelle Ausbeutung, Cybergrooming, Hassrede), die teils durch KI in ihrem Ausmaß verstärkt wird, dringend und notwendig.

Eine kinderrechtliche Perspektive bedeutet, **Kinder als handelnde Subjekte** zu verstehen und dabei **entwicklungsbezogene Verletzlichkeiten** zu berücksichtigen, stets mit dem Ziel, die kindliche Autonomie und freie Entfaltung zu fördern (Stapf 2022). Während dies in kinderrechtlichen Diskursen weitgehender Konsens ist, wird etwa bei der Gestaltung von Regulierung, Anbietermaßnahmen und häufig bei Präventionsprogrammen zur Sicherheit von Kindern im Digitalen immer noch sehr stark auf den Schutz, aber oft zu wenig auf die Befähigung oder die Beteiligung von Kindern Wert gelegt. Aus Perspektive der Sicherheitsethik gilt es jedoch gerade die womöglich mit dem Wert der Sicherheit konkurrierenden Ansprüche auf informationelle Selbstbestimmung, Teilhabe und Meinungsbildung kindbezogen abzustim-

men. Die Medienethik wiederum kann eine kritische Reflexion und eine nuancierte Abwägung insbesondere bezogen auf bestehende Zielkonflikte und Spannungsfelder mit Blick auf digitale Medien ermöglichen. Auf diese Weise kann eine kinderrechtliche Perspektive auf Sicherheit im Online-Raum auch unterschiedliche Kinderrechte miteinander verbinden.

3.1.2 Ein Forschungsethisches Konzept für sensible Themenbereiche

Unter Federführung des Teilprojekts Ethik wurde in SIKID ein **Konzept mit 12 Leitlinien für die systematische Einbindung von Kindern in die zivile Sicherheitsforschung entwickelt** (Stapf et al. 2022). Das Forschungsethische Konzept bildet die Grundlage für eine **ethisch reflektierte Forschung mit Kindern in sensiblen Themenbereichen der Sicherheitsforschung.** Dabei ist es dezidiert ethisch fundiert, interdisziplinär und unter Einbezug rechtlicher Aspekte ausgerichtet. Die Forschung **mit** Kindern ist aus kinderrechtlicher Perspektive notwendig, denn Kinder haben laut UN-Kinderrechtskonvention (UN-KRK) unter Artikel 12 ein Recht auf Beteiligung in allen sie betreffenden Fragen.
Einerseits ist die Partizipation von Kindern also selbst eine ethische Anforderung der Beteiligungsrechte, zugleich erweitert Partizipation die ethischen Fragen im Forschungsprozess. Ethische Fragen im Zusammenhang der Partizipation betreffen unter anderem die informierte Einwilligung, Vertraulichkeit und Datenschutz, die Rolle der Eltern oder den Schutz vor Verängstigung oder Retraumatisierung. Das Forschungsethische Konzept bietet auch für den internationalen Kontext (Stapf & Heesen 2024) eine **Grundlage zur ethischen Sensibilisierung der Forschenden**, welche durch geteilte Erfahrungen und Feedback ergänzt werden sollte. Eine kinderrechtlich fundierte Forschungsethik bedarf überdies der Entwicklung altersangemessener Methoden für verschiedene Forschungssettings und Zielgruppen (z.B. Kinder mit Fluchterfahrung oder mit Beeinträchtigungen) und im Idealfall auch die partizipative Einbindung von jungen Menschen in die Entwicklung konkreter forschungsethischer Ansätze in Forschungsprojekten (Stapf, Bieß, Pfetsch & Paschel 2023). Das erarbeitetes Forschungsethische Konzept durchdringt Forschungsethik erstmals aus kinderrechtlicher Perspektive und ist für andere Kontexte oder auch für jüngere Kinder anpassbar.

3.1.3 Ein Konzept für *Positive Media Governance*

Als Teil der wissenschaftlichen Arbeit im Projekt hat sich der Bereich SIKID-Ethik insbesondere aus medien- und sicherheitsethischer sowie kinderrechtlicher Sicht mit der Frage beschäftigt, wie ein **geeignetes Framework für die Entwicklung, Nutzung und Regulierung der digitalen Medienwelt** aussehen könnte. Dabei wurde der **Begriff der *Positive Media Governance*** geprägt. Basierend auf Ansätzen der Positiven Psychologie (Seligman 2002; Seligman & Csikszentmihalyi 2000) fokussiert die Positive Medienpsychologie auf die Potenziale für junge Menschen durch (digitale) Medien und fordert „a more holistic view of mediated experience, searching for the full spectrum of experience, the problems and the benefits in order to pursue the positive potential" (Rutledge 2020, S. 2). Damit diese Potenziale trotz bestehender Sicherheitsgefährdungen gestärkt werden können, sollte sich auch die Medienregulierung darauf ausrichten. Dies impliziert die **Schaffung von „Möglichkeitsräumen" für junge Menschen in digitalen Umgebungen**, die an ganz verschiedenen Rechten von Kindern ausgerichtet sind und dabei **Anreizsysteme für Anbieter** ebenso schafft wie **Fördergrundlagen für „Positive Medien"** etabliert. Ziel ist es, kind- und entwicklungsgerechte Angebote zu stärken, welche kindliche Entwicklungsverletzlichkeiten, aber auch -themen ins

Zentrum rücken. Ansätze, die eine „systematische Einbeziehung der kinderrechtlichen Perspektive und der Kinderperspektive durch partizipatorische Verfahren" leisten, „können auch zu verbesserten Maßnahmewirkungen, höherer Akzeptanz und guter Praxistauglichkeit führen" (Stapf et al. 2023, S. 17). Der Ansatz einer *Positive Platform Governance* impliziert die Ausrichtung an diesen Zielen, mit denen Ansätze altersangemessener Gestaltung (*Age-Appropriate Design*) oder Konzepte kontextsensibler (*Contextual Design*) und individualisierter fähigkeitenbasierter Ansätze (*Asset-Based Design*) in den Vordergrund rücken (Stapf et al. 2023).

Kinderrechte können damit selbst ein *Asset* für Anbieter werden, wenn sich Kontexte entfalten, in denen Aufmerksamkeit i.S. eines **positiven Kinder- und Jugendmedienschutzes** entsteht. Verstanden als *Positive Platform Governance* gilt es dann als Qualitätsmerkmal, dass kindgerechte Angebote in den Bereich von ***Good* oder *Best Practice*** fallen. Im Zuge eines Multi-Stakeholder Ansatzes wurden zudem im Rahmen von Expert:innen-Interviews (Prinzing & Stapf 2024; Stapf & Prinzing 2024) auch Fragen des zunehmend diskutierten **Konzeptes von *Digital Wellbeing*** untersucht. Dabei konnte herausgestellt werden, dass es auf die gemeinsame Schaffung von Bedingungen ankommt, die digitales Wohlergehen „im Netzwerk verschiedener Akteure und im Zuge einer sich an aktuelle Entwicklungen anpassenden Medienpolitik gemeinsam mit der Zivilgesellschaft" ermöglicht, die „*Digital Wellbeing* auch strukturell – und nicht nur reduziert auf Maßnahmen des resilienten Individuums – ermöglichen" (Prinzing & Stapf 2024, S. 136).

3.1.4 Konzept zur Befähigung von Kindern im Digitalen durch *Digital Street Work*

Um die Sicherheit von Kindern im Digitalen angesichts zunehmender Online-Interaktionsrisiken zu stärken, braucht es aus kinderrechtlicher Perspektive Methoden und Konzepte zur Befähigung von Kindern. **Befähigung ist eine Sicherheitsressource**, denn wenn Kinder und Jugendliche in der Lage sind, Risiken einzuschätzen, im Falle einer Verletzung ihrer Rechte oder der Rechte anderer Kinder einzuschreiten und sich ggfs. auch Hilfe zu suchen, können sie sich selbstbestimmter in digitalen Umwelten bewegen. Die **Ausgestaltung eines *Digital Streetwork*-Konzepts vom Kind aus gedacht** ist ein Versuch, die Sicherheit von Kindern in digitalen Welten niederschwellig und plattformübergreifend zu fördern (Bieß 2023). Das Konzept setzt an bestehende Formen der (mobilen) Jugendarbeit oder Einzelfallhilfe an, wobei Digital Street Work immer auch einen aufsuchenden Charakter hat, denn die Jugendarbeiter:innen kommen „zum Kind" und in die Lebenswelten der auch digitalen Kindheit. Die konzeptuelle Ausarbeitung der Idee kann helfen, neue Strategien für die soziale Arbeit zu entwickeln bzw. weiterzuentwickeln, und steht im Kontext einer allgemeinen Bemühung zur Gewaltprävention und Friedenspädagogik, die im Digitalen Anwendung finden sollte (Bieß et al. 2022).

3.2 Die rechtliche Perspektive

In den vergangenen Jahren befand sich der Jugendmedienschutz im Wandel und musste auf die wachsende Digitalisierung und neue Risiken reagieren. Durch die zunehmende Aus-

stattung mit autonom nutzbaren Online-Endgeräten sowie durch neue interaktive Angebotsformen haben sich die Praktiken der Mediennutzung von Minderjährigen fundamental verändert. Neben neuen Möglichkeiten des Austausches und der Kommunikation oder erleichtertem Zugang zu Wissen weisen die digitalen Umgebungen auch sicherheitsrelevante Risiken für Kinder und Jugendliche auf, die bislang nur zum Teil vom bestehenden Rechtsrahmen gefasst werden können. Die neuen Risikopotenziale gehen über die Anwendungsbereiche klassischer Jugendmedienschutzregulierung hinaus und liegen quer zu traditionellen Rechtsbereichen wie dem Datenschutzrecht, Verbraucherschutzrecht oder dem Strafrecht.
Die rechtswissenschaftliche Perspektive im SIKID-Projekt hat den bestehenden Rechtsrahmen für den Phänomenbereich der Online-Interaktionsrisiken von Kindern und Jugendlichen systematisch untersucht und kritisch auf mögliche Graubereiche und Umsetzungsprobleme hin analysiert. Ein zentraler Teil der Untersuchung ist eine Governance-Analyse, die klassische Rechtsanalysen, normprogrammbezogene Analysen sowie Akteursanalysen umfasst und so einen umfassenden Überblick über Ordnungsrahmen, Regelungsstrukturen und Akteurskonstellationen ermöglicht. Auf Grundlage der Untersuchungsergebnisse entwickelt das Teilprojekt gesetzliche Maßnahmen zur Verbesserung der Sicherheit von Kindern im Internet und Handlungsoptionen zur Verzahnung von Akteuren und Maßnahmen des repressiven gesetzlichen Jugendmedienschutzes mit denen aus dem Bereich des präventiven und erzieherischen Jugendmedienschutzes. Ziel dabei ist es, die Sicherheitsarchitektur effizienter und risikogerechter aufzustellen.

3.2.1 Rechtliche Rahmung von Interaktionsrisiken

Interaktions- und Kommunikationsrisiken sind **neuartige Risikotypen** bei der Mediennutzung Heranwachsender. Die Rechts- und Governance-Analysen haben ergeben, dass **viele der Begehungsformen bereits strafrechtlich, medienordnungsrechtlich und zivilrechtlich fassbar** sind (Dreyer, Andresen & Wysocki 2024, i.E.). Wenige **andere Risiken** hingegen, wie etwa Formen der aufgedrängten Sexualität im Digitalen, sind **noch nicht umfassend abgebildet** (Andresen & Dreyer 2021). Im strafrechtlich relevanten Bereich zeigt sich zudem, dass das Entdeckungsrisiko im Internet weiterhin gering ist. Viele betroffene Minderjährige teilen Verletzungen nicht mit, etwa aus Angst vor der Kenntnisnahme durch die Eltern und damit einhergehenden möglichen Konsequenzen für die eigene Mediennutzung.
Zudem sind sich viele jüngere Betroffene unsicher, welche Handlungen tatsächlich (Rechts-)Verletzungen darstellen, welche Rechte sie haben, und an wen sie sich in Verletzungsfällen wenden können (siehe Kapitel 3.4 Ergebnisse Kommunikationswissenschaftliche Perspektive). Erschwerend tritt hinzu, dass in vielen Konstellationen konsensualen Sextings eine Strafbarkeit von Jugendlichen nicht ausgeschlossen werden kann (Andresen & Dreyer et al. 2023). Kommt es zu einer Verletzung, fokussiert der derzeitige Rechtsrahmen vor allem auf die Verfolgung von Täter:innen. Ein systematischer Rahmen für Opferschutz und Begleitung betroffener Minderjähriger ist nicht vorhanden.

3.2.2 Die Rolle der Eltern in der Governance-Struktur

Eltern werden in den verschiedenen Regelungsbereichen **unterschiedlichste Rollen** zuteil: Sie sollen ihre Kinder schützen, befähigen und sie darüber hinaus in bestimmten Bereichen vertreten – so beispielsweise bei der datenschutzrechtlichen Einwilligung oder im Gerichtsverfahren. Dass diese Ziele zu **schwierigen Abwägungsprozessen und Doppelrollen** führen

können, zeigt sich beispielsweise bei Art. 8 DSGVO, wenn die Erziehungsberechtigten für ihre unter 16-jährigen Kinder bei Angeboten von Diensten der Informationsgesellschaft die Einwilligung zur Verarbeitung von personenbezogenen Daten geben. Dabei kann es für Eltern schwierig sein, eine gute Entscheidung zwischen Teilhabe und Schutz für ihre Kinder zu treffen (Andresen & Dreyer 2022). Hier und an anderen Stellen – z.B. im Phänomenbereich des *Sharenting* – kann es zu Situationen kommen, in denen Eltern in ihrer Doppelrolle als fürsorgender und befähigender Begleiter befangen sind (Dreyer 2024). Auch kommt es zu **Interessenkollisionen** in Fällen, in denen das Interesse des Kindes an der Geheimhaltung bzw. seines Vertrauensschutzes bzgl. eines bestimmten Sachverhalts, insbesondere des Erziehungsrechts und -interesses der Eltern, überwiegt. In jenen Situationen gerät das aktuell als fremdnütziges Recht gedachte **Erziehungsrecht an strukturelle Grenzen.** Ein Beispiel ist, wenn Eltern anstelle der Kinder in die Datenverarbeitung einwilligen, ohne aber ausreichendes Wissen über die Praxis vollautomatisierter und teils invasiver Datenverarbeitung zu haben.

3.2.3 Ambivalenz technischer Lösungen

Als eine Form der Begegnung von Online-Risiken werden im politischen Diskurs auch **technische Lösungen** vorgeschlagen. Im Fokus stehen dabei u. a. **Altersverifikationssysteme**, aber auch Ansätze wie eine **Vorratsdatenspeicherung** oder **Anbieterpflichten** zum Monitoring von Nutzer:innen-Dateien und Kommunikationsinhalten, die eine bessere Identifizierung von Taten und Täter:innen insbesondere im Zusammenhang mit sexuellem Missbrauch von Kindern und Kinderpornographie[4] ermöglichen sollen. Mit Blick auf die teils transformativen Entwicklungssprünge im Bereich der Künstlichen Intelligenz treten auch (teil-)automatisierte Verfahren der Risikoerkennung und -minimierung in den Markt. Neben der **Ambivalenz von technischen Lösungen** vor allem in Bezug auf ihre **Verhältnismäßigkeit im Angesicht der Grundrechte** von (allen) Erwachsenen und Kindern und mit Blick auf den Zugang und die Teilhabe zu Kommunikations- und Informationsangeboten sind die Möglichkeiten wie die Grenzen technischer Maßnahmen vertieft zu beachten. Mit Blick auf die vorgenannten Punkte erscheinen **technische Lösungen nicht als Allheilmittel**; hier sollte stets eine **Abwägung zwischen Interessen und erreichbaren Zielen einerseits und widerstreitenden relevanten Grundrechten** andererseits erfolgen.

3.2.4 Vorsorgemaßnahmen auf Seiten der Anbieter

In den vergangenen Jahren wurden die **Governance-Ansätze im Jugendmedienschutz** mit Blick auf Online-Plattformen mit nutzer:innengenerierten Inhalten und Interaktions- bzw. Kommunikationsfunktionen deutlich erweitert. Dazu gehören insbesondere Pflichten von Plattformen zur **Schaffung von (Vorsorge-)Maßnahmen, um einen hohen Grad an Schutz, Privatheit und Sicherheit zu gewährleisten.** Zunächst sah der 2021 neu eingeführte § 24a JuSchG a.F. entsprechende Implementationspflichten vor, mittlerweile wurde die Vorschrift von Art. 28 Abs. 1 DSA auf EU-Ebene abgelöst. Die rechtlichen Analysen haben ergeben, dass

[4] Wir sprechen bei Missbrauchsdarstellungen von CSAM (*child sexual abuse material*) und nutzen nicht den kritisierten Begriff der „Kinderpornographie". Dieser wird nur dort verwendet, wo es um die strafrechtliche Bezeichnung geht.

Teile der vom Gesetzgeber genannten Vorsorgemaßnahmen erst nach einer Realisierung des Risikos wirken (z.B. Melden, Beratungsangebote). Um anbieterseitige Maßnahmen vor und nach Verletzungen systematisch auszubauen, bieten sich **neben einer altersgemäßen Angebotsgestaltung und Funktionsaktivierung auch Formen des begleitenden Monitorings** an, das insbesondere **kontextbezogene Vorsorgemaßnahmen** ermöglicht. Das zuletzt durch Art. 7 DSA privilegierte Monitoring durch Anbieter erleichtert die rechtssichere Überwachung von Kindern auf Plattformen, aber sowohl dieses Monitoring als auch die Einführung angebotsweiter Altersüberprüfungen führen zu Eingriffen in die Kommunikation von Kindern.

Insgesamt haben die Novellen der Regelungsrahmen im Bereich der Interaktionsrisiken mit der Einführung präventiv wirkender Maßnahmen eine **strukturelle Veränderung und Erweiterung der Governance-Ansätze** im Jugendschutz zur Folge, dessen Auswirkungen im Bereich der Umsetzung und Rechtsanwendung noch nicht vollständig durchdrungen sind. Im Bereich von Online-Interaktionsrisiken tritt hinzu, dass die Realisierung eines Risikos von dem Zutun eines Dritten abhängt. Gerade im Rahmen von höchstpersönlicher Interaktion und Kommunikation geht dadurch ein Teil der effizienten Schutzmöglichkeiten auf den Einflussbereich der kommunizierenden Kinder und – nur in Teilen – auf die Eltern über. Daraus folgt eine **deutliche Verbreiterung und Vertiefung der Aufgaben von Akteuren im erzieherischen Jugendmedienschutz und in der weiteren offenen Kinder- und Jugendarbeit,** die nicht immer die dafür notwendige Expertise und bzw. oder die erforderlichen Ressourcen haben. Mit der Einführung der neuen Normen allein ist nur der erste Schritt getan, ihre Umsetzung hat Folgen für das **gesamte „Ökosystem Jugendschutz"** (Dreyer, Andresen & Wysocki 2022), ohne, dass der Gesetzgeber dafür die nötigen Ressourcen in der Breite vorgesehen hätte. Durch den **Querschnittscharakter der rechtlichen Einhegung von Online-Interaktionsrisiken sind zudem eine Vielzahl von verantwortlichen Akteuren berührt**, so dass für die effektive Umsetzung eine hohe Akzeptanz des Rechtsrahmens in allen Akteurskategorien nötig ist. Dies verweist auf die Wichtigkeit eines als **Verantwortungsnetzwerk verstandenen, befähigenden Jugendmedienschutzes** (Dreyer, Andresen & Wysocki 2024, i.E.). Die seit 2021 erweiterten Aufgaben der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ), die u.a. die „Förderung einer gemeinsamen Verantwortungsübernahme von Staat, Wirtschaft und Zivilgesellschaft" zur Koordinierung im Jugendmedienschutz und eines „regelmäßigen Informationsaustauschs" vorsehen, sind als erster wichtiger Schritt der legislativen Umstellung eines klassischen staatlichen Jugendschutzrahmens zu sehen.

3.3 Die psychologische Perspektive

Die psychologische Perspektive fokussiert die Erforschung **menschlichen Erlebens und Verhaltens** im Kontext von Online-Interaktionsrisiken und der **entwicklungsangemessenen Förderung positiver Online-Interaktionen**, insbesondere des Verhaltens der Bystander, die solche Online-Interaktionsrisiken beobachten. Durch die theoretisch-konzeptionelle **Analyse von Online-Interaktionsrisiken im Entwicklungsverlauf**, die **qualitativ-empirische Erfassung der Sicht von Jugendlichen** auf das Verhalten von Bystandern sowie die Entwicklung und Erprobung eines **Bildungsprogramms zu digitaler Zivilcourage unter Jugendlichen** bietet die psychologische Perspektive einen fokussierten theoretischen, empirischen und

praxisbezogenen Zugang zur Förderung der Sicherheit von Kindern und Jugendlichen im Internet.

Online-Interaktionsrisiken **entstehen aus sozialer Kommunikation und Interaktion (als menschliche Grundbedürfnisse) im digitalen Raum** und können mit **negativen Konsequenzen für das physische und psycho-soziale Wohlbefinden** einhergehen. Im Fokus des psychologischen Teilprojekts standen **Cybermobbing, Online-Hatespeech, non-konsensuales Sexting und Cybergrooming als exemplarische Interaktionsrisiken.** Diese Risiken stellen unterschiedliche Formen aggressiven bzw. grenzverletzenden Verhaltens dar und können schwerwiegende und langanhaltende Beeinträchtigungen des Wohlbefindens und der Entwicklung von Kindern und Jugendlichen nach sich ziehen. Ein Kausalzusammenhang zwischen Viktimisierungserfahrungen auf der einen und Beeinträchtigungen der psychischen Gesundheit, des Sozialverhaltens oder (schulischer) Leistungen auf der anderen Seite ist nicht einfach nachzuweisen oder gar zu beziffern. Dennoch liegen mittlerweile viele empirische Studien mit unterschiedlichen Designs (querschnittlich und längsschnittlich; experimentell und korrelativ) sowie Meta-Analysen vor, die zeigen, dass **Betroffene negative Folgen erleben können, die weit über kurzfristige negative Emotionen in der Situation hinausreichen** (etwa Depressionen, selbstverletzendes Verhalten, Suizidalität, Ängstlichkeit, eigene Aggressionen, Drogen-/Substanzmissbrauch, Aufmerksamkeitsstörungen, Verringerung des Selbstwertgefühls und mehr (Doyle et al. 2021; Gardella et al. 2017; Gini et al. 2018; Kwan et al. 2020; Marciano et al. 2020; Moore et al. 2017; Schoeler et al. 2018; Wachs et al. 2021; Wright & Wachs 2019).

3.3.1 Online-Interaktionsrisiken im Entwicklungsverlauf

Besonderheiten von Online-Interaktionsrisiken sind eng mit Kommunikationscharakteristika verbunden: die dynamische Natur, die Geschwindigkeit, Orts- und Zeitunabhängigkeit, mit denen sie sich entwickeln, sowie die geringe Vorhersehbarkeit und Nachvollziehbarkeit ihres Auftretens. Gerade weil **Online-Kommunikation** einen niederschwelligen Zugang zu einem potenziell großen Publikum bietet und Kommunikationspartner:innen flexibel gewählt werden können, sind sie **eng mit psycho-sozialen Bedürfnissen und Entwicklungsaufgaben von Kindern und Jugendlichen** (Hurrelmann & Quenzel 2018) **verknüpft.** Dazu gehören unter anderem die Konsolidierung sozialer Normen und Werte sowie Einstellungen gegenüber anderen sozialen Gruppen, die Exploration der eigenen Geschlechtsrolle und Sexualität, das Eingehen romantischer Beziehungen und letztendlich die Findung einer eigenen, kohärenten Identität. Im Rahmen der fortschreitenden Mediatisierung findet die **Bearbeitung der Entwicklungsaufgaben zunehmend online, insbesondere in sozialen Medien statt.** Die genannten Kommunikations-Charakteristika erzeugen ein **Spannungsfeld** zwischen einer **Unterschätzung des Gefahren- und Schädigungspotenzials** von auftretenden unangenehmen (oder gefährlichen) Situationen auf der einen und dem **Wunsch nach sozialer und gesellschaftlicher Teilhabe über soziale Medien** auf der anderen Seite.

Auch wenn die Häufigkeit (Prävalenzen), mit denen Kinder und Jugendliche Betroffene, Ausübende oder Bystander von Online-Interaktionsrisiken sind, je nach Erhebungsmethode, erfragten Verhaltensweisen und Stichprobe variieren, zeigen vielfältige empirische Studien, dass viele Kinder und Jugendliche im Internet in Cybermobbing, Online-Hatespeech, non-

konsensualem Sexting und Cybergrooming involviert sind. Bereits 6-Jährige sind mit Cybergrooming konfrontiert (Landesanstalt für Medien NRW 2024), Cybermobbing weist besonders hohe Prävalenzen in der siebten und achten Jahrgangsstufe auf (Tokunaga 2010), non-konsensuales Sexting und Online-Hatespeech sind vor dem Hintergrund des Entwicklungsstands und der Entwicklungsaufgaben insbesondere in der späten Adoleszenz (ca. 15 bis 18 Jahre) relevant (Hasebrink, Lampert & Thiel 2019; Madigan et al. 2018; Vogelsang 2017). Da klassischer Kinder- und Jugendmedienschutz Online-Interaktionsrisiken aufgrund ihrer Dynamik und Unvorhersehbarkeit nicht ausreichend eindämmen kann, sind **ergänzend Befähigungsansätze** für Kinder und Jugendliche notwendig. Die **Präventionslandschaft solcher Befähigungsansätze ist sehr heterogen.** Es existiert eine unüberschaubare Vielzahl an Angeboten (Aufklärungskampagnen, Unterrichtseinheiten, Bildungsprogramme), insbesondere im Bereich Cybermobbing. Von vielen dieser Angebote ist allerdings nicht bekannt, inwiefern diese theoretisch oder empirisch fundiert und auf ihre Wirksamkeit hin geprüft sind. Des Weiteren ist bisher die **größte Zielgruppe unter Jugendlichen, nämlich Bystander, weitestgehend unberücksichtigt.** Bystander sind Personen, die einen Vorfall mitbekommen, ohne zunächst aktiv beteiligt zu sein. Sie können durch prosoziales Verhalten einen großen Einfluss auf den Verlauf von Situationen nehmen, längerfristig prosoziale Verhaltensnormen festigen und so zu einer Verringerung von Viktimisierungserfahrungen beitragen. Weitere zusammengetragene Erkenntnisse über Online-Interaktionsrisiken im Entwicklungsverlauf von Kindern und Jugendlichen finden sich in Paschel, Schultz, von Salisch & Pfetsch (i.E.).

3.3.2 Perspektiven Jugendlicher auf Sicherheit im Internet

Bystander standen im Fokus einer qualitativen Erhebung zu Interaktionsrisiken. Im Rahmen von leitfadengestützten Gruppendiskussionen mit 11-18-jährigen Jugendlichen wurden soziale und normative Faktoren identifiziert, die beeinflussen, ob und wie jugendliche Bystander im Falle einer Konfrontation mit Cybermobbing, Online-Hatespeech oder non-konsensualem Sexting eingreifen. Situationen im Internet sind sehr komplex und schwer einzuschätzen, da oftmals Kontextinformationen fehlen. Darüber hinaus entsteht für Bystander leicht ein Gefühl der Machtlosigkeit in Anbetracht des großen Publikums in sozialen Netzwerken, die den Beitrag eines Einzelnen aus Sicht der Jugendlichen als unbedeutend erscheinen lassen. Insbesondere im Bereich sexualisierter Risiken ist *Victim Blaming*, also die Verantwortungszuschreibung an die betroffene Person, ein großes Problem, das insbesondere Mädchen betrifft. **Obwohl Jugendlichen eine Vielzahl an Handlungsmöglichkeiten bekannt ist, beschränken sie sich – sofern sie überhaupt eingreifen – weitestgehend auf private Reaktionen im Alleingang.** Die Möglichkeit, gemeinsam mit Peers zu agieren, ist kaum salient, bietet aber einen Ansatzpunkt für die Förderung digitaler Zivilcourage (Pfetsch 2019; Paschel & Pfetsch 2024a).

3.3.3 Bildungsmaterialien zur Förderung digitaler Zivilcourage unter Jugendlichen

Um die Lücke in der Präventionslandschaft im Bereich der Online-Interaktionsrisiken und die identifizierten Hürden für jugendliche Bystander für ein (öffentlich sichtbares) Eingreifen zu adressieren, entstand ein **Bildungsprogramm zur Förderung digitaler Zivilcourage** (*FairNetzt: Füreinander einstehen statt zusehen*). Das Programm basiert auf einschlägigen The-

orien und empirischen Befunden, verfolgt kognitive und sozial-emotionale Lernziele und richtet sich an Schüler:innen der 6. bis 10. Jahrgangsstufe. Es ist handlungsorientiert gestaltet, um den Teilnehmenden eine Erprobung von Handlungsmöglichkeiten und die Stärkung von Selbstwirksamkeitserwartungen zu ermöglichen. FairNetzt umfasst neun aufeinander aufbauende Module, die idealerweise über einen Zeitraum von etwa 12 Wochen eigenständig von pädagogischen Fachkräften (z.B. Lehrkräften, Schulsozialarbeiter:innen, Erzieher:innen) durchgeführt werden. Die Materialien, bestehend aus einem Manual, einer begleitenden Präsentation, Arbeits- und Lösungsblättern, werden unter einer CC-BY-Lizenz kostenfrei zur Verfügung gestellt und können von den Fachkräften für die Besonderheiten ihrer Lerngruppe angepasst werden. Die Materialien wurden im Rahmen von Workshops mit Schüler:innen der 6. bis 10. Klasse pilotiert, in Folge überarbeitet und anschließend im Rahmen eines Workshops mit pädagogischen Fachkräften validiert. Eine systematische Evaluationsstudie ist in Planung (Paschel & Pfetsch 2024b).

Insgesamt ermöglichen die theoretisch-konzeptionelle Analyse von Online-Interaktionsrisiken im Entwicklungsverlauf, die qualitativ-empirische Erfassung der Sicht von Jugendlichen auf das Bystanderverhalten sowie die Entwicklung und Erprobung eines Bildungsprogramms zu digitaler Zivilcourage unter Jugendlichen einen ganzheitlichen Zugang zur Förderung der Sicherheit von Kindern und Jugendlichen im Internet.

3.4 Die kommunikationswissenschaftliche Perspektive

Die Kommunikationswissenschaft befasst sich u.a. mit **Nutzungspraktiken und -erfahrungen** und liefert z.B. Befunde dazu, in welchem Umfang etwa Kinder und Jugendliche mit Online-Risiken in Berührung kommen (Gebel et al. 2022; Smahel et al. 2020; Hasebrink, Lampert & Thiel 2019). Neben teilweise großen Unterschieden in der Online-Nutzung allgemein und in den Prävalenzzahlen zeigt sich, dass Kinder und Jugendliche ein **anderes Risikoverständnis** haben als Erwachsene. Im Rahmen dieses qualitativen Teilprojekts wurde daher der Frage nachgegangen, was Heranwachsende in Online-Interaktionskontexten als belastend wahrnehmen, wie sie in kritischen Situationen reagieren und an welcher Stelle sie Unterstützung benötigen. Im Sinne des partizipativen Projektansatzes hatten Jugendliche überdies im Rahmen von Co-Creation-Workshops die Gelegenheit, ihre Vorstellungen von einem sicheren Internet zu entwickeln. Die vollständigen Ergebnisse (inklusive Implikationen für Forschung und Praxis) sind dokumentiert (Thiel & Lampert 2023a, 2023b und 2024).

3.4.1 Wahrnehmung und Bewertung belastender Erfahrungen in Online-Interaktionskontexten

Einen wichtigen Schutzfaktor gegen langfristig negative und beeinträchtigende Auswirkungen von Online-Interaktionsrisiken stellt die **souveräne Bewältigung** (***Coping***) entsprechender Erfahrungen dar (Livingstone 2014). Um den individuellen Bewältigungsprozess aus Sicht junger Menschen besser zu verstehen und Unterstützungsbedarfe zu identifizieren, wurden in einer **qualitativen Interviewstudie** 16 Jugendliche zu ihrer Wahrnehmung, Bewertung und Bewältigung belastender Erfahrungen in Online-Interaktionskontexten (insbesondere Cybermobbing/Cyberaggression, Hate Speech und sexuelle Grenzverletzungen) befragt.

Gezeigt hat sich, dass Jugendliche je nach Nutzungspräferenzen und -gewohnheiten mit vielfältigen, multiplen Interaktionsrisiken konfrontiert sind, die sie als unterschiedlich belastend empfinden. Das emotionale Erleben ist dabei stark von situativen (z.B. Kommunikationsinhalt, Erwartbarkeit, Grad der Öffentlichkeit), absenderbezogenen (z.B. bekannt vs. unbekannt, Alter, Geschlecht, Anzahl der Beteiligten), persönlichen (z.B. Alter, Geschlecht, frühere Erfahrungen) und wahrnehmungsbezogenen (z.B. wahrgenommene Kontrollierbarkeit, normative Signifikanz) Faktoren beeinflusst. Beleidigungen, die sensible Themen berühren und wunde Punkte der Jugendlichen betreffen, Ausgrenzung in der Peer Group und Erlebnisse mit realweltlichem Bezug werden tendenziell als besonders belastend erlebt. In Bezug auf sexuelle Grenzverletzungen sowie Hass und Hetze in Gaming-Kontexten zeichnen sich bei einigen Teilnehmenden Tendenzen zur Desensibilisierung und Resignation bzw. ein Gefühl von Machtlosigkeit ab. In Fällen von Cybergrooming fällt es den Betroffenen anfangs häufig schwer, die Situation richtig einzuschätzen, da der zunächst freundschaftliche Beziehungsaufbau mit positiven Gefühlen verbunden ist.

3.4.2 Umgang mit belastenden Online-Erfahrungen

Hinsichtlich des Umgangs mit negativen Interaktionserfahrungen lässt sich, zumindest bei „Risiko-erfahrenen" Jugendlichen, eine Art **Standard-Coping-Repertoire** feststellen, das darauf abzielt, den unangenehmen Kontakt abzubrechen: ignorieren, blockieren und ggf. melden. Je nach Dynamik, Dauer des Kontakts, Beteiligten (bekannt vs. unbekannt) und Intensität des Belastungserlebens wird dieses Vorgehen um emotionsorientierte Strategien und die Suche nach Unterstützung ergänzt. Dabei zeigt sich eine Unterstützungskaskade: Sind die individuellen Bewältigungsbemühungen allein nicht ausreichend, wenden die Betroffenen sich zunächst an ihr persönliches Umfeld, meist Eltern und Freund:innen. Nur im Notfall ziehen sie institutionelle Unterstützung (z.B. Polizei, seelsorgerische Beratungsangebote) in Erwägung. Vorbehalte und Unsicherheiten zeigen sich vor allem in Bezug auf Polizei und Strafverfolgung sowie Meldemöglichkeiten auf den Plattformen.

3.4.3 Wünsche, Ideen und Anregungen Jugendlicher für ein sicheres Internet

Zur Frage, wie Sicherheit für Kinder und Jugendliche im Internet erhöht und potenzielle Belastungen reduziert werden können, wurden im Verlauf des Projekts nicht nur Stakeholder konsultiert (Stakeholder-Workshops), sondern zusätzlich auch diejenigen, die es unmittelbar betrifft: **Jugendliche selbst**. Im Herbst 2023 wurden vier ganztägige Co-Creation-Workshops mit Schüler:innen der 8. und 9. Klasse an zwei Hamburger Schulen (einem Gymnasium und einer Stadtteilschule) durchgeführt. Neben einer gemeinsamen Reflexion relevanter Interaktionsrisiken standen ihre Ideen und Anregungen zur Verbesserung der Online-Sicherheit und die Entwicklung konkreter Lösungsvorschläge im Fokus. Entstanden sind dabei Vorschläge, die (A) die Gegebenheiten der Plattformen, (B) Unterstützungs- und Beratungsmöglichkeiten und (C) die individuellen Risiko- und Bewältigungskompetenzen betreffen:

A) **Sichere Plattformen:** Die Teilnehmenden fordern strengere Regeln und Konsequenzen für Fehlverhalten auf Online-Plattformen sowie technische Lösungen wie KI-ba-

sierte Programme zur Erkennung und Verhinderung von Beleidigungen und sexuellen Inhalten. Zudem wünschen sie sich Altersverifikationen und getrennte Versionen von Apps für verschiedene Altersgruppen (z.B. Instagram Kids für Minderjährige).

B) **Unterstützung und Beratung:** Die Jugendlichen betonen die Notwendigkeit präventiver Maßnahmen zur Sensibilisierung für Online-Risiken und Beratungsmöglichkeiten nach negativen Erfahrungen. Letztere müssen aus ihrer Sicht an Bekanntheit gewinnen (beispielsweise durch *Influencer*-Kampagnen und Werbemaßnahmen). Zudem schlagen sie schulische und außerschulische Programme zur Stärkung des Selbstbewusstseins und der persönlichen Widerstandsfähigkeit vor.

C) **Wissen und Können:** Risikokompetenz, Medienkompetenz und Resilienz sind aus Sicht der Jugendlichen entscheidende Fähigkeiten, um sich sicher durch die digitale Welt zu navigieren. Kinder sollten, aus ihrer Sicht, daher frühzeitig über Online-Risiken aufgeklärt und Fähigkeiten gestärkt werden, um Risiken zu vermeiden und im Ernstfall souverän mit ihnen umzugehen.

Die Ergebnisse der Workshops finden sich in Form eines Werkstattberichts auf dem Media Research Blog des Leibniz-Instituts für Medienforschung (Thiel & Lampert 2024).

Die Arbeit an den Schnittstellen der Teilbereiche und die skizzierten Projektergebnisse zeigen auf, dass rein disziplinäre Zugänge angesichts der Vielschichtigkeit der Problemsituation zu kurz greifen. Andererseits bedürfen interdisziplinäre Ansätze ausreichend Zeit für Prozesse, voran einen Erkenntnisaustausch, durch den die Ergebnisse immer wieder neu zusammengeführt werden. In dieser Hinsicht hat die entstandene vernetzte Forschungsmethode im Projekt weiterführbare Erfahrungswerte ermöglicht. Es ist ein Kernergebnis des Abgleichs, dass es bei einem komplexen Themenfeld wie der Stärkung von Online-Sicherheit für junge Menschen auf verschiedene Zugänge, Methoden und Perspektiven und damit auch auf viele Akteursgruppen im Zusammenspiel ankommt. Die folgenden Forschungsergebnisse können für das Akteursnetzwerk im Bereich Sicherheit und Kinder- und Jugendmedienschutz festgehalten werden.

TEIL II: Systematik und Anwendungsbezug

4. Das Akteursnetzwerk: Vernetzte Verantwortung als Ankerpunkt nachhaltiger Sicherheit

In der SIKID-Projektarbeit wurden der **Ansatz vernetzter Verantwortung** auf den **Bereich von Interaktionsrisiken bezogen und zentrale Akteure identifiziert, die gemeinsam Verantwortung im Themenfeld tragen**. Ausgehend von Kindern und Jugendlichen selbst, die im Zentrum der Analyse standen, wurden verschiedene Akteursgruppen zusammengefasst, die jeweils eine **Teilverantwortung** für die Sicherheit von Kindern in digitalen Umgebungen sowie die Stärkung kindlicher Rechte tragen.

Abbildung 1: Das Akteursnetzwerk

Kennzeichnend ist dabei, dass es ein **ganzes Netzwerk an Akteuren braucht, um Sicherheit als Kinderrecht zu stärken**. Keine Akteursgruppe kann dieses Ziel allein umsetzen. Da viele Akteursgruppen angesprochen sind, ist es gleichzeitig wichtig darauf zu achten, dass es **nicht zu Phänomenen der Verantwortungsdiffusion bzw. Verantwortungsleerstellen kommt**, indem sich Akteure auf andere Akteure verlassen oder ihre Verantwortung auch aufgrund fehlender Einforderung (rechtlicher oder auch moralischer Art) nicht wahrnehmen (müssen) (siehe zum ethischen Verantwortungsbegriff bei medialem Handeln und Regulierung auch Stapf 2006; Funiok 2007). Somit zeigt sich auch in der Verwobenheit der unterschiedlichen Zugänge aus Ethik, Recht, Pädagogik und Psychologie, dass die Online-Sicherheit von Kindern wesentlich einer vernetzten Verantwortung bedarf.

Verantwortung und Freiheit als komplementäre Konzepte

Fragen der Sicherheit stehen in einem (teilweise ambivalenten) Zusammenhang zu Fragen der Freiheit. Denn, um selbstbestimmte Entscheidungen – auch in Kontexten der Unsicherheit – treffen zu können, bedarf es eines weitgehend sicheren Umfeldes, das andererseits aber nicht die Grundfreiheiten der Individuen beschneiden darf, nur um Sicherheit herzustellen. Entscheidend für die Wahrnehmung von Freiheit ist es, dass eine bewusste Wahl möglich wird, und auf diese Weise auf eigene Lebensentscheidungen eingewirkt werden kann. Freiheit, Verantwortung und Autonomie sind Leitwerte der Medienethik. Als „Krisenreflexion" (Riedel 1979) hat die Medienethik eine „praxisbegleitende, -erklärende und praxisregulierende Funktion" (Wunden 1998) und strebt eine „verantwortete Freiheit" (Stapf 2016) an. Gerade die digitale Mediengesellschaft hat Techniken hervorgebracht, deren Einsatz mit ethischen Herausforderungen einhergeht, sowie Akteuren und Intermediäre, die Einfluss auf die öffentliche Meinungsbildung nehmen (Prinzing & Stapf 2024) und das Einfordern von Verantwortung erschweren. Regulierungslücken mit Blick auf plattformisierte Öffentlichkeiten zeigen sich an Sicherheitsgefährdungen für junge Menschen. Aus medienethischer Perspektive gilt die Verantwortungsfrage als zentral: Aufgrund der besonderen Schutzbedürftigkeit von Kindern, die diese Plattformen nutzen, und im Kontext von Regulierungslücken ist zu bestimmen, welche Akteure welche Verantwortung tragen und wie diese eingefordert werden kann. Modelle vernetzter Verantwortung (Stapf 2016) betonen, dass einzelne Akteure zwar keine Gesamtverantwortung tragen können, aber bei steigender Macht und bei wachsendem Einfluss mehr Verantwortung tragen müssen (Krainer 2002, S. 168), weil es sonst zur Verantwortungsdiffusion oder zu einem Verantwortungsvakuum kommen kann. Zentrale Aspekte für die Wahrnehmung von Verantwortung sind die W-Fragen: Wer (Subjekt) ist für was (Objekt: Handlung/Unterlassung), wem gegenüber (Adressat), vor welcher Instanz, warum (Normen) und in welcher Zeitperspektive verantwortlich? (Stapf & Prinzing 2024; Funiok, 2002).

Wesentlich kommt es daher auf **Schnittstellen und Brücken an, die den Austausch, Transfer und Feedback unter den Akteuren ermöglichen** und sich dabei auf die übergeordnete Zielsetzung beziehen, Sicherheit als Kinderrecht im Digitalen zu gewährleisten. Im Rahmen der **SIKID-Akteursanalysen** wurden auf Basis des Rechtsrahmens formal zuständige Stellen und zugewiesene Verantwortlichkeiten gesichtet und in unterschiedliche Stakeholderkategorien eingeordnet. Die Ergebnisse wurden auf Basis von strukturierten Recherchen nach gesetzlich nicht genannten, aber in der Praxis relevanten Organisationen und Stellen erweitert und in ein Akteursmapping für den Bereich der Online-Sicherheit von Kindern überführt.

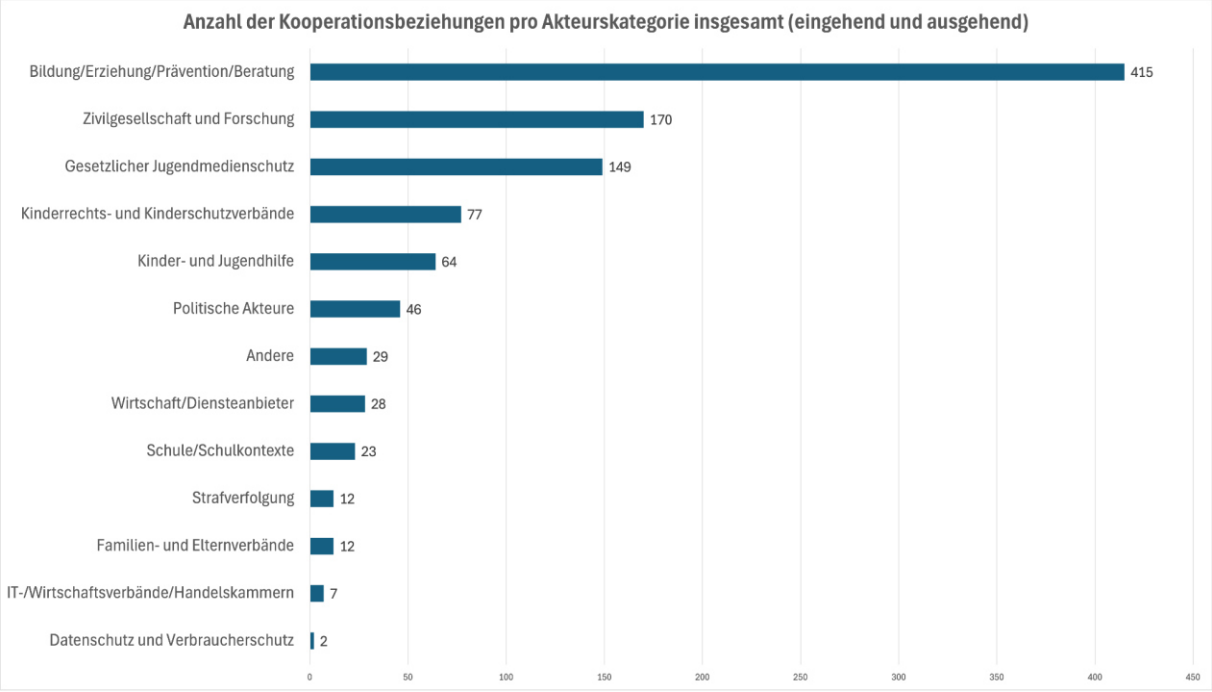
Kernergebnis des Mappings ist, dass Online-Interaktionsrisiken eine ganze Reihe von Rechtsmaterien und damit auch zuständigen Stellen berührt; die gesetzlich genannten Akteure treffen in der Praxis auf eine Vielzahl weiterer relevanter Stakeholder: Der Phänomenbereich weist grundsätzlich ein sehr breites und weites Netz von Akteuren auf; je nach Granularität der Betrachtung handelt es sich bei Online-Interaktionsrisiken von Kindern um ein rechtliches und Praxisfeld, das 120 bis 40.000 Akteure alleine in Deutschland umfasst.[5]

Die akteursbezogenen Rechtsanalysen konnten bereits gesetzlich vorgesehene Kooperationsformen zwischen zwei oder mehr unterschiedlichen Stellen identifizieren. Angesichts der

[5] Die hohe Zahl der Akteure in diesem Bereich erklärt sich bei einer sehr granularen Betrachtung insbesondere durch die hohe Anzahl von Schulen (~32.700), Jugendämter (~600) und Einrichtungen der offenen Kinder- und Jugendarbeit (~5.000) auf kommunaler Ebene.

meist in sich geschlossenen Rechtsbereiche und Gesetzeswerke finden sich aber **nur wenige gesetzlich vorgesehene Verschränkungen und Kooperationsformen zwischen unterschiedlichen Rechtsrahmen** (wie etwa die Verzahnung der Kommission für Jugendmedienschutz (KJM) und der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) oder die Meldepflichten von digitalen Diensten an das BKA). Erst mit der JuSchG-Reform 2021 wurden erste Schritte in Richtung einer bereichsübergreifenden – wenn auch nicht zwingend formalisierten – Zusammenarbeit und Koordination, ausgehend von der BzKJ als Aufgabenträger (vgl. § 17a JuSchG), manifest. Im Rahmen des ersten SIKID-Workshops 2022 mit Stakeholdern wurde deutlich, dass daneben eine **größere Zahl von Akteurskooperationen auf untergesetzlicher und informeller Ebene stattfindet.** Eine Akteurserhebung zu Kooperationsformen und -erfahrungen sowie die daran anschließende qualitative Netzwerkanalyse im Frühsommer 2024 haben gezeigt, dass sich in der Praxis eine große Zahl von Kooperationsbeziehungen und -praxen herausbilden (Dreyer, Andresen & Wysocki 2024, i.E.): **Der Querschnittscharakter von Online-Sicherheit von Kindern bildet sich ab in vielzähligen bereits bestehenden Akteurs- und Kooperationskonstellationen,** mit einzelnen Foren (z.B. ZUKUNFTSWERKSTATT der BzKJ, National Coalition – Netzwerk zur Umsetzung der UN-Kinderrechtskonvention) und Gremien (z.B. Beirat des deutschen Safer Internet Centres klicksafe.de, Expert:innenkreis Kinderrechte in der digitalen Welt beim DKHW); als akteursbereichsübergreifende Schnittstellen.

Abbildung 2: Anzahl der Kooperationsbeziehungen von Akteurskategorien im Bereich Online-Sicherheit von Kindern



Dabei wird deutlich, dass sich insbesondere der gesetzliche und erzieherische Jugendmedienschutz stark aufeinander zubewegen bzw. sich zunehmend verschränken, und zwar auf der Akteursebene wie auf der Inhaltsebene. Durch die Einführung des **Schutzziels der „persönlichen Integrität"** in das Jugendschutzgesetz 2021 und die damit einhergehende spezifische **Erweiterung des Rechtsrahmens im Jugendmedienschutz um Interaktions- und**

Kommunikationsrisiken führen zu einer **Konvergenz gesetzlicher und erzieherischer Maßnahmen** – und damit auch zu vermehrten Überlappungen und Kooperationen von Akteursgruppen bzw. Akteuren.

Auffällig bei den Akteurs- und Netzwerkanalysen ist die im Vergleich **schwache Ausprägung von Verbindungen der Sicherheitsbehörden zu anderen Akteurskategorien**[6]: Hier gibt es neben den gesetzlich vorgesehenen Meldepunkten, etwa von Hotlines und Beschwerdestellen, in Richtung des BKA und der Teilnahme von Sicherheitsbehörden an einzelnen Gremien nur vereinzelte Kooperationen zwischen etwa den Präventionsstellen der Polizei oder den Staatsanwaltschaften mit Akteuren etwa des erzieherischen Jugendmedienschutzes (z.B. die Kooperation des Projekts ZEBRA mit der ZAC NRW oder die Initiative „Verfolgen statt Löschen"), obwohl beide Seiten von Kooperationen profitieren könnten.

Abbildung 3: Anzahl der angegebenen Kooperationsbeziehungen der Akteurskategorien untereinander

Beispielsweise verfügen die Sicherheitsbehörden aufgrund der Verfolgung von einschlägigen Straftaten über Einblicke in Kommunikations- und Handlungsverläufe bei Online-Interaktionsrisiken. Sie kennen Motive und Vorbereitungshandlungen, Praktiken der Verschleierung

[6] Ein interaktives Sehnen-Diagramm der unterschiedlich stark ausgeprägten Beziehungen zwischen den Akteurskategorien findet sich auf https://public.flourish.studio/story/2445976/.

und Entdeckungsverhinderung und Formen der Ansprache und Vertrauensgewinnung durch Täter:innen. Gleichzeitig verfügen Fachkräfte in der Medienpädagogik und bei Institutionen der Medienbildung über besondere didaktische Erfahrungen der niederschwelligen und altersgemäßen Vermittlung von Befähigung und Schutz an Kinder und Jugendliche. Kriminalpolizeiliche Präventionsstellen können hier theoretisch eine besondere Schnittstellenfunktion zwischen den beiden Bereichen übernehmen. In der Praxis zeigt sich in der Art der Ansprache und Kommunikation eine starke Gewichtung der strafrechtlichen Relevanz von bestimmten Verhaltensweisen, wo es aus Kindersicht ggf. offenerer Dialoge über Informations- und Kommunikationsbedürfnisse sowie Nutzungspraktiken und -risiken bräuchte.

Auch die qualitativen Aussagen über Hürden bei der Kooperation mit anderen Akteuren im Rahmen der Netzwerkanalyse deuten darauf hin, dass Sicherheitsbehörden für andere Akteursgruppen besondere Herausforderungen darstellen: Teilweise sind Ansprechpartner:innen unklar, teilweise gibt es keine Ressourcen oder kein Interesse an Kooperationen außerhalb der Strafverfolgung, und Kooperationen sind dann abhängig von motivierten Einzelpersonen. Sicherheitsbehörden verweisen im Gegensatz dazu auf ihre hohe Auslastung und den gesetzlichen Auftrag zur Strafverfolgung, der nur in begrenztem Umfang Kooperationen im Bereich der strafrechtlichen Prävention zulässt – und darüber hinaus wenig Möglichkeiten bei Kooperationen mit Akteuren aus der Medienbildung lässt.

Insgesamt haben die Untersuchungen der Governance-Strukturen im SIKID Projekt gezeigt, dass Kommunikations- und Interaktionsrisiken verschiedene Rechtsbereiche und -normen berühren können, und dass die Begegnung von diesen Risiken im Handlungsbereich einer Vielzahl unterschiedlicher Akteursgruppen liegt. Entsprechend vielfältig sind die Hintergründe, Organisationsformen, Agenden und Handlungsmaximen der relevanten Stakeholdergruppen. Zwar gibt es zwischen den Akteuren wenig formelle, aber dafür vielzählige informelle und projektbezogene Kooperationen, insbesondere die Aktivitäten der Medienbildung und von Sicherheitsbehörden bleiben aber größtenteils unverbunden.

Mit Blick auf das Akteursnetzwerk zeigt sich damit, dass eine systematisch angelegte Kooperation hilfreich sein kann, die über informelle Vernetzungen hinausgeht. Deutlich wird, dass dieses Akteursnetzwerk in Grundzügen bereits angelegt ist, dass es aber einer Verstetigung bedarf, um insgesamt bezogen auf Sicherheitsherausforderungen effektiv handeln zu können (siehe auch Kapitel 6, Abschnitt Handlungsoption Akteursnetzwerk).

5. Systematisierung: Ein Modell für Sicherheit von Heranwachsenden online

Um die **Komplexität und Verwobenheit der Sicherheit von jungen Menschen in digitalen Umwelten** aufzeigen, wurde ein **systematisierendes Modell** entwickelt, das zentrale Handlungsfelder aufzeigt, die bei einem kinderrechtlichen Ansatz bezogen auf Interaktionsrisiken (voran Cybermobbing, Cybergrooming, Hate Speech und non-konsensuales Sexting) herangezogen werden sollten. Im Zentrum des Schaubilds stehen Kinder und Jugendliche selbst. Sie sind zentraler Teil im **Netzwerk verschiedener Akteure bzw. Stakeholdergruppen, die**

Verantwortung für die Sicherheit von Kindern tragen. Dies sind Eltern bzw. Sorgeberechtigte, (vor-)schulische und außerschulische Bildung (aber auch Erwachsenenbildung), Sicherheitsbehörden (Polizei, Strafverfolgung usw.), Anbieter (auch mit Blick auf verwendete Technologien) und Entwickler und Gestalter digitaler Angebote, Unterstützungsangebote (wie Hotlines, Opferschutz, Kinder- und Jugendhilfe), Media Governance, darunter vor allem Institutionen des gesetzlichen Kinder- und Jugendmedienschutzes sowie die Forschung und Wissenschaft.

Die komplexe Problemlage im Bereich der Interaktionsrisiken im digitalen Umfeld macht das gesamte **Akteursnetzwerk** zentral, um systemische und nachhaltige Lösungen zu ermöglichen. Das Akteursnetzwerk ist dabei auf gesellschaftlich-kultureller Ebene eingebettet in einen **konkreten Rechtsrahmen und bestehendes Recht**, aber auch **technische Infrastrukturen, gesellschaftliche Moral(en) sowie schließlich auch gelebte Kulturen, die auch die Praxis der Menschenrechte (als gelebte Rechte)** umfassen. Aus dieser Gemengelage heraus entsteht ein Rahmen aus Normen und Werten, die den derzeitigen Maßnahmen zugrunde liegen, z.B. wieviel Sicherheit für Kinder wesentlich ist, was eine „gute Kindheit" ausmacht oder wo strafrechtlich relevante Tatbestände vorliegen, aber auch, was Kinder an „gelebten Menschenrechten" selbst schon erfahren können. Dieses Feld ist wiederum eingebettet in den europäischen Kontext (z.B. Rechtsakte wie der DSA oder der AI Act, aber auch politische Strategien wie die EU-Kinderrechtsstrategie, die Better Internet for Kids+-Strategie oder Rahmenvorgaben des Europarats) und den internationalen Kontext (vor allem die UN-Kinderrechtskonvention).

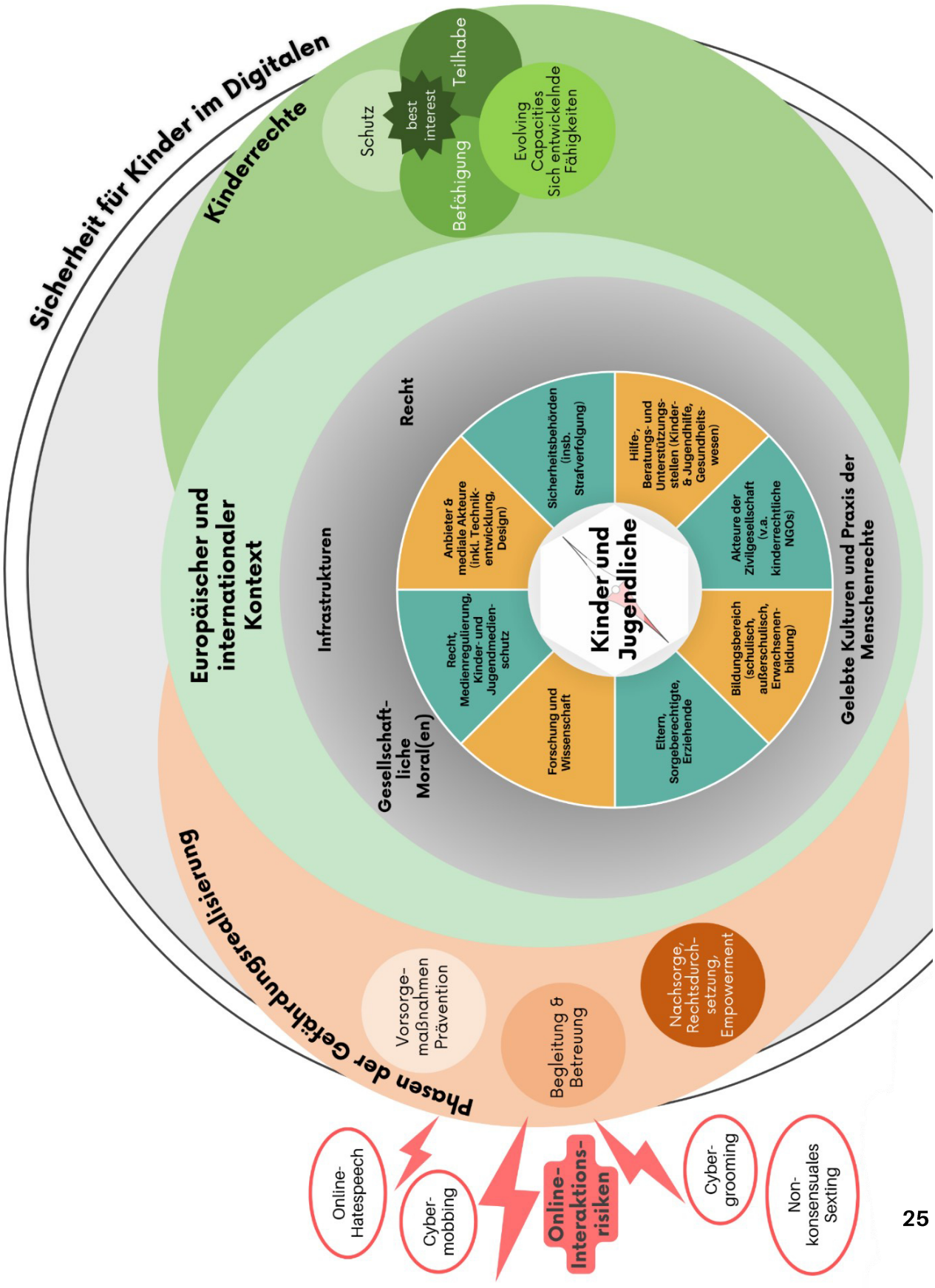
In diese Felder verwoben ist aus kinderrechtlicher Perspektive der Kinderrechte-Dreiklang von Teilhabe, Befähigung und Schutz. Das heißt: Um im Themenfeld Kinderrechte zu stärken, sind einerseits die Kontextbedingungen (Recht, gelebte Moralen, usw.) sowie auch alle relevanten Akteursgruppen zu berücksichtigen. Was die verschiedenen Rechte von Kindern angeht, gilt es weiterhin bei Interaktionsrisiken in digitalen Umgebungen besonders auf die sich entwickelnden Fähigkeiten (*Evolving Capacities*) zu achten, d.h. dass sich sowohl Verletzungen, aber auch Maßnahmen auf **Entwicklungsthemen in der Kindheit** (so auch Sexualität), und damit verbunden auch **Entwicklungsverletzlichkeiten** beziehen (siehe auch Paschel, Schultz, von Salisch & Pfetsch, i.E.). Dabei soll das Kindeswohl (Art. 3 UN-KRK) bzw. das Wohlergehen von Kindern (*Best Interest*) vorrangige Berücksichtigung finden.

Schließlich kommen in einer umfassenden Auseinandersetzung mit Sicherheitsfragen rund um das Thema Kinder in digitalen Welten auch **verschiedene Phasen der Gefährdungsrealisierung** zum Tragen, für die Akteure und Maßnahmen vernetzt abzustimmen sind. Diese sind die Phase der Vorsorgemaßnahmen und Prävention, die Phase der Begleitung und Betreuung, wenn Gefährdungen gerade eintreten oder eingetreten sind und die Phase der Nachsorge, Rechtsdurchsetzung, aber auch das Empowerment betroffener Kinder im Nachgang von Verletzungen, die ihrem auch zukünftigen Wohlergehen dienen sollen.

Das SIKID-Schaubild ermöglicht eine differenzierte Befassung mit dem Themenfeld in seiner Komplexität und kann für weitere Forschung und Entwicklung ausdifferenziert und ange-

passt werden. Um Handlungsoptionen zu erarbeiten, wurden in einem weiteren Schritt Handlungsfelder extrapoliert, die – das Akteursnetzwerk übergreifend – im Themenfeld wirkmächtig sind.

Abbildung 4: Schaubild SIKID-Kompass – Sicherheit für Kinder in der digitalen Welt



TEIL III: Maßnahmen

6. Handlungsfelder und -optionen: Maßnahmen und Handlungsspielräume für das Akteursnetzwerk

Vor dem Hintergrund der vorgestellten Ergebnisse und Erkenntnisse aus den Teilprojekten und den Expert:innen-Workshops im Stakeholder-Netzwerk wurden **sieben zentrale Handlungsfelder mit entsprechenden Handlungsoptionen herausgearbeitet** und interdisziplinär verwoben. Folgende **Handlungsfelder** konnten **identifiziert werden:** Ein Fundament bildet die Kooperation im Akteursnetzwerk, der Bereich von Forschung und Wissenschaft sowie Maßnahmen nach einer eingetretenen Verletzung (z.B. Rechtsdurchsetzung, aber auch die Aufarbeitung von Verletzungen und zukunftsorientierte Befähigung). Darauf aufbauend und damit verbunden sind die Handlungsfelder Fort- und Weiterbildung, Technikentwicklung und -gestaltung, das Handlungsfeld infrastrukturelle Anbietermaßnahmen und Regulierung sowie die schulische und außerschulische Medienbildung.

Abbildung 5: Identifizierte Handlungsfelder

6.1 Handlungsfeld: Kooperation im Akteursnetzwerk

Ein zentrales Handlungsfeld ist die Etablierung, Formalisierung und Verstetigung eines Akteursnetzwerks, in dem Erfahrungsaustausch und die Koordination von Aktivitäten möglich sind. Aus dem Umstand, dass **Kinder- und Jugendmedienschutz als kinderrechtlicher Querschnittsbereich** konzipiert wird und bei seiner effektiven Umsetzung **auf die Akzeptanz aller beteiligten Akteure angewiesen** ist, ergibt sich das **Ziel einer netzwerkgerechten Gestaltung dieses Akteursverbunds.** Das Leitprinzip einer zeitgemäßen Governance von Interaktionsrisiken heißt auch, die notwendige Veränderung in Richtung einer Netzwerklogik anzuerkennen und systematisch zu verfolgen. Dabei können die Handlungsoptionen auf eine Vielzahl bereits gelebter formeller und informeller Kooperationsbeziehungen aufbauen.

Handlungsoptionen für die Kooperation im Akteursnetzwerk

Etablierung bzw. Verstetigung eines Akteursnetzwerks „Prävention von Online-Interaktionsrisiken"

Der erste Schritt sollte die Förderung einer besseren Vernetzung der relevanten Stakeholder sein, insbesondere durch die **Etablierung eines offiziellen, ständigen und ggf. auch formelleren Netzwerks**. Dieses sollte nachhaltig und über einzelne persönliche und Projektbeziehungen hinaus Aktivitäten entfalten, wofür es Unterstützung durch politische Maßnahmen (etwa Beschließen einer mittelfristigen Strategie für ein koordiniertes Akteursnetzwerk samt Strategiepapier wie auch Anschubfinanzierung) braucht. Wichtig ist es, zu prüfen, **in welcher Form** weitere Akteursgruppen (vermehrt) in das Akteursnetzwerk einbezogen werden sollten (z.B. Erziehungsberechtigte, Medienpädagog:innen und Lehrkräfte).

Unterstützung von Kooperation und Koordination im Akteursnetzwerk

Da kinderrechtliche Verbürgungen in digitalen Medienumgebungen als Querschnittsbereich fungieren, die ganz unterschiedliche Stakeholdergruppen berühren, sollte die **Unterstützung eines intensiven Wissens- und Erfahrungsaustauschs** ein zentrales Vorhaben des Netzwerks sein. *Good* und *Best Practice*-Beispiele, Erfahrungen in der Zusammenarbeit und praxisrelevante Evaluationserkenntnisse sollten Kernbereiche des Transfers und Austauschs sein. Ein besonderes Augenmerk sollte dabei auf der Etablierung von fruchtbaren Formen des Austauschs zwischen medienpädagogischen Initiativen und Projekten einerseits und didaktischen Ansätzen der polizeilichen Präventionsarbeit andererseits liegen, da hierdurch beide Seiten voneinander lernen können.

Kooperationen auf kommunaler und regionaler Ebene sichtbarer machen

Es existieren fast flächendeckend Initiativen und Kooperationen zwischen Schulen, Trägern der offenen Jugendhilfe und der Polizei im Bereich der Kriminal- oder Gewaltprävention (insb. Präventionsräte oder -gremien), von denen sich viele bereits auch um neuere medienvermittelte Themen wie Online-Interaktionsrisiken kümmern. Oft sind derartige Zusammenschlüsse jedoch nur dem Fachpersonal vor Ort bekannt. Auch für Kinder und Eltern bzw. Erziehungsberechtigte sollten die genannten Initiativen sichtbarer werden (etwa durch online vorgehaltene und gebündelte Informationen und leicht auffindbare Ansprechpartner:innen), um von ihnen profitieren zu können. Die Vernetzung der Akteursgruppen auf kommunaler und regionaler Ebene kann dabei spezifischer und kontextsensibler auf Gegebenheiten vor Ort eingehen und Erfahrungswerte bündeln.

Kultur(en) für *Positive Plattform Governance* im Netzwerk schaffen

Nicht nur Anbieter haben sich für eine kinderrechtssensible Gestaltung ihrer Angebote einzusetzen, auch **das Akteursnetzwerk insgesamt sollte die Perspektive einer *Positive Platform Governance* einnehmen**: Nicht das rechtlich geforderte Mindestmaß sollte dabei zentraler Orientierungspunkt für die Aktivitäten sein, sondern die **möglichst optimale Gewährleistung der Kinderrechte im Digitalen**. Netzwerkkultur bedeutet hier das Bewusstsein für die Notwendigkeit einer guten Zusammenarbeit aller Beteiligten auf der Basis gegenseitiger Wertschätzung, wobei auch die jeweiligen Ressourcen zu berücksichtigen bzw. bereitzustellen sind, damit dies auch langfristig möglich bleibt. Mit dem neu aufgelegten Förderprogramm

„Kindgerechte digitale Angebote und Maßnahmen zur Orientierung“ der BzKJ existiert hier eine erste unterstützende Förderlinie.

Netzwerkgerechtere Gesetzgebungsverfahren etablieren und leben

Im Gesetzgebungsverfahren werden Einschätzungen zu Gesetzesentwürfen im Bereich der Online-Risiken für Kinder und Jugendliche zwar von vielen Akteuren im Netzwerk eingeholt (z.B. durch Stellungnahmen), dabei bleibt der Gesetzgeber aber der zentrale politische Akteur. Nimmt man den oben beschriebenen Netzwerkgedanken ernst, wird die Notwendigkeit der Stärkung einer Konsultations- und Zusammenarbeitskultur bei der Gesetzgebung im Zusammenhang mit Kinder- und Jugendmedienschutz deutlich. Das Einholen von Stellungnahmen reicht dann nicht mehr, sondern es bedarf einer frühzeitigen Einbindung aller Akteure (z.B. im Rahmen von konstruktiven *Legal Design Jams* oder *Legal Clinics*, Donoso et al. 2011), in denen die Grundlagen eines Problems, mögliche Ansätze mit ihren Herausforderungen und Vor- und Nachteilen geprüft und anhand des vorhandenen Akteurswissens priorisiert und ausgestaltet werden. Hilfreich ist auch eine Veränderung der Gesetzgebungskultur, in der die Übernahme von Verbesserungsvorschlägen in neue Entwürfe deutlich gemacht würden. Die Quelle(n) eines Vorschlags würden auf diese Weise sichtbarer, was die Netzwerkarbeit weiter stärken und die Akzeptanz der Gesetzgebung fördern kann.

6.2 Handlungsfeld: Forschung und Wissenschaft

Die Wissenschaft bietet wesentliche Grundlagen für das gesamte Akteursnetzwerk. Das Generieren von Wissen, empirischen Grundlagen, die Evaluation von Maßnahmen, aber auch der Bezug zu demokratischen Grundwerten und der reflektierte Umgang mit Ambivalenzen und Spannungsfeldern sowie ihre Vernetzungsfunktion macht die Wissenschaft zu einem zentralen Handlungsfeld für die Sicherheit von jungen Menschen in digitalen Umgebungen.

In diesem Handlungsfeld zeigt sich, dass **Sicherheitsfragen einer unabhängigen, interdisziplinären (und teils transdisziplinären), praxisbezogenen und auch langfristig wirksamen Forschung bedürfen.** Für die Forschung zu Sicherheitsfragen ist nicht nur die zivile Sicherheitsforschung selbst wesentlich, sondern auch andere Fachdisziplinen, da Sicherheitsfragen als hochkomplex zu verstehen und anzugehen sind. Um Maßnahmen für Kinder und Jugendliche (als besonders vulnerable gesellschaftliche Gruppe) zu entwickeln, sollte die Forschung inter- und transdisziplinär und im Zusammenspiel mit Akteuren der Praxis durchgeführt werden. Hierzu gilt es, **Forschungsförderung daraufhin auszugestalten und auch stärker als bisher in ihrer Nachhaltigkeit zu fördern.** Denn Sicherheitsfragen im Digitalen entwickeln sich zum einen kontinuierlich und schnell weiter, aber auch die Evaluation der Ergebnisse und ihre Verankerung in der Praxis sollten langfristig begleitet werden.

Insoweit es um Sicherheitsfragen bezogen auf junge Menschen geht, zeigt sich überdies, dass **Gelingensbedingungen für die notwendige partizipative Forschung mit Kindern** zu berücksichtigen sind. Aus einer kinderrechtlichen Perspektive sind Kinder in allen sie betreffenden Belangen zu beteiligen, also auch bezüglich der Teilnahme und Mitwirkung an Forschung (Alderson & Morrow 2004, Bell 2008, Nairn & Clarke 2012). Dabei sind in Bezug auf Kinder aufgrund ihrer sich entwickelnden Fähigkeiten und des ihnen zugesprochenen Schutzstatus besondere Aspekte zu berücksichtigen, die in der Medienforschung zu Online-

Interaktionsrisiken wie Cybergrooming, Online Hate Speech, Cybermobbing oder sexuellen Grenzverletzungen bei Kindern deutlich werden. Gerade in sensiblen Themenbereichen, die mit Scham, Loyalitätsfragen oder gar Trauma verbunden sind, ist diese Forschung allerdings von Spannungsfeldern geprägt, etwa zwischen Schutz- und Partizipationsrechten, Forschungszielen und dem individuellen Kindeswohl (Pfetsch et al. 2024; Stapf, Bieß, Pfetsch & Paschel 2023).

Handlungsoptionen für die Forschung und Wissenschaft

Forschende befähigen, sicherheitsrelevante Fragen ethisch zu bearbeiten

Damit Forschung zu sensiblen Themenbereichen ethisch reflektiert durchgeführt werden kann, sind Fortbildungs- und Informationsangebote für Forschende der zivilen Sicherheitsforschung wesentlich, die sie mit forschungsethischen Grundlagen und konkreten Reflexionskriterien für den Einbezug von Kindern vertraut machen. Die Fortbildungsangebote sollten auch Grundlagen einer Abwägung verschiedener Güter, die Gestaltung von Prozessen v.a. bei partizipativer Forschung, forschungsethische Fragen zu entwicklungsangemessenen Methoden in sämtlichen Phasen des Forschungsprozesses umfassen. Über Fortbildungen hinaus sollte die Bedeutung eines kinderrechtlichen Ansatzes und seiner ethischen Implikationen für die Sicherheitsforschung in der Ausbildung, in der wissenschaftlichen Alltagspraxis und in der Wissenschaftskommunikation präsent sein.

Kinder stärker als bisher in Forschung einbeziehen

Kinder sollten aus kinderrechtlicher Sicht in unterschiedliche Schritte des Forschungsprozesses einbezogen werden. Hierzu sollten verschiedene und möglichst niederschwellige Optionen (und Intensitätsgrade) der Partizipation angeboten werden (z.B. Workshops, Werkstattformate, Kolloquien), um Kindern unterschiedlicher Altersstufe und Milieus eine Beteiligung zu ermöglichen. Für sehr engagierte Kinder können dies Formate wie Forschungskolloquien mit Kindern oder auch Journals für Kinder und Jugendliche sein, bei denen diese als Reviewer auftreten, für Kinder mit weniger Zeit und Engagement aber auch niederschwellige Formate wie punktuelle Workshops beispielsweise zu Perspektiven junger Menschen auf spezifische Interaktionsrisiken. Zentral ist es, dass die Ergebnisse partizipativer Forschungsprojekte auch an Kinder zurück gespiegelt, mit ihnen diskutiert oder gar gemeinsam entworfen werden (siehe als Best Practice-Beispiel den Bericht „Our Rights", der in kindgerechter Sprache zentrale Aspekte des General Comments Nr. 25 im Rahmen einer Befragung von Kindern für Kinder selbst aufbereitet (Third & Moody 2021). Damit partizipative Forschung gelingt, braucht es Ressourcen für Kinder- und Jugendbeteiligung, vor allem aber Zeit und Raum. Sinnvoll ist es dabei, den „Kosmos der Kinder", d.h. ihre konkreten lebensweltlichen Bezüge mit einzubeziehen, indem die Partizipation in ihre Lebenswelten eingebettet wird. Beispielsweise kann es hilfreich sein, Jugendzentren einzubinden und auf Kinder- und Jugendbeiräte bzw. -panels zurückzugreifen. Aus kinderrechtlicher Perspektive sind auch das angemessene Maß und die angemessene Form von Partizipation ethisch zu reflektieren, um Überforderungen bei beteiligten Kindern, „Scheinpartizipation" oder Partizipation ohne Folgen zu vermeiden. Partizipation von jungen Menschen sollte folglich auch einen echten Einfluss (*impact*) haben.

Mehr empirische Forschung zu intersektional marginalisierten Kindern durchführen und fördern

Bislang existieren wenige Informationen über die besonderen Erlebnisse von Kindern, die marginalisierten sozialen Gruppen angehören. Es fehlen beispielsweise Erkenntnisse zu ihren (verstärkten) Erfahrungen von Hass und Ausbeutung oder auch zu den Gründen des Versagens von Schutzmechanismen. Auch besteht ein Mangel an kulturell und sozial sensiblen Ansätzen zur Prävention von Interaktionsrisiken bei intersektional marginalisierten jungen Menschen. In Rückbezug auf die vorhergehenden Empfehlungen ist es wichtig zu fragen, wie marginalisierte junge Menschen angemessen an Forschung beteiligt werden können, um ihre Perspektiven ausreichend zu berücksichtigen.

Die Nachhaltigkeit der Vernetzung und den Erfahrungsaustausch im Forschungsfeld fördern

Gerade bei sensiblen Themenbereichen ist der Austausch unter Forschenden wesentlich, um auf bestehende Erfahrungswerte aufbauen und Methoden optimieren zu können. Dies erfordert eine Wissenschaftskultur, in der es Bereitschaft dafür gibt, eine offene Fehlerkultur zu entwickeln, um gegenseitig aus Fehlern, aber auch aus Erfolgen zu lernen. Dies im Netzwerk zu etablieren könnte z.B. durch eine Austausch-Plattform für Erfahrungswerte geleistet werden (Stapf, Bieß, Pfetsch & Paschel 2023), die über internationale Dachverbände oder durch internationale Netzwerkförderung im Gebiet der Sicherheitsforschung initiiert und gepflegt wird. Beispiele können geteilte Formulare zur informierten Einwilligung oder methodische Konzepte für besondere Kontexte sein. Eine solche auf Nachhaltigkeit und Synergien ausgelegte Vernetzung kann insbesondere als Teil eines umfassenden Akteursnetzwerk Wirkung erzielen (siehe 6.1 Handlungsfeld Akteursnetzwerk).

Anreizsysteme und Fördermöglichkeiten für forschungsethisch fundierte Forschungsprojekte schaffen und strukturell fördern

Um Kinder systematisch an der empirischen Forschung zu Interaktionsrisiken beteiligen zu können, braucht es Anreize und Fördermöglichkeiten für fundierte Forschungsprojekte, die Forschungsethik kontextspezifisch ausgestalten und Methoden für angemessene Partizipation entwickeln. Hierzu können Plattformen zum Austausch von Forschenden auf internationaler Ebene weiterführend sein, die Vernetzungsmöglichkeiten zur Forschung in sensiblen Themenbereichen anbieten, um Methoden weiter auszudifferenzieren (Stapf, Bieß, Pfetsch & Paschel 2023).

Theorie- und Empirie-gestützte Entwicklung von Materialien zur Prävention von Online-Interaktionsrisiken fördern

Gerade für neu entstehende Risiken und Risikobereiche sollten zielgruppenspezifische Präventions- und Unterstützungsmaterialien bedarfsorientiert und im Austausch von Wissenschaft und Praxis entwickelt werden. Im Idealfall sollten die Materialien pädagogisch erprobt und wissenschaftlich evaluiert werden, um gegebenenfalls Anpassungen vornehmen zu können, sowie wissenschaftlich auf ihre Wirksamkeit hin analysiert werden, um die Präventionspraxis durch evidenzbasierte Materialien zu unterstützen. Dies erfordert die Bereitstellung entsprechender zeitlicher, personeller und finanzieller Ressourcen, wodurch jedoch positive Auswirkungen auf die Qualität, Nutzung und Effektivität zu erwarten sind.

6.3 Handlungsfeld: Maßnahmen nach Verletzungen (Unterstützung Betroffener, Ermittlung Verursachender)

Betroffene von Übergriffen und kriminellen Handlungen brauchen ein gutes und umfassendes **Unterstützungs-Ökosystem, das sich an den Bedarfen im konkreten Verletzungsmoment und im Nachgang orientiert.** Dies ist insbesondere für Interaktionsgefahren online relevant, da es nicht selten zu einer vielschichtigen **Viktimisierung** Betroffener kommt. Gleichzeitig müssen **Ermittlungsaktivitäten effizient und effektiv gestaltet** sein, um Personen, von denen Verletzungen oder illegale Handlungen ausgehen, zu identifizieren und – wo nötig und angemessen – mit spürbaren Sanktionen belegen zu können. Nur dann kann aus der Verfolgung von Übergriffen ein **Präventionseffekt für künftige Handlungen** folgen. Ein besonderer Umstand ist, dass auch **Kinder und Jugendliche** im Bereich von Kommunikations- und Interaktionsrisiken **nicht nur Betroffene von Grenzverletzungen sein können, sondern ggf. selbst (auch) als Verletzende agieren,** wobei die Rollen teils dynamisch sind und sich innerhalb eines Kommunikationszusammenhangs verändern können.

Handlungsoptionen für die Stärkung von Maßnahmen nach Übergriffen

Verbesserung der Bekanntheit und Zugänglichkeit von Unterstützungs- und Beratungsangeboten für Kinder und Jugendliche

Für Kinder und Jugendliche ist es zentral, **im Falle von Verletzungen, Übergriffen oder Straftaten umgehend Unterstützung zu erhalten.** Wichtige Akteure sind hier Beratungsstellen, die im Rahmen (ggf. anonymer) Beratung professionelle Hilfe bieten. Die **Bekanntheit von derartigen Unterstützungs- und Beratungsangeboten** deutlich zu erhöhen ist daher essentiell, etwa durch Werbekampagnen, kontextbezogene Verlinkungen auf relevante Angebote, aber auch durch institutionelle Vernetzung, um die Personen mit Hilfsbedarfen schnell an relevante Angebote vermitteln zu können. Um die Nutzung von Beratungsangeboten niederschwelliger zu machen, sollten diese hinsichtlich des Ablaufes transparent sein, gerade auch, was die Geheimhaltung angesichts von Kinderinteressen und die Folgen des Hinzuziehens Dritter angeht.

Verbesserung der Unterstützung von Betroffenen

Im Nachgang zu einer Verletzung sind eine **schnelle und gute psychosoziale Beratung und Begleitung von Betroffenen** (auch im Kontext von Gerichtsverfahren) wichtig. Hier können Verfahren helfen, die größtmögliche Anonymität wahren, zügige persönliche Unterstützung und ggf. einen flexiblen Schulwechsel ermöglichen. Mittelfristig zu diskutieren sind daneben mögliche Fonds für die Entschädigung von Opfern. Rechtspolitisch ist zu diskutieren, inwieweit die Geheimhaltungsinteressen von Kindern im Rahmen höchstpersönlicher Kommunikation den Erziehungsrechten der Eltern entgegenstehen. Dies hätte zur Folge, dass über Möglichkeiten z.B. der Erstattung einer Strafanzeige durch Minderjährige oder der Ermöglichung von Begleitpersonen für Kinder und Jugendliche in Gerichtsverfahren, nachgedacht wird.

Gewährleistung einer effizienten Verfolgung von Rechtsverstößen

Die Verfolgung von Rechtsverletzungen dient nicht nur der Umsetzung bestehenden Rechts, sondern kann auch vor zukünftigen Verletzungen schützen, insbesondere durch die Erhö-

hung des Entdeckungs- bzw. Vollzugsdrucks. Mit Blick auf die sehr unterschiedlichen Verletzungshandlungen bei Online-Interaktionsrisiken erscheinen **Verbesserungen im Sexualstrafrecht** vor allem bei Formen der aufgedrängten sexualisierten Gewalt notwendig. Gleichzeitig müssen Reformen auf die systematische Entkriminalisierung von Jugendlichen abzielen, die derzeit im Rahmen konsensualen Sextings unter Gleichaltrigen in den Bereich der Strafbarkeit fallen. Ob und inwieweit ausschließlich das Strafrecht zur Verfolgung von Verletzungen gelangen soll, bleibt einer weiteren Untersuchung und rechtspolitischen Diskussionen vorbehalten. So kann etwa auch die (geplante) Einführung eines Digitalen Gewaltschutzgesetzes zu der Verbesserung der Rechtsschutzmöglichkeiten Betroffener führen. Als ambivalent sind dagegen Teile der rechtspolitischen Vorschläge zu bewerten, die auf eine Verbesserung ermittlungstechnischer Möglichkeiten von Sicherheitsbehörden abzielen, etwa durch eine anlasslose Vorratsdatenspeicherung oder Formen automatisierter Erkennung und Ausleitung von vermeintlich strafrechtsrelevanten Verhaltensweisen. Mit Blick auf derartige Vorschläge ist eine grundlegende Handlungsempfehlung, dass die **Gewährleistung von Grund- und Menschenrechten** (auch der von Kindern und Jugendlichen), die Wahrnehmung besonders sensibler Abwägungspflichten und die umfassende Prüfung der Verhältnismäßigkeit von geplanten Maßnahmen im Vordergrund legislativer Überlegungen stehen müssen.

6.4 Handlungsfeld: Schulische und außerschulische Medienbildung für Kinder und Jugendliche

Die schulische Bildung in Deutschland liegt stark in der Verantwortung der Bundesländer. Es gibt zwar verbindliche, bundesweit geltende Bildungsstandards für bestimmte Klassenstufen bzw. Schulabschlüsse sowie für ausgewählte Kernfächer, die von der Kultusministerkonferenz (KMK) verabschiedet werden. Die Implementation dieser Standards in landeseigene Vorgaben stellen allerdings die Bundesländer sicher. Auch die Medienbildung betreffend hat die KMK 2016 die Strategie zur „Bildung in der digitalen Welt" verabschiedet und 2021 durch „Lehren und Lernen in der digitalen Welt" ergänzt. Teil dieser Strategie ist ein **verbindlicher Kompetenzrahmen**, der die sechs Bereiche Suchen und Verarbeiten, Kommunizieren und Kooperieren, Produzieren und Präsentieren, Schützen und sicher agieren, Problemlösen und Handeln sowie Analysieren und Reflektieren umfasst (KMK 2016, 2021). Zwar ist auch die **Medienbildung in den Curricula der Bundesländer verankert, allerdings in unterschiedlicher Form und in unterschiedlichem Ausmaß**. Mit dem DigitalPakt Schule erhalten die Bundesländer durch den Bund Finanzhilfen zur Förderung der digitalen kommunalen Bildungsinfrastruktur (IT-Systeme, Vernetzung von Schulen, länderübergreifende digitale Bildungsinfrastruktur). Die Verantwortung für die Fort- und Weiterbildung des pädagogischen Personals liegt bei den Bundesländern (BMBF 2019). Das Handlungsfeld der **schulischen Medienbildung** ist also, u.a. aufgrund der föderalen Struktur der Bildungslandschaft, **sehr heterogen und komplex**. Hinzu kommen Unterschiede zwischen einzelnen Schulen hinsichtlich der technischen Ausstattung, personeller Ressourcen, Kompetenzen des pädagogischen Personals sowie der schulischen Medienkonzepte.

Gerade das breite Feld der Medienbildung vor dem Schuleintritt und ergänzend zur schulischen Medienbildung kann stärker vom Kind aus Angebote machen, die Heranwachsende

auch in weniger formalisierten Settings und außerhalb des schulischen Machtgefüges sensibilisieren und stärken. Zu den außerschulischen Angeboten zählen u.a. Jugendzentren, Medienkompetenzzentren, Landesmedienanstalten, bundesweite Projekte (z.B. Klicksafe, juuuport, Internet ABC) und verschiedenste kommunale Projekte, Vereine und Initiativen. Während Medienbildung in Schulen aufgrund der Schulpflicht nahezu alle Kinder und Jugendlichen erreichen kann, sind **außerschulische Angebote freiwillig**. Sie können dafür stärker an **lebensweltliche Relevanzen der Zielgruppe anknüpfen** (Rauschenbach et al. 2007). Im Lichte der unterschiedlichen Dynamiken schulischer und außerschulischer Bildung ist es aktuell eine schwierige Aufgabe für das Handlungsfeld, Kinder und Jugendliche allgemein für einen kritischen Umgang mit Online-Medien, aber auch speziell zum Umgang mit dynamischen Online-Interaktionsrisiken der Gegenwart zu befähigen.

Handlungsoptionen für die schulische und außerschulische Medienbildung

Aufnahme von Kompetenzförderung zu Online-Interaktionsrisken für alle Schularten und Altersgruppen in den verpflichtenden Teil der Schulcurricula

Online-Interaktionsrisiken sind dynamische Phänomene, die sich in ihrer Relevanz innerhalb von Entwicklungsphasen, sozialen Gruppen und Milieus unterscheiden und sich durch fortwährend neu erscheinende Apps und Funktionen schnell verändern. Dementsprechend wichtig sind die Entwicklung, Erprobung und Evaluation entsprechender Materialien und Programme, die im Schulkontext eingesetzt werden können, sowie **regelmäßige Bildungsmaßnahmen** (etwa zu den einschlägigen Themen Privatheit, Datenschutz, Kinderrechte, soziale Kompetenz und digitale Zivilcourage sowie Cybermobbing, Cybergrooming, Online-Hatespeech oder non-konsensuales Sexting bzw. den jeweils aktuellen Online-Interaktionsrisiken). Zusätzlich sollten die Materialien und Programme wissenschaftlich evaluiert werden, um die Wirksamkeit und Eignung für die jeweilige Zielgruppe besser zu verstehen. Wird die Kompetenzförderung zu solchen Themen im verpflichtenden Teil von Schulcurricula aufgenommen, sollten je nach Besonderheiten und Herausforderungen der jeweiligen Lerngruppe inhaltliche Schwerpunkte gewählt werden.

Förderung digitaler Zivilcourage von Bystandern durch Präventionsprogramme

Viele Kinder und Jugendliche kommen als Bystander, also als zunächst nicht direkt beteiligte „Zuschauer:innen", mit diversen Online-Interaktionsrisiken in Berührung (Kheredmand 2022). Aus unterschiedlichen Gründen bleiben die meisten jungen Menschen in solchen Fällen passiv (Atzmüller et al. 2019). Wünschenswert wären allerdings zivilcouragiert agierende Bystander, die öffentlich Position beziehen, die Betroffenen unterstützen und möglicherweise weitere Bystander zum Eingreifen motivieren. Präventionsprogramme im Bereich der Online-Interaktionsrisiken sollten entsprechend auch mit Blick auf Bystander – und damit nicht nur Betroffene und Ausübende – entwickelt und in schulischen und außerschulischen Kontexten angewandt werden.

Zertifizierung/Qualitätssiegel für Institutionen, die evidenzbasierte Materialien und Programme einsetzen

Als Anreiz für Schulen wie auch außerschulische Institutionen, evidenzbasierte Materialien und Programme umzusetzen, erscheint eine **Zertifizierung der Institutionen bzw. die**

Vergabe eines offiziellen Qualitätssiegels für den Einsatz evidenzbasierter Materialien lohnenswert. Erst durch den Einsatz nach wissenschaftlichen Kriterien empirisch auf die Wirksamkeit evaluierter Materialien und Programme kann sichergestellt werden, dass begrenzte zeitliche, personelle und materielle Ressourcen effektiv und effizient eingesetzt werden, um Online-Interaktionsrisiken präventiv entgegen zu wirken. Eine Zertifizierung der Institutionen kann Aufmerksamkeit schaffen und Legitimität fördern, sollte jedoch im Hinblick auf ihre Umsetzbarkeit mit allen relevanten Stakeholdern in einem gemeinsamen Verfahren geprüft werden.

Ergänzend zur Projektförderung nachhaltige Strukturen durch die Politik fördern

Angebote und Materialien sowie deren Evaluation entstehen häufig im Rahmen von drittmittelgeförderten und zeitlich begrenzten Projekten, doch findet die tatsächliche **Implementation der Materialien** nach Projektende statt. Schulen und außerschulische Akteure müssen mit knappen zeitlichen, finanziellen und personellen Ressourcen umgehen und benötigen daher Unterstützung durch externe Strukturen. Grundlegend sollten die Bekanntheit und Nutzung bereits bestehender **Informationsplattformen** zu evidenzbasierten Angeboten gestärkt werden (z.B. Grüne Liste Prävention; Bremer et al. 2022). Nachhaltiger wäre allerdings die Schaffung eines **fortwährend aktualisierten Online-Repositoriums.** Dieses könnte Open-Access-Materialien, Fort- und Weiterbildungsangeboten und Workshops zur Qualifizierung pädagogischen Personals im Umgang mit den bereitgestellten Materialien umfassen sowie einen „Trainer:innenpool", der die Durchführung von Angeboten in Schulen personell unterstützt.

6.5 Handlungsfeld: Fort- und Weiterbildung mit Bezug zu Online-Interaktionsrisiken für unterschiedliche Zielgruppen

Neben Kindern und Jugendlichen selbst gilt es, weitere Zielgruppen in die Verbesserung der Sicherheit für Kinder in der digitalen Welt einzubinden. Zu diesen Zielgruppen zählen **Eltern bzw. Erziehungsberechtigte, pädagogische Fachkräfte, Akteure der Bildungsverwaltung und -politik, Anbieter von Online-Apps, Content-Creator:innen sowie Polizei und Sicherheitskräfte.**

Eltern und Erziehungsberechtigte haben nicht dieselben Mediensozialisationserfahrungen wie die heutigen Kinder und Jugendlichen. Sie benötigen daher Unterstützungsangebote, die einerseits die eigene (kritische) Medienkompetenz fördern und andererseits geeignete Medienerziehungs- und Medienbegleitungsstrategien vermitteln. **Pädagogische Fachkräfte**, die mit Heranwachsenden zu Online-Interaktionsrisiken arbeiten, benötigen ihrerseits Kompetenzen im Umgang mit diesen Risiken. **Akteure der Bildungsverwaltung und -politik** beeinflussen maßgeblich, in welchem Ausmaß und in welcher Form Fort- und Weiterbildungsangebote konzipiert und implementiert werden können. **Anbieter von Online-Apps** schaffen Plattformen, die von Kindern genutzt werden – bisher häufig unabhängig davon, ob sie diese für Kinder gestalten. **Influencer:innen und Content-Creator:innen** können als Vorbild für Kinder und Jugendliche wirken, sei es direkt durch ihre Äußerungen oder indirekt durch Verhalten, Sprache, Auftreten oder Wahl der Inhalte. **Polizei und Sicherheitskräfte** sind für die Aufdeckung, Anzeige und Verfolgung von strafrechtlich relevanten Taten zentral und

benötigen insbesondere bei Vorfällen sexualisierter Gewalt eine hohe Sensibilität im Umgang mit betroffenen Kindern und Jugendlichen.

Die **Einbindung dieser verschiedenen Akteure in die Stärkung der Online-Sicherheit** von Kindern und Jugendlichen kann durch **Fort- und Weiterbildung (bzw. Erwachsenenbildung)** unterstützt werden, welche als vierte Säule des Bildungssystems einen Teil des lebenslangen Lernens darstellt und durch Prinzipien der Praxis- und Handlungsorientierung sowie Partizipation gekennzeichnet ist (Nuissl 2018).

Handlungsoptionen für die Fort- und Weiterbildung mit Bezug zu Online-Interaktionsrisiken für unterschiedliche Zielgruppen

Fort- und Weiterbildungsangebote für Eltern und Erziehungsberechtigte sollten eine Bandbreite an praktischen Maßnahmen zur Begleitung und Unterstützung ihrer Kinder vermitteln

Um ihre Kinder gegenüber den vielfältigen und dynamischen Herausforderungen durch Online-Interaktionsrisiken sicher zu unterstützen, erscheint für Eltern die Kombination eigener (kritischer) Medienkompetenz sowie restriktiver, aktiver, technischer und partizipativ-lernender Medienerziehungsstrategien am besten geeignet. Diese kann – abhängig vom Alter – auch den wachsenden Kompetenzen der Kinder und Jugendlichen angepasst werden (Pfetsch 2018). Günstig hierfür sind offene Angebote der Erwachsenenbildung (z.B. angeschlossen an Einrichtungen der Elementarpädagogik oder Schulen) oder digital gestützte Angebote, die ortsunabhängig und zeitlich flexibel nutzbar sind und für eine Diversität von Lernenden anpassbar sind (KMK 2016).

Angebote für pädagogische Fachkräfte sollten neue Entwicklungen von Online-Interaktionsrisiken oder das Phänomen der Opferabwertung umfassen

Über eine grundlegende Qualifizierung von pädagogischen Fachkräften zu Online-Interaktionsrisiken hinaus sollten **Fort- und Weiterbildungsangebote insbesondere neuartige Aspekte** umfassen (etwa Veränderungen durch KI, Verschränkungen der Risiken). Darüber hinaus ist eine Sensibilisierung für Prozesse der Opferabwertung (*Victim Blaming*), insbesondere im Bereich sexualisierter Grenzverletzungen empfehlenswert. Lehrkräfte sollten über alle drei Phasen der Lehrkräftebildung (Lehramtsstudium, Vorbereitungsdienst, berufliche Weiterbildung) umfassend für das Lernen mit und über Medien qualifiziert werden (Vogler et al. 2022) und sich ihrer Verantwortlichkeit auch für vermeintlich private (nicht-schulische) Medienerfahrungen von Schüler:innen bewusst sein, wenn diese das Wohlbefinden und den Schulfrieden stören.

Bewusstsein der Akteure der Bildungsverwaltung und -politik für Online-Interaktionsrisiken fördern

Im Bereich der Bildungsverwaltung und -politik sollte ein Umdenken stattfinden, indem die **Evidenzbasierung und die Strukturförderung im Bereich der Prävention stärker in den Vordergrund rücken** (vgl. Handlungsoptionen im Handlungsfeld schulische und außerschulische Medienbildung). Inhaltlich sollten Fort- und Weiterbildungsangebote geplant und gefördert werden, die pädagogisches Personal zu Online-Interaktionsrisiken und neuen digita-

len Entwicklungen qualifiziert. Nur wenn Bildungsverwaltung und Bildungspolitik die Bedeutung dynamischer Risiken in der Medienbildung erkennen, können grundlegende Entscheidungen getroffen werden, die in der Folge auch die Fort- und Weiterbildung auf diese Gefahren hin ausrichten.

Anbieter von Online-Apps sollten über Entwicklungsverletzlichkeiten und das Spannungsverhältnis von Schutz- und Teilhabebedürfnissen informiert werden, um kindgerechte Apps entwickeln zu können

Anbieter von Online-Apps sollten für Entwicklungsverletzlichkeiten von Kindern und Jugendlichen sensibilisiert werden. Dies umfasst auch die Sensibilisierung für persönliche Zielkonflikte, die mit dem Spannungsverhältnis zwischen kindlichen bzw. jugendlichen Bedürfnissen und risikobewusstem Verhalten einhergehen. Dies kann über Fort- und Weiterbildung durch wissenschaftliche oder zivilgesellschaftliche Akteure geleistet werden (siehe Handlungsoptionen im Handlungsfeld „Technikentwicklung"). Besonders vielversprechend erscheint hier die Vernetzung mit und Teilnahme am Akteursnetzwerk, um Erfahrungsaustausch und die Vermittlung von gesellschaftlichen Erwartungen, aber auch die gegenseitige Ansprechbarkeit zu ermöglichen. Um möglichst viele Anbieter dazu zu motivieren, sollten hierzu Anreizsysteme für Anbieter entwickelt werden.

Kooperationen und Projekte zu Online-Interaktionsrisiken mit Influencer:innen und Content-Creator:innen

Positive Influencer:innen und Content-Creator:innen haben das Potenzial, Kinder und Jugendliche niederschwellig zu erreichen, Bewusstsein für konkrete Risiken zu schaffen und soziale Normen und Werte zu beeinflussen. Durch die Kooperation mit Influencer:innen und Content-Creator:innen oder gemeinsame Projekte wie *Our feed, our future* können sie als Multiplikator:innen zur Verringerung von Online-Interaktionsrisiken und von Viktimisierungserfahrungen beitragen.

Fort- und Weiterbildung für Polizei und Sicherheitskräfte in Bezug auf sexualisierte Gewalt und Grenzverletzungen

Polizei und Sicherheitskräfte sind entscheidende Akteure, wenn sich Online-Interaktionsrisiken als Übergriffe und Straftaten realisieren. Gerade bei der Aufdeckung, Anzeige und Verfolgung von Vorfällen sexualisierter Gewalt gegenüber Kindern und Jugendlichen wird relevant, dass in vielen Fällen sexualisierter Gewalt im Internet nach aktueller Rechtslage Jugendliche als Täter:innen und Opfer sexualisierter Grenzverletzungen involviert sind (z.B. Jugendpornographie auch bei konsensuell geteiltem Bildmaterial). Zentral sind ebenso Kenntnisse über kindzentrierte Vernehmungsmethoden in Fällen sexualisierter (Online-)Gewalt. Zielgruppenspezifische Fort- und Weiterbildungen können bestehende Expertise auf diesen Gebieten erweitern und zusätzlich sensibilisieren.

6.6 Handlungsfeld: Technikentwicklung

Neben der Plattform- und Angebots-Governance gibt es im Kontext von Interaktionsrisiken große Potenziale, kinderrechtliche Aspekte bei der Entwicklung neuer Technikprodukte einzubeziehen. Die Gestaltung von digitalen Medien ist ausschlaggebend für die Erfahrungen von Kindern und Jugendlichen in ihrer Interaktion untereinander, mit Erwachsenen und mit

Geräten sowie der Software. In modernen technisierten Gesellschaften sind fast alle Bereiche des Lebens von Computersystemen bzw. digitalen Medien durchzogen („Kultur der Digitalität", Stalder 2016). Damit sind lebensweltliche Erfahrungen von Kindern durch die Darstellung von Informationen, neue Kommunikationsformen und Kulturen der Online-Interaktionen (inklusive Interaktionsrisiken) maßgeblich durch Technikdesign geprägt (Tillmann & Hugger 2014, S. 32).

Innerhalb der Informatik beschäftigt sich der Bereich *Child-Computer Interaction* damit, welche Bedarfe und Präferenzen sich für Kinder im Umgang mit Smartphones, Apps, Computerspielen und smarten Spielzeugen ergeben. Hierbei wird auch auf die **Methode des Co-Designs** zurückgegriffen, wenn Kinder als Expert:innen ihrer technisch vermittelten Lebenswelt ernst genommen werden (Mahboob Kanafi et al. 2022; Badillo-Urquiola et al. 2021). Weniger Beachtung finden derzeit noch die **Komplexität und Intersektionalität von kindlichen Erfahrungen in der Interaktion mit Technik.** Insbesondere Nuancen, die sich durch spezifische Bedarfe, aber auch Diskriminierungserfahrungen für unterschiedlich situierte Kinder im Alters- und Entwicklungsverlauf ergeben, bleiben unterbeleuchtet. **Online-Interaktionsrisiken wie Cybermobbing verschränken sich mit gesellschaftlichen Diskriminierungsmustern** und können hierdurch Kinder mit einem „diversen" Hintergrund anders betreffen (Schultze-Krumbholz et al. 2022). Für den Bereich *Child-Computer Interaction* ist es zudem zentral, ethische Fragen bei der Partizipation von Kindern und bei der Datensammlung und -analyse zu beachten und kontinuierlich zu reflektieren (Hourcade et al. 2017) (siehe Handlungsfeld „Forschung und Wissenschaft").

Die Technikentwicklung ist in ihrem Design von Produkten und Services maßgeblich von **supranationaler Gesetzgebung** beeinflusst. Für Europa sind hier insbesondere die Europäische Datenschutz-Grundverordnung (DSGVO), aber auch der Digital Services Act (DSA) und der Artificial Intelligence Act (AI Act) zu nennen. Durch den komplexen EU-Rechtsrahmen entsteht ein hoher Druck auf Anbieter, ihre Produkte mit den regulatorisch formulierten Anforderungen und Pflichten in Einklang zu bringen. Dabei sind die Vorgaben durch die Gesetzgebung teilweise unkonkret und die Umsetzung der Maßnahmen liegt im Gestaltungsspielraum der Unternehmen. Technikunternehmen können sich bei der Umsetzung aber an gesetzlichen Ausgestaltungsmöglichkeiten und kinderrechtlich orientierten Technikentwicklungsprozessen orientieren, die von zivilgesellschaftlichen Organisationen und Forschung zu einem integrativen Forschungsdesign bereitgestellt werden (z.B. 5Rights Foundation 2024; Kurian 2024; UK Information Commissioner's Office 2020).

Handlungsoptionen für die Technikentwicklung

Anbieter digitaler Medien sollten bei der Gestaltung ihrer Angebote die Besonderheiten der Zielgruppe Kinder und Jugendliche berücksichtigen

Bei der Gestaltung von digitalen Angeboten ist es wichtig, die besondere Lebensrealität von Kindern unterschiedlicher Alters- und Entwicklungsstufen zu beachten. Dabei sollte ein besonderer Blick auf die **Entwicklungsverletzlichkeiten** im Altersverlauf geworfen werden, welche Online-Interaktionsrisiken begünstigen können (siehe Kapitel 3.3 Ergebnisse Psychologische Perspektive). Anbieter sollten außerdem Möglichkeiten schaffen, dass **Aufklärungs-**

kampagnen Kinder und Jugendliche über die Plattformen erreichen (und nicht durch automatisierte Filter aufgrund eines Bezugs zu Sexualität im Fall von Präventionsangeboten zu non-konsensualem Sexting und Cybergrooming blockieren). Anbieter digitaler Medien sollten bei der Gestaltung ihrer Angebote auch die **Besonderheiten von intersektionaler Diskriminierung**, voran Erfahrungen von Kindern mit Migrationshintergrund, diverse Fähigkeiten und Geschlechteridentitäten, berücksichtigen. Kinder aus strukturell benachteiligten Gruppen bedürfen einer besonderen Unterstützung im Digitalen und bei der Partizipation in Technikentwicklungsprozessen, da sich Online-Interaktionsrisiken für sie anders oder intensiviert materialisieren können. Schutz- und Befähigungsmaßnahmen sollten daher im Kontext gesellschaftlicher Machtverhältnisse entwickelt werden.

Orientierung für die Umsetzung von Vorsorgemaßnahmen anbieten

In interdisziplinären, kollaborativen Konsultationsprozessen mit allen relevanten Stakeholdern sollten Rahmenbedingungen entwickelt werden, die angesichts (noch) unbestimmter rechtlicher Vorgaben eine Orientierung für Vorsorgemaßnahmen schaffen. **Bestehende Unsicherheiten bei der Umsetzung von Regulierung können auf diese Weise abgebaut werden.** Insbesondere sollten *Best Practices* für die Umsetzung kinderrechtlicher Prinzipien im Digitalen (vor allem im Bereich Vorsorge, etwa Privatheit, Sicherheit und Schutz) benannt werden. Orientierende Umsetzungskriterien und Positivbeispiele unterstützen gleichzeitig zivilgesellschaftliche und private Akteure dabei, sich zukünftig auf konkrete Standards zu beziehen, wenn sie eine Verletzung von gesetzlichen Vorgaben vermuten. Solche Vorgaben und Empfehlungen können sich etwa aus den geplanten Leitlinien nach Art. 28 Abs. 4 DSA oder einem EU Age-appropriate Design Code ergeben, sie können aber auch im Rahmen von dialogischen Verfahren der Aufsichtsstellen wie der BzKJ, der dort neu eingerichteten „Stelle zur Durchsetzung von Kinderrechten in digitalen Diensten" (KidD) oder den Landesmedienanstalten und der KJM mit einzelnen Anbietern oder Anbietergruppen entwickelt werden.

Durch Beratung für Online-Anbieter und Technikunternehmen Bewusstsein für die Berücksichtigung von Kinderrechten schaffen

Beratung für Online-Anbieter zur systematischen Berücksichtigung und Implementierung von Kinderrechten ist eine zentrale Voraussetzung für ein kindgerechtes und sicheres Technikdesign. Technikunternehmen sollten motiviert werden, sich entsprechende Expertise einzuholen und sie zum Merkmal ihrer Angebotsgestaltung zu machen. Die **Kooperation von Expert:innen im Bereich Kinderrechte und Technikentwicklung** sollte gestärkt und gefördert werden. Wissenschaftliche Arbeiten an Universitäten ebenso wie Kinderrechtsorganisationen bieten für die Technikentwicklung relevante Einblicke in die Umsetzung von Kinderrechten im Digitalen. Hier ist es wichtig, **Anreize** für die interdisziplinäre und – wenn sinnvoll – transdisziplinäre Zusammenarbeit zu schaffen (siehe Handlungsfeld „Forschung und Wissenschaft").

Das gesamte Akteursnetzwerk ist gefragt, in Interaktion mit Anbietern die **Potenziale einer kinderrechtlichen Perspektive in der Technikentwicklung zu vermitteln.** Besondere Verantwortung tragen hier öffentliche Institutionen wie die Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) oder die Landesmedienanstalten, wenn sie den bestehenden (komplexen) Rechtsrahmen interpretieren, konkretisieren und auf den Einzelfall anwenden. Wichtige Aufgaben für die Schaffung von Bewusstsein für Kinderrechte auf Anbieterseite

übernehmen daneben Selbstkontrolleinrichtungen und Branchenverbände der Privatwirtschaft.

6.7 Handlungsfeld: Infrastrukturelle Anbietermaßnahmen

Im derzeitigen Ordnungsrahmen für die Online-Interaktion und -Kommunikation von Kindern und Jugendlichen gilt der **Grundsatz der Anbieterverantwortlichkeit**: Die Anbieter von Online-Plattformen und digitalen Diensten müssen hiernach die gesetzlichen und eigenen Vorgaben im Umgang mit Kommunikations- und Interaktionsrisiken umsetzen. Für einzelne Darstellungen und die Kommunikation in ihren Diensten sind die Anbieter erst ab Kenntnis verantwortlich, so dass derzeitige Regulierungsansätze vor allem Vorgaben auf infrastruktureller Ebene machen (s. oben infrastrukturelle Maßnahmen). Damit ist das komplexe Feld der ***hybrid governance*** angesprochen, in dem die plattformeigenen Vorgaben und Schutzmaßnahmen mit den regulatorischen Vorgaben zur Governance von Online-Angeboten und -Plattformen verschränkt sind. Hier sind Entwicklungen im Bereich der Plattform-Governance beobachtbar, welche die Regulierungsinstrumente von konkreten inhaltsbezogenen Ansätzen weiterentwickeln und auf ziel- und prinzipienbasierte Vorgaben umstellen (Dreyer, Andresen & Wysocki 2022). Bei diesen neuen Ansätzen, wie etwa Pflichten zur Einziehung von risikobezogenen Maßnahmen, haben die Anbieter aufgrund ihrer eigenen Grundrechte und mit Blick auf den Grundsatz der Vertragsautonomie einen **Umsetzungsspielraum** bei der Gestaltung ihrer Angebote; sie werden dadurch zu mächtigen Akteuren der rechtlichen Umsetzung. Die zuständigen Aufsichtsstellen wie die BzKJ und die Landesmedienanstalten mit der KJM überprüfen die Einhaltung der gesetzlichen Vorgaben dabei anhand relativ unbestimmter Maßstäbe; hier kommt es in Zukunft auf die Etablierung von rechtlichen Leitlinien und einer kohärenten Aufsichts- und Spruchpraxis an. Für alle Seiten gilt, dass durch eher bewahrpädagogische Ansätze und Zugangsverhinderungen (zu ganzen Plattformen) Risiken durch den Kinder- und Jugendmedienschutz entstehen können, die den Aspekten der Befähigung und Teilhabe von Kindern entgegenstehen. Hier ist es wichtig, einen **angemessenen Ausgleich zwischen Schutz und Teilhabe** zu finden, wobei Befähigungsmaßnahmen für **beide** Dimensionen eine zentrale Rolle spielen.

Handlungsoptionen für die Verbesserung infrastruktureller Anbietermaßnahmen

Ko-regulative Ansätze im Kinder- und Jugendmedienschutz stärken und ausbauen

Die im deutschen und europäischen Kinder- und Jugendmedienschutz bestehenden und in der Praxis erprobten **Ansätze der Ko-Regulierung** erscheinen als **optimale Ausgangsbasis für die Implementierung eines zeitgemäßen und effektiven Rechtsrahmens** – auch und gerade im Hinblick auf Interaktionsrisiken. Durch die prinzipien- oder zielorientierten Regulierungsansätze bedarf es weiterhin struktureller Schutzvorkehrungen, um die Haftungsprivilegierung von Plattformanbietern nicht zu unterlaufen. Ko-Regulierung kann hier **flexiblere Ansätze** für Maßnahmen und Aktivitäten bereithalten, **Anreize** zur Teilnahme am System Kinder- und Jugendmedienschutz schaffen und konkrete Pflichten von staatlichen (Aufsichts- und Durchsetzungs-)Maßnahmen entkoppeln: Ko-Regulierung kann damit auch die Herstellung von Demokratiefestigkeit der Media Governance unterstützen.

Auf präventive und befähigende Maßnahmen fokussieren

Die bisher im rechtlichen Rahmen vorfindbaren Vorsorgemaßnahmen stellen sich bei genauerer Betrachtung teilweise nicht als Maßnahmen der klassischen Prävention dar, sondern wirken höchstens im Nachgang zu einer Verletzung (z.B. Meldesysteme, Beratungs- und Hilfsangebote). Mit Blick auf die Anbieter folgt daraus die **Notwendigkeit von verstärkten konzeptionellen Anstrengungen zur Entwicklung, Stärkung und Förderung von präventiv wirkenden Maßnahmen**. Dazu gehört die Schaffung von (mehr) Bewusstsein für Kinderrechte in digitalen Medienumgebungen (siehe die Handlungsfelder „Schulische und außerschulische Medienbildung" sowie „Fort- und Weiterbildung"). Außerdem können Anbieter angehalten sein, die mit dem Digital Services Act (DSA) privilegierten, freiwilligen Monitoringmaßnahmen einzuführen bzw. auszubauen (siehe auch Handlungsfeld „Technikentwicklung").

Interdisziplinäre und praxisnahe Frameworks für eine alters- und entwicklungsangemessene Gestaltung entwickeln

Die Umsetzung von abstrakten, zielorientierten Pflichten zur Einziehung von anbieterseitigen Maßnahmen, die auf Basis empirischer Nutzungsdaten optimiert werden und die die partizipatorische Einbindung von Kindern vorsehen, ist außerordentlich voraussetzungsvoll und komplex. Hier bedarf es der **interdisziplinären Entwicklung und Weiterentwicklung von kinderrechtssensiblen Frameworks und Leitfäden**, welche Anbieter bei der Erstellung und Umsetzung von Verfahren zur Angebotsgestaltung nutzen können. Dabei sind insbesondere Kooperationen von Wissenschaft, erzieherischem Medienschutz und Anbietern zu unterstützen (siehe auch Handlungsfeld „Technikentwicklung").

Kurzversion der Handlungsoptionen

Vor dem Hintergrund der vorgestellten Ergebnisse und Erkenntnisse aus den Teilprojekten und den Expert:innen-Workshops im Stakeholder-Netzwerk wurden **sieben zentrale Handlungsfelder mit entsprechenden Handlungsoptionen extrapoliert** und interdisziplinär verwoben:

Handlungsfeld: Kooperation im Akteursnetzwerk

Ein zentrales Handlungsfeld ist die Etablierung, Formalisierung und Verstetigung eines Akteursnetzwerks, in dem Erfahrungsaustausch und die Koordination von Aktivitäten möglich sind. Aus dem Umstand, dass **Kinder- und Jugendmedienschutz als kinderrechtlicher Querschnittsbereich** konzipiert wird und bei seiner effektiven Umsetzung **auf die Akzeptanz aller beteiligten Akteure angewiesen** ist, ergibt sich das **Ziel einer netzwerkgerechten Gestaltung dieses Akteursverbunds.**

Handlungsoptionen für die Kooperation im Akteursnetzwerk

- ✓ Etablierung bzw. Verstetigung eines Akteursnetzwerks „Prävention von Online-Interaktionsrisiken"
- ✓ Unterstützung von Kooperation und Koordination im Akteursnetzwerk
- ✓ Kooperationen auf kommunaler und regionaler Ebene sichtbarer machen
- ✓ Kultur(en) für Positive Plattform Governance im Netzwerk schaffen
- ✓ Netzwerkgerechtere Gesetzgebungsverfahren etablieren und leben

Handlungsfeld: Forschung und Wissenschaft

Die Wissenschaft bietet wesentliche Grundlagen für das gesamte Akteursnetzwerk. Das Generieren von Wissen, empirischen Grundlagen, die Evaluation von Maßnahmen, aber auch der Bezug zu demokratischen Grundwerten und der reflektierte Umgang mit Ambivalenzen und Spannungsfeldern sowie ihre Vernetzungsfunktion macht die Wissenschaft zu einem zentralen Handlungsfeld für die Sicherheit von jungen Menschen in digitalen Umgebungen.

Handlungsoptionen für die Forschung und Wissenschaft

- ✓ Forschende befähigen, sicherheitsrelevante Fragen ethisch zu bearbeiten
- ✓ Kinder stärker als bisher in Forschung einbeziehen
- ✓ Mehr empirische Forschung zu intersektional marginalisierten Kindern durchführen und fördern
- ✓ Die Nachhaltigkeit der Vernetzung und den Erfahrungsaustausch im Forschungsfeld fördern
- ✓ Anreizsysteme und Fördermöglichkeiten für forschungsethisch fundierte Forschungsprojekte schaffen und strukturell fördern
- ✓ Theorie- und Empirie-gestützte Entwicklung von Materialien zur Prävention von Online-Interaktionsrisiken fördern

Handlungsfeld: Maßnahmen nach Verletzungen (Unterstützung Betroffener, Ermittlung Verursachender)

Betroffene von Übergriffen und kriminellen Handlungen brauchen ein gutes und umfassendes **Unterstützungs-Ökosystem, das sich an den Bedarfen im konkreten Verletzungsmoment und im Nachgang orientiert.**

Handlungsoptionen für die Stärkung von Maßnahmen nach Übergriffen

- ✓ Verbesserung der Bekanntheit und Zugänglichkeit von Unterstützungs- und Beratungsangeboten für Kinder und Jugendliche
- ✓ Verbesserung der Unterstützung von Betroffenen
- ✓ Gewährleistung einer effizienten Verfolgung von Rechtsverstößen

Handlungsfeld: Schulische und außerschulische Medienbildung für Kinder und Jugendliche

Die schulische Bildung in Deutschland liegt stark in der Verantwortung der Bundesländer. Es gibt zwar verbindliche, bundesweit geltende Bildungsstandards für bestimmte Klassenstufen bzw. Schulabschlüsse sowie für ausgewählte Kernfächer, die von der Kultusministerkonferenz (KMK) verabschiedet werden. Die Implementation dieser Standards in landeseigene Vorgaben stellen allerdings die Bundesländer sicher. Zwar ist auch die **Medienbildung in den Curricula der Bundesländer verankert, allerdings in unterschiedlicher Form und in unterschiedlichem Ausmaß.** Das Handlungsfeld der **schulischen Medienbildung** ist also, u.a. aufgrund der föderalen Struktur der Bildungslandschaft, **sehr heterogen und komplex.**

Handlungsoptionen für die schulische und außerschulische Medienbildung

- ✓ Aufnahme von Kompetenzförderung zu Online-Interaktionsrisken für alle Schularten und Altersgruppen in den verpflichtenden Teil der Schulcurricula
- ✓ Förderung digitaler Zivilcourage von Bystandern durch Präventionsprogramme
- ✓ Zertifizierung/Qualitätssiegel für Institutionen, die evidenzbasierte Materialien und Programme einsetzen
- ✓ Ergänzend zur Projektförderung nachhaltige Strukturen durch die Politik fördern

Handlungsfeld: Fort- und Weiterbildung mit Bezug zu Online-Interaktionsrisiken für unterschiedliche Zielgruppen

Neben Kindern und Jugendlichen selbst gilt es, weitere Zielgruppen in die Verbesserung der Sicherheit für Kinder in der digitalen Welt einzubinden. Zu diesen Zielgruppen zählen **Eltern bzw. Erziehungsberechtigte, pädagogische Fachkräfte, Akteure der Bildungsverwaltung und -politik, Anbieter von Online-Apps, Content-Creator:innen sowie Polizei und Sicherheitskräfte.**

Handlungsoptionen für die Fort- und Weiterbildung mit Bezug zu Online-Interaktionsrisiken für unterschiedliche Zielgruppen

- ✓ Fort- und Weiterbildungsangebote für Eltern und Erziehungsberechtigte sollten eine Bandbreite an praktischen Maßnahmen zur Begleitung und Unterstützung ihrer Kinder vermitteln
- ✓ Angebote für pädagogische Fachkräfte sollten neue Entwicklungen von Online-Interaktionsrisiken oder das Phänomen der Opferabwertung umfassen
- ✓ Bewusstsein der Akteure der Bildungsverwaltung und -politik für Online-Interaktionsrisiken fördern
- ✓ Anbieter von Online-Apps sollten über Entwicklungsverletzlichkeiten und das Spannungsverhältnis von Schutz- und Teilhabebedürfnissen informiert werden, um kindgerechte Apps entwickeln zu können
- ✓ Kooperationen und Projekte zu Online-Interaktionsrisiken mit Influencer:innen und Content-Creator:innen
- ✓ Fort- und Weiterbildung für Polizei und Sicherheitskräfte in Bezug auf sexualisierte Gewalt und Grenzverletzungen

Handlungsfeld: Technikentwicklung

Neben der Plattform- und Angebots-Governance gibt es im Kontext von Interaktionsrisiken große Potenziale, kinderrechtliche Aspekte bei der Entwicklung neuer Technikprodukte einzubeziehen. Die Gestaltung von digitalen Medien ist ausschlaggebend für die Erfahrungen von Kindern und Jugendlichen in ihrer Interaktion untereinander, mit Erwachsenen und mit Geräten sowie der Software.

Handlungsoptionen für die Technikentwicklung

- ✓ Anbieter digitaler Medien sollten bei der Gestaltung ihrer Angebote die Besonderheiten der Zielgruppe Kinder und Jugendliche berücksichtigen
- ✓ Orientierung für die Umsetzung von Vorsorgemaßnahmen anbieten
- ✓ Durch Beratung für Online-Anbieter und Technikunternehmen Bewusstsein für die Berücksichtigung von Kinderrechten schaffen

Handlungsfeld: Infrastrukturelle Anbietermaßnahmen

Im derzeitigen Ordnungsrahmen für die Online-Interaktion und -Kommunikation von Kindern und Jugendlichen gilt der **Grundsatz der Anbieterverantwortlichkeit:** Die Anbieter von Online-Plattformen und digitalen Diensten müssen hiernach die gesetzlichen und eigenen Vorgaben im Umgang mit Kommunikations- und Interaktionsrisiken umsetzen. Die zuständigen Aufsichtsstellen überprüfen die Einhaltung der gesetzlichen Vorgaben anhand relativ unbestimmter Maßstäbe. Für beide Seiten gilt, dass durch eher bewahrpädagogische Ansätze und

Zugangsverhinderungen (zu ganzen Plattformen) Risiken durch den Kinder- und Jugendmedienschutz entstehen können, die den Aspekten der Befähigung und Teilhabe von Kindern entgegenstehen.

Handlungsoptionen für die Verbesserung infrastruktureller Anbietermaßnahmen

- ✓ Ko-regulative Ansätze im Kinder- und Jugendmedienschutz stärken und ausbauen
- ✓ Auf präventive und befähigende Maßnahmen fokussieren
- ✓ Interdisziplinäre und praxisnahe Frameworks für eine alters- und entwicklungsangemessene Gestaltung entwickeln

7. Fazit und Ausblick

Der vorliegende Kompass gibt **Einblick in das komplexe Themenfeld der Sicherheit von Kindern in digitalen Welten.** Er basiert auf einer interdisziplinär fundierten und kinderrechtlich ausgerichteten Perspektive auf Kinder als handelnde Akteure im digitalen Raum. Der SIKID-Kompass stellt Handlungsoptionen bezogen auf relevante Handlungsfelder vor, die sich an das gesamte Akteursnetzwerk richten. Als Ergebnis kann festgehalten werden, dass Sicherheit eine Art „Basisrecht" ist, auf das viele weitere Kinderrechte aufbauen, wobei es immer anzustreben ist, dass verschiedene Rechte von Kindern, die gleichwertig sind, gewährleistet werden sollen. Sicherheit gilt als Grundbedingung nicht nur für die freie Entfaltung von Persönlichkeitsrechten, sondern auch eine unbeschwerte demokratische Teilhabe in Digitalen. Online-Interaktionsrisiken **entstehen aus sozialer Kommunikation und Interaktion (als menschliche Grundbedürfnisse) im digitalen Raum.** Dabei ist die Online-Kommunikation Heranwachsender eng mit Entwicklungsaufgaben verknüpft, die es zu berücksichtigen gilt. Online-Interaktionsrisiken sollten daher immer im Entwicklungsverlauf (mit Blick auf die *evolving capacities*) betrachtet werden. Die Projektergebnisse haben aufgezeigt, dass junge Menschen ein anderes Risikoverständnis haben als Erwachsene, und, dass sie Angebote brauchen, die ihnen die Umsetzung verschiedener Rechte (z.B. auf Spiel und Freizeit, auf Teilhabe oder Bildung) ermöglichen, ohne dass dies auf Kosten der Sicherheit gehen muss. Aktuelle Regulierungsvorhaben und neue Ansätze von *Child Rights-by-Design* sind hierzu ebenso vielversprechend wie schulische und außerschulische Bildungsangebote oder Fort- und Weiterbildungsangebote von Lehrkräften oder Akteuren der Sicherheitsbehörden.
Zentrales Ergebnis ist, dass all dies nicht ohne weitergehende und verstetigte Vernetzung der verschiedenen Akteursgruppen gelingen kann. **Sicherheit sollte immer im digitalen (und sozialen) Ökosystem gedacht werden.** Auszugehen ist von einer vernetzten Verantwortung, da es eine strukturelle Sicherheitsgefährdung darstellt, wenn ein Verantwortungsvakuum entsteht. Befähigung ist eine „Sicherheitsressource", an der sich zeigt, dass gerade präventive und befähigende Ansätze im Netzwerk zentraler Stakeholder eine Möglichkeit bieten, individuell und strukturell anzusetzen, so dass Sicherheitsrisiken idealerweise erst gar nicht eintreten. Dennoch muss gleichzeitig ein grundlegender Schutz und eine zielführende Strafverfolgung und Nachbetreuung bei Grenzüberschreitungen erfolgen, damit unbeschwerte Teilhabe von Kindern im Netz möglich bleibt. Und, so ein weiteres Ergebnis, die existierenden Initiativen zur Beratung und Unterstützung sollten sichtbarer und zugänglicher für eine Vielzahl junger Menschen werden.

Der Kompass umfasst daher auch Hinweise, wie die **Forschung anwendungsorientiert und partizipativ** gelingen kann. Denn dies ermöglicht, die Sichtweisen von Kindern selbst einzuholen, um Kinder als diverse gesellschaftliche Gruppe in der Folge auch bei der Entwicklung von Angeboten (z.B. Co-Design) oder als Teil von Regulierungsmaßnahmen zu beteiligen. In sensiblen Themenbereichen, wie Interaktionsrisiken, braucht es hierbei einen forschungsethischen Ansatz, der im Projekt zugrunde gelegt wurden und der in andere Bereiche transferiert werden kann. Das entwickelte Bildungsangebot FairNetzt kann exemplarisch Grundlagen wie Empathie und (digitale) Zivilcourage fördern.
All diese Ergebnisse sind Impulse, die nun weiterer Diskurse und der Schaffung neuer verstetigter Diskursräume bedürfen und in verschiedenen Anwendungsfeldern ausdifferenziert werden können.

Danksagung

Dank gebührt allen Autor:innen des Kompasses und allen, die einen Beitrag dazu geleistet haben. Dies sind insbesondere Cora Bieß, die bis 2023 im SIKID-Projekt mitgearbeitet hat, sowie die studentischen Mitarbeiter:innen Mary Schultz, Yannick Epple und Carlina Schreiber. Besonderer Dank gilt unseren assoziierten Partnern des Projekts, insbesondere Niels Brüggen, Christa Gebel und Achim Lauber vom JFF-Institut für Medienpädagogik, die diese Arbeit konstruktiv und kritisch begleitet und unterstützt haben. Auch Maria von Salisch als assoziierter Partnerin gilt besonderer Dank für ihre inhaltliche Unterstützung. Weiterer Dank gilt dem Kreis von Expert:innen der beiden Stakeholder-Workshops im Jahr 2022 und 2024, die sich engagiert und multiperspektivisch in den Workshops oder auch durch Beiträge in unserem Jour Fixe eingebracht haben. Schließlich gebührt Fabian Rosenkranz besonderer Dank sowie Dr. Christine Prokopf vom Projektträger VDI für die kooperative Projektbetreuung. Wir danken allen, die im Bereich der Sicherheit von Kindern in digitalen Welten arbeiten und sich für den Schutz und das Empowerment von Kindern und Jugendlichen im Internet einsetzen.

Abbildungsverzeichnis

Abkürzungsverzeichnis

BKA	Bundeskriminalamt
DSGVO	Datenschutz-Grundverordnung
KJM	Verzahnung der Kommission für Jugendmedienschutz
UN-KRK	Kinderrechtskonvention der Vereinten Nationen
ZAC NRW	Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen

Literatur

Alderson, Priscilla; Morrow, Virginia (2004): Ethics, Social Research and Consulting with Children and Young People. Ilford, Essex: Barnardo's.

Ammicht Quinn, Regina (Hg.) (2014): Sicherheitsethik. Wiesbaden: Springer VS Wiesbaden. DOI: 10.1007/978-3-658-03203-6.

Andresen, Sünje; Dreyer, Stephan (2021): Straf- und jugendschutzrechtliche Bewertung von Online-Formen aufgedrängter Sexualität und sexualisierter Belästigung. In: JMS-Report 6/2021, S. 2--6. DOI: 10.5771/0170-5067-2021-6-2.

Andresen, Sünje; Dreyer, Stephan (2022): Die Rolle der Eltern bei der datenschutzrechtlichen Einwilligung. In: DuD 46, S. 361-366.

Andresen, Sünje; Dreyer, Stephan; Huerkamp, Dinah; Knabenschuh, Silke (2023): Aktuelles Sexualstrafrecht als Kinderrechteverstoß? Zur strafrechtlichen Problematik konsensualen Sextings unter Beteiligung von jungen Menschen. In: KJuG 4, S. 163–171.

Atzmüller, Christiane; Zartler, Ulrike; Kromer, Ingrid (2019): Online Held*innen gibt es nicht? Was 14- bis 19-jährige Jugendliche an Zivilcourage im Internet hindert. In: SWS-Rundschau 59, S. 87–109.

Badillo-Urquiola, Karla; Shea, Zachary; Agha, Zainab; Lediaeva, Irina; Wisniewski, Pamela (2021): Conducting Risky Research with Teens. Co-designing for the Ethical Treatment and Protection of Adolescents. In: Proc. ACM Hum.-Comput. Interact. 4 (CSCW3), S. 1–46. DOI: 10.1145/3432930.

Bell, Nancy (2008): Ethics in Child Research: Rights, Reason and Responsibilities. In: Children's Geographies 6 (1), S. 7-20.

Bieß, Cora (2023): Befähigung durch Digital Streetwork: Stärkung von Kinder(rechte)n auf Social Media. Tübingen: IZEW, Materialien zur Ethik in den Wissenschaften, Band 22. https://publikationen.uni-tuebingen.de/xmlui/handle/10900/146888.

Bieß, Cora; Stapf, Ingrid; Heesen, Jessica (2023): Sicherheit von Kindern in digitalen Welten als Kinderrecht. In: Erich Marks, Claudia Heinzelmann und Gina Rosa Wollinger (Hg.): Kinder im Fokus der Prävention. Ausgewählte Beiträge des 27. Deutschen Präventionstages. Mönchengladbach: Forum Verlag Godesberg, S. 261-277. https://www.praeventionstag.de/nano.cms/vortraege/id/5624.

Bremer, K.; Brender, R.; Groeger-Roth, F.; Walter, U. (2022): Grüne Liste Prävention – Eine Datenbank evidenzbasierter Präventionsprogramme. In: Das Gesundheitswesen, 84(08/09), S. 864. DOI: 10.1055/s-0042-1753992.

Brüggen, Niels; Dreyer, Stephan; Gebel, Christa; Lauber, Achim; Materna, Georg; Müller, Raphaela; Schober, Maximilian; Stecher, Sina (2022): Gefährdungsatlas. Digitales Aufwachsen. Vom Kind aus denken. Zukunftssicher handeln. Bonn: Bundeszentrale für Kinder- und Jugendmedienschutz (2. Auflage).

Bundesministerium für Bildung und Forschung (BMBF) (2019): Verwaltungsvereinbarung DigitalPakt Schule 2019 bis 2024. Kultusministerkonferenz. https://www.kmk.org/fileadmin/pdf/Themen/Digitale-Welt/VV_DigitalPaktSchule.pdf.

Bundesministerium des Innern und der Heimat (BMI) (2024): Polizeiliche Kriminalstatistik 2023. Ausgewählte Zahlen im Überblick. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/pks-2023.pdf?__blob=publicationFile&v=4.

Burr, Christopher; Taddeo, Mariarosara; Floridi, Luciano (2020): The Ethics of Digital Well-Being: A Thematic Review. In: Sci Eng Ethics 26, S. 2313–2343. https://doi.org/10.1007/s11948-020-00175-8.

Burr, Christoper; Floridi, Luciano (2020): The Ethics of Digital Well-Being: A Multidisciplinary Perspective. In Christopher Burr and Luciano Floridi (Hg.) Ethics of Digital Well-Being: A Multidisciplinary Approach. Springer.

Cousseran, Laura; Gebel, Christa; Tauer, Johanna; Brüggen, Niels (2021): Online-Interaktionsrisiken aus der Perspektive von Neun- bis Dreizehnjährigen. „Aber ich würde sagen, dass es sinnvoller ist, die Person einfach zu blockieren." Deutsches Kinderhilfswerk e.V. https://www.dkhw.de/fileadmin/Redaktion/1_Unsere_Arbeit/1_Schwerpunkte/6_Medienkompetenz/6.24_Studie_Interaktionsrisiken/DKHW_Schriftenreihe_Qualitative_Studie_Heranwachsende_281021_final.pdf.

Cramer, Claus; Mischkowitz, Robert (2013): Die Aussagekraft der Polizeilichen Kriminalstatistik. In: Dieter Dölling und Jörg.Martin Ihle (Hg.): Täter, Taten, Opfer, Grundlagenfragen und aktuelle Probleme der Kriminalität und ihrer Kontrolle. Mönchengladbach: Forum Verlag Godesberg, S. 715–736.

Donoso, Verónica; Van Mechelen, Maarten; Verdoodt, Valerie (2014): Increasing User Empowerment through Participatory and Co-design Methodologies. EMSOC Paper, Brüssel/Leuven/Ghent, September 2014.

Doyle, Caoimhe; Douglas, Ellen; O'Reilly, Gary (2021): The outcomes of sexting for children and adolescents: A systematic review of the literature. In: Journal of Adolescence 92(1), S. 86–113. DOI: 10.1016/j.adolescence.2021.08.009.

Dreyer, Stephan (2024): Kinderdatenschutz als Querschnittsbereich. Friktionen zwischen Datenschutz- und Jugendmedienschutzrecht im Mehrebenensystem. In: PinG 4/, S. 199–206. DOI: 10.37307/j.2196-9817.2024.04.13.

Dreyer, Stephan; Andresen, Sünje; Wysocki, Neda (2024, im Erscheinen): Rechtliche Absicherung von Interaktions- und Kommunikationsrisiken bei der Online-Nutzung von Kindern und Jugendlichen. Arbeitspapiere des Leibniz-Instituts für Medienforschung, Hamburg.

Dreyer, Stephan; Andresen, Sünje; Wysocki, Neda (2022): The best is yet to come? Folgen der sich wandelnden Regulierungsansätze im Jugendmedienschutz. In: JMS-Report 45(6), S. 2–5. DOI: 10.5771/0170-5067-2022-6-2.

Feierabend, Sabine; Rathgeb, Thomas; Kheredmand, Hediye; Glöckler, Stephan (2023a): KIM-Studie 2022. Kindheit, Internet, Medien. Basisuntersuchung zum Medienumgang 6-13-Jähriger. Medienpädagogischer Forschungsverbund (mpfs). https://www.mpfs.de/fileadmin/files/Studien/KIM/2022/KIM-Studie2022_website_final.pdf.

Feierabend, Sabine; Rathgeb, Thomas; Kheredmand, Hediye; Glöckler, Stephan (2023b): JIM-Studie 2023. Jugend, Information, Medien. Basisuntersuchung zum Medienumgang 12- bis 19-jähriger. Medienpädagogischer Forschungsverbund (mpfs). https://www.mpfs.de/fileadmin/files/Studien/JIM/2022/JIM_2023_web_final_kor.pdf.

Feinberg, Joel (1980): Child's Right to an Open Future. In: William Aiken und Hugh LaFollette (Hg.): Whose Child? Parental Rights, Parental Authority and State Power. Totowa, NJ: Rowman and Littlefield, S.124–153.

Find a Balance with Technology that Feels Right for You. (03.09.2024) Google Digital Wellbeing. https://wellbeing.google/.

Funiok, Rüdiger (2002): Medienethik: Trotz Stolpersteinen ist der Wertediskurs über Medien unverzichtbar. In: Matthias Karmasin (Hg.): Medien und Ethik. Stuttgart: Reclam, S. 37–58.

Funiok, Rüdiger (2007): Medienethik. Verantwortung in der Mediengesellschaft. Stuttgart: Kohlhammer.

Gardella, Joseph H.; Fisher, Benjamin W.; Teurbe-Tolon, Abbie R. (2017): A Systematic Review and Meta-Analysis of Cyber-Victimization and Educational Outcomes for Adolescents. In: Review of Educational Research 87(2), S. 283–308. DOI: 10.3102/0034654316689136.

Gebel, Christa; Lampert, Claudia; Brüggen, Niels; Dreyer, Stephan; Lauber, Achim; Thiel, Kira (2022): Jugendmedienschutzindex 2022. Der Umgang mit Onlinebezogenen Risiken. Berlin: Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.

Gini, Gianluca; Card, Noel. A.; Pozzoli, Tiziana (2018): A meta-analysis of the differential relations of traditional and cyber-victimization with internalizing problems. In: Aggressive Behavior, 44(2), S. 185–198. DOI: 10.1002/ab.21742.

Gui, Marco; Fasoli, Marco; Carradore, Roberto (2017): „Digital Well-Being". Developing a New Theoretical Tool For Media Literacy Research. In: Italian Journal of Sociology of Education, 9(1), S. 155–173. DOI: 10.14658/pupj-ijse-2017-1-8.

Hasebrink, Uwe; Lampert, Claudia; Thiel, Kira (2019): Online-Erfahrungen von 9- bis 17-Jährigen: Ergebnisse der EU Kids Online-Befragung in Deutschland 2019. (2. überarb. Auflage). Hamburg: Hans-Bredow-Institut.

HateAid (2024): In meinem Netz soll es keine Gewalt geben! Wie junge Erwachsene digitale Gewalt erleben und wie sie damit umgehen. Berlin.

Hourcade, Juan Pablo; Zeising, Anja; Iversen, Ole Sejer; Pares, Narcis; Eisenberg, Michael; Quintana, Chris; Skov, Mikael B. (2017): Child-Computer Interaction SIG. Ethics and Values. In: Gloria Mark (Hg.): Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, S. 1334–1337. DOI: 10.1145/3027063.3049286.

Hurrelmann, Klaus; Quenzel, Gudrun (2018): Developmental tasks in adolescence. London: Routledge.

I-KiZ. Zentrum für Kinderschutz im Internet (2017): Modell des Intelligenten Risikomanagements. https://kinderrechte.digital/hintergrund/index.cfm/topic.279/key.1497.

Kheredmand, Hediye (2022): JIMplus 2022. Fake News und Hatespeech – Fake News und Hatespeech im Alltag von Jugendlichen. Medienpädagogischer Forschungsverbund Südwest (mfps). https://www.lfk.de/fileadmin/PDFs/Publikationen/Studien/JIMplus-2022/JIMplus-2022.pdf.

Krainer, Larissa (2002): Medienethik als angewandte Ethik: Zur Organisation ethischer Entscheidungsprozesse. In Matthias Karmasin (Hg.): Medien und Ethik. Stuttgart: Reclam, S. 156–174.

Kurian, Nomisha (2024): EU AI Act: How well does it protect children and young people? Leverhulme Centre for Future of Intelligence. https://www.lcfi.ac.uk/news-events/blog/post/eu-ai-act-how-well-does-it-protect-children-and-young-people.

Kultusministerkonferenz (KMK) (2016): Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt". (Beschluss der Kultusministerkonferenz vom 08.12.2016. Berlin: Sekretariat der Kultusministerkonferenz. https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2018/Digitalstrategie_2017_mit_Weiterbildung.pdf.

Kultusministerkonferenz (KMK) (2021): Lehren und Lernen in der digitalen Welt. Die ergänzende Empfehlung zur Strategie „Bildung in der digitalen Welt". Beschluss der Kultusministerkonferenz vom 09.12.2021. Berlin: Sekretariat der Kultusministerkonferenz. https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2021/2021_12_09-Lehren-und-Lernen-Digi.pdf.

Kwan, Irene, Dickson, Kelly; Richardson, Michelle; MacDowall, Wendy, Burchett, Helen; Stansfield, Claire; Brunton, Ginny; Sutcliffe, Katy; Thomas, James (2020): Cyberbullying and Children and Young People's Mental Health: A Systematic Map of Systematic Reviews. In: Cyberpsychology, Behavior, and Social Networking, 23(2), S. 72–82. DOI: 10.1089/cyber.2019.0370.

Landesanstalt für Medien NRW (2024): Kinder und Jugendliche als Opfer von Cybergrooming. Zentrale Ergebnisse der 4. Befragungswelle 2024. https://www.medienanstalt-nrw.de/fileadmin/user_upload/Forschung/LFM_Cybergrooming_Studie_2024.pdf.

Livingstone, Sonia (2014): Risk and harm on the internet. In: Amy B. Jordan und Daniel Romer (Hg.): Media and the well-being of children and adolescents, S.129–146. Oxford University Press.

Livingstone, Sonia; Haddon, Leslie (Hg.) (2009): Kids Online. Opportunities and Risks for Children. Bristol: The Policy Press.

Livingstone, Sonia; Stoilova, Maria (2021): The 4Cs: Classifying Online Risk to Children. In: CO:RE Short Report Series on Key Topics. Hamburg: Leibniz-Institut für Medienforschung, Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. DOI: 10.21241/ssoar.71817.

Madigan, Shery; Ly, Anh; Rash, Christina L., Van Ouytsel, Joris; Temple, Jeff R., (2018): Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis. In: JAMA Pediatrics Patient Page, 172(4), S. 327–335. DOI: 10.1001/jamapediatrics.2017.5314.

Mahboob Kanafi, Matin; Iivari, Netta; Kinnula, Marianne; Sharma, Sumita (2022): Uncovering Children's Situated Design Capital – A Nexus Analytic Inquiry. In: Interaction Design and Children. IDC '22: Interaction Design and Children. Braga Portugal, 27.06.2022 - 30.06.2022. New York, NY, USA: ACM, S. 408–421.

Marciano, L., Schulz, P. J., & Camerini, A.-L. (2020): Cyberbullying Perpetration and Victimization in Youth: A Meta-Analysis of Longitudinal Studies. In: Journal of Computer-Mediated Communication, 25(2), S. 163–181. DOI: 10.1093/jcmc/zmz031.

Moore, Sophie. E.; Norman, Rosana E.; Suetani, Shuichi; Thomas, Hannah J.; Sly, Peter. D.; Scott, James G. (2017): Consequences of bullying victimization in childhood and adolescence: A systematic review and meta-analysis. In: World Journal of Psychiatry, 7(1), S. 60–76. DOI: 10.5498/wjp.v7.i1.60.

Nairn, Agnes; Clarke, Barbie (2012): Researching Children: Are We Getting it Right? A Discussion of Ethics. In: International Journal of Market Research 54 (2), S. 177–198. DOI: 10.2501/IJMR-54-2-177-198.

Nuissl, Ekkehard (2018): Weiterbildung/Erwachsenenbildung. In: Rudolf Tippelt und Bernhard Schmidt-Hertha (Hg.): Handbuch Bildungsforschung. Wiesbaden: Springer Fachmedien Wiesbaden, S. 485–504.

Paschel, Felix; Pfetsch, Jan. (2024a): Sicht jugendlicher Bystander auf Cybermobbing, Online-Hatespeech und non-konsensuales Sexting: Fokusgruppen zu sozialen und normativen Einflüssen auf die Bystander bei Online-Interaktionsrisiken [Poster]. Forum Interaktionsrisiken II, 05.03.2024, Berlin. http://sikid.de/content/files/2024/07/Poster-SIKID4_TUBerlin.pdf.

Paschel, Felix; Pfetsch, Jan (2024b): „FairNetzt" - Entwicklung eines Bildungsprogramms zur Förderung digitaler Zivilcourage [Präsentation]. SIKID-Abschlussveranstaltung, 24.06.2024, Berlin. https://sikid.de/content/files/2024/06/SIKID-Pr-sentation-Abschlusstagung_2024_06_24-1.pdf.

Paschel, Felix, Schultz, Mary, von Salisch, Maria, Pfetsch, Jan (im Erscheinen): Online -Interaktionsrisiken von Kindern und Jugendlichen aus psychologischer Sicht: Cybermobbing, Hatespeech, Sexting und Cybergrooming. Beltz Juventa.

Pfetsch, Jan (2018): Jugendliche Nutzung digitaler Medien und elterliche Medienerziehung – Ein Forschungsüberblick. In: Praxis der Kinderpsychologie und Kinderpsychiatrie 67 (2), S. 110–133. DOI: 10.13109/prkk.2018.67.2.110.

Pfetsch, Jan (2019): Exkurs: Förderung von Zivilcourage zur Prävention von Aggression in der Schule. In: Matthias Böhmer; Georges Steffgen (Hg.): Mobbing an Schulen. Prävention, Intervention und Nachsorge. Wiesbaden: Springer. S. 99–112. DOI: 10.1007/978-3-658-26456-7_6.

Pfetsch, Jan; Paschel, Felix; Bieß, Cora; Stapf, Ingrid (2024, im Erscheinen): Forschungsethik und Kinderrechte. Spannungsfelder der Forschung mit Heranwachsenden am Beispiel der informierten Einwilligung. Medienpädagogik.

Prinzing, Marlis; Stapf, Ingrid (2024): Gutes Leben im Digitalen regeln. Eckpunkte einer ethisch und multiperspektivisch ausgerichteten Media Governance. In: Michael Litschka, Claudia Paganini und Lars Rademacher (Hg.): Digitalisierte Massenkommunikation und Verantwortung. Politik, Ökonomik und Regulierung von Plattformen. Baden-Baden: Nomos, S. 121–140.

Rauschenbach, Thomas; Düx, Wiebken; Sass, Erich (2007): Einleitung. In: Thomas Rauschenbach, Wiebken Düx und Erich Sass (Hg.): Informelles Lernen im Jugendalter: Vernachlässigte Dimensionen der Bildungsdebatte. 2. Aufl. Beltz Juventa, S. 7–14.

Riedel, Manfred (1979): Norm und Werturteil: Grundprobleme der Ethik. Stuttgart: Reclam.

Rutledge, Pamela B. (2020): Positive Media Psychology. In: Jan van den Bulck; David R. Ewoldsen; Marie-Louise Mares; Erica Scharrer (Hg.): The International Encyclopedia of Media Psychology. Hoboken: John Wiley & Sons. DOI: 10.1002/9781119011071.iemp0281.

Schoeler, Tabea; Duncan, Lauren; Cecil, Charlotte M.; Ploubidis, George B.; Pingault, Jean-Baptiste (2018): Quasi-experimental evidence on short- and long-term consequences of bullying victimization: A meta-analysis. Psychological Bulletin, 144(12), S. 1229–1246. DOI: 10.1037/bul0000171.

Schultze-Krumbholz, Anja; Pfetsch, Jan S.; Lietz, Katrin (2022): Cyberbullying in a Multicultural Context—Forms, Strain, and Coping Related to Ethnicity-Based Cybervictimization. In: Frontiers in Communication 7 (Art.846794). DOI: 10.3389/fcomm.2022.846794.

Seligman, Martin E. P. (2002): Authentic happiness: Using the new positive psychology to realize your potential for lasting fulfillment. New York: Free Press.

Seligman, Martin E. P.; Csikszentmihalyi, Mihaliy (2000): Positive Psychology: An Introduction. In: American Psychologist. 55 (1), S. 5–14. DOI: 10.1037/0003-066X.55.1.5.

Smahel, Daniel; Machackova, Hana; Mascheroni, Giovanna; Dedkova, Lenka; Staksrud, Elisabeth; Ólafsson, Kjartan; Livingstone, Sonia; and Hasebrink, Uwe (2020): EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. DOI: 10.21953/lse.47fdeqj01ofo.

Stapf, Ingrid (2006): Medien-Selbstkontrolle. Ethik und Institutionalisierung. UVK-Verlag-Ges.

Stapf, Ingrid; Bieß, Cora; Heesen, Jessica; Adelio, Oduma; Pavel, Carla; Andresen, Sünje; Dreyer, Stephan; Lampert, Claudia; Paschel, Felix; Pfetsch, Jan; Thiel, Kira (2022): Zwischen Fürsorge und Forschungszielen. Ethische Leitlinien für die Forschung mit Kindern zu sensiblen Themenbereichen. Tübingen: Internationales Zentrum für Ethik in den Wissenschaften. Materialien zur Ethik in den Wissenschaften, Band 20. https://sikid.de/content/files/2023/07/SIKID-Forschungsethisches-Konzept.pdf.

Stapf, Ingrid; Bieß, Cora; Pfetsch, Jan; Paschel, Felix (2023): Respecting children's rights in research ethics and research methods. In: Journal of Children and Media 17 (3), S. 393–399. DOI: 10.1080/17482798.2023.2235815

Stapf, Ingrid; Dreyer, Stephan; Schelenz, Laura; Andresen, Sünje; Heesen, Jessica (2023): Die Stärkung von Kinderrechten durch den Digital Services Act (DSA): Wege zu Best-Practice-Ansätzen. DOI: 10.5281/zenodo.8358649.

Stapf, Ingrid; Heesen, Jessica (im Erscheinen): Ethical guidelines for doing research with children in sensitive subject areas. In: Pranee Liamputtong (Hg.): Handbook of Sensitive Research in the Social Sciences. Edward Elgar Publishing.

Stapf, Ingrid; Prinzing, Marlis (2024): Selbstbestimmte Teilhabe und Schutz vor Verstörung. Kindgerechte Plattformregulierung: Multistakeholder*innen-Perspektiven in Zeiten von Krieg und Polykrisen. merz | medien + erziehung, 68(4), I–IX. https://www.merz-zeitschrift.de/fileadmin/user_upload/merz/PDFs/merz_24-4_online_exklusiv_stapf_ingrid_prinzing_marlis_selbstbestimmte_teilhabe_und_schutz_vor_verstoerung.pdf.

Stapf, Ingrid; Dreyer, Stephan (im Erscheinen): Ethische Reflexionsräume als deliberatives Instrument in der Technikregulierung. In: Jörg Noller und Karoline Reinhardt (Hg.): Handbuch Philosophie der Digitalität. Springer.

Stalder, Felix (2016): Kultur der Digitalität. Berlin: Suhrkamp.

Süss, Daniel (2012): Positiver Medienumgang und Medienkompetenz. In: Christoph Steinebach, Daniel Jungo und René Zihlmann (Hg.): Positive Psychologie in der Praxis. Anwendung in Psychotherapie, Beratung und Coaching. Weinheim: Julius Beltz GmbH & Co. KG, S. 220–227.

The Forum for Well-being in Digital Media. (04.09.2024). Israel National Commission for UNESCO. https://hwbdigitalmedia.wixsite.com/hwb-digitalmedia-/modus-operandi.

Thiel, Kira; Lampert, Claudia. (2023a): Wahrnehmung, Bewertung und Bewältigung belastender Online-Erfahrungen von Jugendlichen. Eine qualitative Studie im Rahmen des Projekts „SIKID – Sicherheit für Kinder in der digitalen Welt". Hamburg: Hamburg: Hamburg: Leibniz-Institut für Medienforschung, Hans-Bredow-Institut (HBI); Arbeitspapiere des Hans-Bredow-Instituts, Projektergebnisse 65. DOI: 10.21241/ssoar.86633.

Thiel, Kira; Lampert, Claudia (2023b): Zwischen Genervtsein und Belastung – Online-Interaktionsrisiken aus Sicht von Jugendlichen. In: JMS-Report, 46(6), S. 2–5. DOI: 10.5771/0170-5067-2023-6-2.

Thiel, Kira; Lampert, Claudia (2024): Ideen von Jugendlichen für ein sicheres Internet. Hamburg: Hamburg: Leibniz-Institut für Medienforschung, Hans-Bredow-Institut (HBI); Media Research Blog. https://leibniz-hbi.de/ideen-von-jugendlichen-fuer-ein-sicheres-internet/.

Third, Amanda; Moody, Lilly (2021): Our rights in the digital world: A report on the children's consultations to inform UNCRC General Comment 25. London and Sydney: 5Rights Foundation and Western Sydney University.

Tillmann, Angela; Hugger, Kai-Uwe (2014): Mediatisierte Kindheit – Aufwachsen in mediatisierten Lebenswelten. In: Angela Tillmann, Sandra Fleischer und Kai-Uwe Hugger (Hg.): Handbuch Kinder und Medien. Wiesbaden: Springer Fachmedien Wiesbaden, S. 31–45.

Tokunaga, Robert S. (2010): Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior, 26(3), S. 277–287. DOI: 10.1016/j.chb.2009.11.014.

UK Information Commissioner's Office (2020): Age Appropriate Design: a Code of Practice for Online Services. https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf.

Vanden Abeele, Mariek M.P. (2021): Digital Wellbeing as a Dynamic Construct. In: Communication Theory 31(4), S. 932–955. DOI: 10.1093/ct/qtaa024.

Vogelsang, Verena (2017): Sexuelle Viktimisierung, Pornografie und Sexting im Jugendalter—Ausdifferenzierung einer sexualbezogenen Medienkompetenz. Wiesbaden: Springer VS.

Vogler, Hans-Joachim; Anders, Petra; Kunzmann, Stefan; Pfetsch, Jan; Müller, Mathias (2022): Lernen mit und über Medien. Standards für die Medienbildung in der Lehrkräftebildung in Berlin. Arbeitsbündnis Medienbildung, Senatsverwaltung für Bildung, Jugend und Familie. https://www.berlin.de/sen/bildung/unterricht/medien/lehr-und-lernmittel/.

Wachs, Sebastian; Wright, Michelle F.; Gámez-Guadix, Manuel; Döring, Nicola (2021): How Are Consensual, Non-Consensual, and Pressured Sexting Linked to Depression and Self-Harm? The Moderating Effects of Demographic Variables. In: International Journal of Environmental Research and Public Health, 18(5), S. 2597. DOI: 10.3390/ijerph18052597.

Well-being Guide. (04.09.2024) TikTok. https://www.tiktok.com/safety/en/well-being-guide/.

Wellbeing Features on Snapchat. (04.09.2024). Snapchat. https://help.snapchat.com/hc/el/articles/7012398974612-Wellbeing-Features-on-Snapchat.

What is Digital Wellbeing? Defining a Framework to help you find it. (2023) Sentient Digital Consulting. https://www.sentientdigitalconsulting.com/insights/9xvyxue7djj2omogziityvtxs7krt6.

What is Human Security? (04.09.2024) United Nations Trust Fund for Human Security https://www.un.org/humansecurity/wp-content/uploads/2018/04/What-is-Human-Security.pdf.

Wong-Villacres, Marisol; DiSalvo, Carl; Kumar, Neha; DiSalvo, Betsy (2020): Culture in Action: Unpacking Capacities to Inform Assets-Based Design. In: Regina Bernhaupt, Florian 'Floyd' Mueller, David Verweij, Josh Andres, Joanna McGrenere, Andy Cockburn et al. (Hg.): Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. CHI '20: CHI Conference on Human Factors in Computing Systems. Honolulu HI USA, 25 April 2020 - 30 April 2020. New York, NY, USA: ACM, S. 1–14.

Wright, Michelle F.; Wachs, Sebastian (2019): Adolescents' Psychological Consequences and Cyber Victimization: The Moderation of School-Belongingness and Ethnicity. In: International Journal of Environmental Research and Public Health, *16*(14), S. 2493. DOI: 10.3390/ijerph16142493.

Wunden, Wolfgang (1998): Freiheit und Medien. Beiträge zur Medienethik 4. GEP.

5Rights Foundation (2024): World 1st International AI treaty caters to children, but fails to agree mandatory rules for corporates. https://5rightsfoundation.com/in-action/world-1st-international-ai-treaty-caters-to-children-but-fails-to-agree-mandatory-rules-for-corporates.html.