

#DigitaleVorbilder
Familien gehen online.

Orientierungshilfe Datenschutz:

Ein Familien-Guide für den digitalen Dschungel

Scanne den QR-Code und schau dir, zusätzlich zur Broschüre, unsere Bildungsmaterialien wie Videos, Graphic Recordings, Kurzclips und vieles mehr an.

Die hier erstellte „Orientierungshilfe Datenschutz“ befasst sich mit übergreifenden Themen der Medienerziehung und Datenschutzsensibilisierung für Familien mit Wohnort im Geltungsbereich der EU-DSGVO. Die rechtliche Einordnung im Themenabschnitt „Diese Rechte gelten auch im Netz“ findet aus Perspektive des ausführenden Projektlandes Deutschland statt. Dabei spielen neben den international anerkannten UN-Kinderrechten und allgemeinen Persönlichkeitsrechten insbesondere ausschließlich in Deutschland geltende Gesetze eine Rolle, wie das Deutsche Grundgesetz (GG), das Deutsche Strafgesetzbuch (StGB) und die deutschen Jugendschutzgesetze. Ferner beziehen sich die Linktipps ausschließlich auf deutschsprachige Webseiten, die das Projektteam am Ende jedes Kapitels zur weiteren Recherche empfiehlt.

Vorwort

Was hat Datenschutz mit Medienbildung und Medienerziehung zu tun? In unserer digitalisierten Welt wird es immer schwieriger zu überblicken, wo überall Datenspuren verbleiben. Das ist für Erwachsene schon schwierig, aber erst recht für Kinder und Jugendliche. Aus diesem Grund haben wir, die Datenschutzbeauftragten aus Mecklenburg-Vorpommern (LfDI MV) und Hamburg (HmbBfDI), das von der EU geförderte Projekt **#DigitaleVorbilder – Familien gehen online.** ins Leben gerufen. Ziel des Projektes ist es, Familien bei einer aktiven Medienerziehung ihrer Kinder zu unterstützen.



Thomas Fuchs
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Datenschutzaufsichtsbehörden haben - neben der Aufgabe als Aufsichtsbehörde - auch den gesetzlichen Auftrag, „die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung [zu] sensibilisieren und sie darüber auf[zu]klären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;“ (Art. 57 Ziffer 1 lit b DSGVO). Wir bieten in Hamburg und Mecklenburg-Vorpommern deshalb schon seit längerem Angebote zur Medienbildung und Datenschutzsensibilisierung für Kinder und Jugendliche sowie für pädagogische Fachkräfte an. Mit unserem **EU-Projekt** haben wir uns nun einer neuen Zielgruppe gewidmet: **den Familien**.



Sebastian Schmidt
Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Wir sind der Meinung, dass Datenschutzbewusstsein und digitale Kompetenzen notwendiges Wissen sind. Uns ist bewusst, dass im Familienalltag digitale Medien und Apps nicht mehr wegzudenken sind.

Uns leitet der Ansatz, dass Kinder und Jugendliche die Vor- und Nachteile der Nutzung digitaler Medien kennen müssen, um sich **sicher und selbstbestimmt** in unserer digitalen Gesellschaft bewegen zu können.

In unserem EU-Projekt **#DigitaleVorbilder** haben wir viele Expert:innen zu Wort kommen lassen und nach Tipps und Tricks befragt. Das gesamte Fachwissen finden Sie auf unserer Webseite www.digitale-vorbilder.eu und in dieser Broschüre, die Sie in der Hand halten.
Viel Spaß beim Lesen, Durchstöbern und gerne auch Teilen mit interessierten Menschen, denn wir sind alle **#DigitaleVorbilder** für unsere Kinder und Jugendlichen!

Herzliche Grüße,
Thomas Fuchs und Sebastian Schmidt

Inhaltsverzeichnis

1 Vorwort 1

2 Inhaltsverzeichnis 2

3 Wer steht hinter #DigitaleVorbilder? 3-4
Projektvorstellung & Das sagt das Projektteam

4 Themen 5-71

4.1 Einführung in den Datenschutz 5-7
4.2 Die größten Datenschutzmythen 8-13
4.3 Rechte, Pflichten & Verantwortung im digitalen Raum 14-19
4.4 Kinderbilder im Netz 20-25
4.5 TikTok, Insta, Snapchat & Co 26-31
4.6 Mediennutzung in der Familie 32-37
4.7 Gaming: spielend sicher 38-43
4.8 Cybermobbing 44-49
4.9 Tatort Internet – Cybergrooming 50-55
4.10 Smart Family 56-61
4.11 Smarte Spielzeuge 62-67
4.12 Exkurs: Messengerdienste 68-71

5 Literaturverzeichnis 72-73
Verweise zum Nachlesen

6 Index 74-78
Alle wichtigen Begriffe kurz erklärt

7 Danksagung 79

8 Impressum 80

Projektvorstellung

Wer wir sind

#DigitaleVorbilder – Familien gehen online. ist ein Gemeinschaftsprojekt des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) und des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) in Kooperation mit dem Hamburger Bürger:innensender TIDE. Es wird durch das Programm „Citizens, Equality, Rights and Values" (CERV) der Europäischen Union im Zeitraum 11/2022 - 10/2024 finanziert.

Ein bis in die Fingerspitzen motiviertes und engagiertes fünfköpfiges Team aus den Bereichen Sozialpädagogik, Soziologie, Sozialwissenschaften, Kommunikations- und Medienwissenschaften hat das Projekt **#DigitaleVorbilder** länderübergreifend mit Leben gefüllt.

Was wir möchten

Wir haben den Wunsch, das Thema Datenschutz für Familien erlebbar und verständlich zu machen. Wir möchten Familien für die digitale Lebenswelt ihrer Kinder und für neue technologische Entwicklungen begeistern, ihnen Hilfestellungen zum Schutz ihrer Privatsphäre und zur sicheren Mediennutzung ihrer Kinder aufzeigen sowie sie ermutigen, das eigene Mediennutzungsverhalten zu hinterfragen.

Dabei werden sämtliche Themen aufgegriffen, die wir für den Familienalltag rund um den Umgang mit digitalen Medien für wichtig erachtet haben: von smarten Spielzeugen über Rechte und Pflichten im digitalen Raum bis hin zu Gaming oder Social Media.

Um was es in dieser Broschüre geht

Mit dieser Handreichung wollen wir auf einen Blick inhaltlich komprimierte Informationen zur Verfügung stellen, die durch ansprechend gestaltete Graphic Recordings ergänzt werden. Die Grafiken basieren auf den Aufnahmen der zu den Kapiteln passenden Webinare.

Nach einem einleitenden allgemeinen Datenschutzteil und der Klärung einiger ziemlich populärer Datenschutzmythen haben wir in den Kapiteln jeweils die folgenden Fragen beantwortet:

- Warum ist das ausgewählte Thema für Familien relevant?
- Was hat das Thema konkret mit Datenschutz zu tun?
- Welche Rechte werden von dem Thema berührt, die auch im Netz beachtet werden müssen?
- Welche Präventivtipps und welche Notfalltipps können wir Eltern mit auf den Weg geben?

Wir wünschen uns, dass diese Broschüre hilft, im privaten und beruflichen Kontext mit dem eigenen Mediennutzungsverhalten **#DigitaleVorbilder** zu sein. Die Broschüre wurde auch in andere Sprachen übersetzt und kann auf unserer Homepage **www.digitale-vorbilder.eu** heruntergeladen werden.

Viel Freude und erhellende Erkenntnisse beim Lesen wünscht das Projektteam

Antje, Alina, Christina, Isabel und Lydia

Das sagt das Projektteam:

Alina:

Kinder wachsen heute in einer digitalisierten Welt auf und sollten daher frühzeitig lernen, kompetent und verantwortungsvoll mit digitalen Medien umzugehen. Das Projekt **#DigitaleVorbilder** hat eindrucksvoll verdeutlicht, dass das Thema Datenschutz nach wie vor von großer Relevanz ist und viele Familien beschäftigt. Ich freue mich sehr über den großen Zuspruch, den wir in den letzten zwei Jahren erhalten haben. Eines ist jedoch klar: **#DigitaleVorbilder** steht erst am Anfang und es gibt noch viel zu tun!

Antje:

Mit dem Projekt **#DigitaleVorbilder** wollen wir speziell Familien ansprechen und sensibilisieren, sich mit der Medienerziehung und dem Thema Datenschutz für sich und ihre Kinder auseinanderzusetzen. Denn die Kinder haben diese Medienwelt nicht erschaffen, sondern wir Erwachsene. So ist es auch unsere Verantwortung, den Kindern und Jugendlichen die notwendigen Skills und ein mediales Werteverständnis mitzugeben. Viele Eltern scheuen diese Auseinandersetzung. Unser Projekt hat jedoch gezeigt, dass das Interesse da ist, wenn die Inhalte, wie in unserem Projekt, gut aufbereitet werden.



Christina:

Nicht nur Eltern, die ganze Gesellschaft ist gefragt, wenn es darum geht, mit gutem Beispiel voranzugehen. Denn auch im digitalen Raum sind die Persönlichkeitsrechte eines jeden Menschen durch ein respektvolles Miteinander zu wahren. Das fängt beim Respekt vor der eigenen Privatsphäre durch einen achtsamen Umgang mit den eigenen Daten an!

Isabel:

Im digitalen Zeitalter ist der Schutz von persönlichen Daten von großer Bedeutung, insbesondere von Kindern. Es ist wichtig, dass wir als Gesellschaft sicherstellen, dass Datenschutz nicht nur ein Schlagwort, sondern gelebte Realität ist. Dabei sollten wir als digitales Vorbild agieren und die Verantwortung für einen sicheren Umgang mit Daten übernehmen.

Lydia:

Die sichere Nutzung digitaler Medien kann ein verbindendes Element sein. Das habe ich im Rahmen von **#DigitaleVorbilder** festgestellt. Denn die meisten Eltern haben Sorgen, dass ihre Kinder zu viele Informationen im Netz von sich preisgeben oder von Unbekannten angeschrieben werden. Ich habe viele wissbegierige Eltern erlebt, die dankbar über Tipps sind. Wie schön, dass unsere Videos, Graphic Recordings und diese Broschüre noch lange genutzt werden können und sich noch mehr Familien mit diesem wichtigen Thema beschäftigen können.

DATENSCHUTZ FÜR FAMILIEN

Mit diesem einleitenden Kapitel soll ein Grundverständnis für das Thema Datenschutz geschaffen werden. Damit die folgenden Kapitel verständlich und nachvollziehbar sind, ist es wichtig, sich ein Basiswissen zu verschaffen. Auf den folgenden zwei Seiten werden die Grundsätze und gängige Begriffe aus dem Datenschutzrecht erklärt.

WAS WIRD UNTER DATENSCHUTZ VERSTANDEN?

Wenn wir von Datenschutz sprechen, meinen wir den **Schutz der Privatsphäre**. Jede natürliche Person darf über die Preisgabe und Verwendung ihrer personenbezogenen Daten selbst bestimmen. Dies wird auch das **Recht auf informationelle Selbstbestimmung** genannt.



Was sind personenbezogene Daten?
Dies sind alle Informationen, durch die **eine lebende Person identifiziert** werden kann, also z. B.:

- Kontaktdaten (Name, Adresse, Telefonnummer, E-Mail)
- Standortdaten
- Informationen über Vorlieben und Interessen
- wer mit wem und wie lange kommuniziert
- das Kaufverhalten
- die Art des Endgerätes

Es gibt auch **besonders sensible Daten**, die einen **besonderen Schutz** genießen. Dies sind Informationen über:

- die ethnische und kulturelle **Herkunft**
- politische, religiöse und philosophische **Überzeugungen**
- **Gesundheit**
- **Sexualität**
- **Gewerkschaftszugehörigkeit**

DAS EUROPÄISCHE REGELBUCH ZUM DATENSCHUTZ:

Das Regelbuch für den Datenverkehr in Europa ist die Europäische **Datenschutz-Grundverordnung**, kurz **DSGVO**.

Unternehmen und öffentliche Einrichtungen, wie Schulen oder Behörden (laut DSGVO **Verantwortliche**), müssen sich an die DSGVO halten, sobald Daten von Personen (laut DSGVO **Betroffene**) erhoben werden.

Die DSGVO gilt aber nicht, wenn personenbezogene Daten **ausschließlich für familiäre und persönliche Aktivitäten genutzt werden**. Diese fallen unter das „**Haushaltsprivileg**“, wie z.B. privater Schriftverkehr, Adressbuch, private Kontaktlisten, Urlaubsfotos und private Aufnahmen von Freund:innen und Familie.

Ergänzt wird die DSGVO in Deutschland durch das Bundesdatenschutzgesetz (BDSG), Landesdatenschutzgesetze sowie weitere Spezialgesetze, wie z.B. Schulgesetz, Kindertagesförderungsgesetz.

DIE GRUNDSÄTZE DER DSGVO:

Sieben **Grundsätze** bestimmen die Art und Weise, wie personenbezogene Daten verwendet werden dürfen.

Diese sollen sicherstellen, dass mit persönlichen Daten sorgsam und verantwortungsvoll umgegangen wird. Sie bilden die Grundlage für die **Betroffenenrechte**, auf die sich Verbraucher:innen berufen können.

1. Rechtmäßigkeit

Der Grundsatz der **Rechtmäßigkeit** besagt, dass die Verarbeitung personenbezogener Daten prinzipiell verboten ist. Es besteht die Ausnahme, wenn es sich um geltende **Rechtsgrundlagen handelt**, wie z.B. Kauf- oder Behandlungsverträge, Schulgesetze oder Einwilligungen über den Erhalt eines Newsletters.

2. Transparenz

Die DSGVO fordert von den Unternehmen, Behörden und anderen Einrichtungen **Transparenz**. Wenn sie Daten verarbeiten wollen, müssen sie deshalb ihrer **Informationspflicht** nachkommen, weshalb es **Datenschutzerklärungen**, **Cookie-Banner** und **Hinweise auf Kameraüberwachung** im öffentlichen Raum gibt.

Personen, deren Daten verarbeitet werden, haben Dank des Transparenz-Grundsatzes ein **Auskunftsrecht**. Das bedeutet, dass sie Unternehmen und Behörden fragen können, welche Daten von ihnen zu welchem Zweck verarbeitet werden, an wen die Daten ggf. weitergegeben und wie lange diese gespeichert werden. Außerdem erfahren sie, woher die Verantwortlichen diese Daten haben und ob sie diese automatisch, z.B. mit einer KI, auswerten. Die verantwortlichen Stellen müssen diese Fragen innerhalb von einem Monat beantworten.

Die wichtigsten Betroffenenrechte sind:

- **Recht auf Auskunft**
- **Recht auf Berichtigung**, falls falsche Daten im Umlauf sind
- **Recht auf Einschränkung** der Verarbeitung (wie eine „Pause“ für die Verarbeitung der Daten)
- **Recht auf Löschung**, falls die Daten nicht mehr notwendig sind für die Erfüllung eines Vertrags oder gesetzlich vorgeschriebener Aufbewahrungspflichten, wie bspw. im Steuerrecht
- **Recht auf Widerruf** einer Einwilligung mit Wirkung für die Zukunft
- **Recht auf Beschwerde** bei der zuständigen Aufsichtsbehörde

3. Zweckbindung

Der Grundsatz der **Zweckbindung** bedeutet, dass Verantwortliche Daten nur für einen bestimmten, vorab kommunizierten Zweck verwenden dürfen. Beispielsweise dürfen Kontaktdaten, die aufgrund einer Bestellung oder für die Anmeldung zu einem Kurs abgefragt wurden, nicht für die Kontaktaufnahme für Werbezwecke oder einen Newsletter genutzt werden. Es sei denn, man hat mit der Anmeldung gleich zugestimmt. Eine Einwilligung beim Facharzt zur Weiterleitung von Befunden an den Hausarzt bedeutet also nicht automatisch, dass diese Daten auch an ein medizinisches Forschungsinstitut weitergeleitet werden dürfen.

Sind Betroffene der Meinung, dass ihre Daten unrechtmäßig weitergegeben wurden, können sie sich an die zuständige **Datenschutzaufsichtsbehörde** wenden.

4. Datenminimierung

Neben der Zweckbindung ist auch Datensparsamkeit bzw. **Datenminimierung** ein wichtiger Grundsatz der DSGVO. Das heißt, es dürfen nur so viele Daten abgefragt und verarbeitet werden, wie tatsächlich für einen vorher definierten Vorgang benötigt werden. Es ist beispielsweise nicht wichtig für die Anmeldung bei einer Fahrschule zu wissen, welcher Religion eine Person angehört. Dies darf nicht abgefragt werden, nur weil die Fahrschule z.B. eine interne Statistik darüber führen möchte.

5. Richtigkeit

Der Grundsatz der Richtigkeit legt fest, dass gespeicherte Daten **richtig und aktuell** sein müssen. Trifft dies nicht zu, können Betroffene verlangen, dass sie berichtigt oder ggf. gelöscht werden.

6. Speicherbegrenzung

Gespeicherte personenbezogene Daten dürfen nur so lange aufbewahrt werden, wie dies für den vorher festgelegten Zweck und damit einhergehende gesetzliche Verpflichtungen erforderlich ist. Aus diesem Grund müssen Verantwortliche für Datenverarbeitungen ein **Löschkonzept** vorhalten. Können Daten aus bestimmten Gründen noch nicht komplett gelöscht werden, muss darüber informiert werden.

7. Sicherheit der Daten

Betroffene müssen sich darauf verlassen können, dass ihre für einen notwendigen Zweck erhobenen Daten von den dafür Verantwortlichen **vertraulich** behandelt werden und **vor unbefugtem Zugriff geschützt sind**. Um dies sicherzustellen, müssen Einrichtungen technische und organisatorische Maßnahmen umsetzen, wie z. B. eine Schließanlage, Datenschutzschulungen und die Ausstattung der technischen Geräte mit sicheren Passwörtern.

LINKTIPPS

Multimediales Informationsportal für Verbraucher:innen zur DSGVO

↗ https://deinedatendeinerechte.de/

Kindgerechte Informationen des BlnBDI zur DSGVO

↗ https://data-kids.de/

Die größten Datenschutzmythen

– Argumentationshilfen für den Alltag



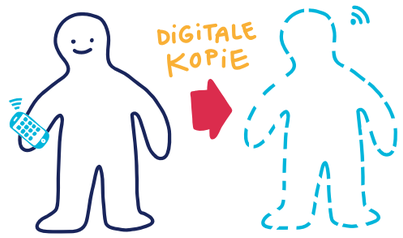
Wir leben in einer Welt ständig verfügbarer Informationen, die dank des Internets von jedem Ort aus abrufbar sind. Damit wir diese Informationen, Apps und Anwendungen nutzen können, braucht es meist eine Anmeldung oder Registrierung. Auf diese Weise sind unsere Daten schnell in alle Welt gestreut. Wer im Netz diese Informationen und Daten sehen kann, ist uns oft nicht bewusst. Einen Überblick über unsere Datenspuren zu behalten, fällt schwer. Im Falle eines Datenlecks kann dies unüberschaubaren Schaden verursachen.

MYTHOS 1: ICH HABE NICHTS ZU VERBERGEN UND MUSS MICH NICHT UM DATENSCHUTZ KÜMMERN.

Falsch! Der **Missbrauch von Daten**, die freiwillig oder unbeabsichtigt im Netz landen, kann großen persönlichen Schaden verursachen.
Es ist schwer zu überblicken, welche Konsequenzen mangelnder Datenschutz nach sich ziehen kann, da die Gefahr abstrakt wirkt. Es ist daher hilfreich, die **Risiken** zu kennen und einschätzen zu können.

Mögliche Folgen von Datenmissbrauch

1. **Verlust der Privatsphäre**, bspw. durch Standortverfolgung, Preisgabe von persönlichen Informationen, Abhörfunktionen oder unverschlüsselte Chats



2. **Profilbildung** durch eingegebene Daten und Verbindung von Daten unterschiedlicher Quellen, um passgenaue Inhalte und Werbung anzuzeigen
3. **Verlust des Grundrechts auf freie Entfaltung der Persönlichkeit** durch das Gefühl der Überwachung oder Bewertung
4. **Intransparente Datenübermittlung**, z.B. an Werbefirmen, Geheimdienste
5. **Manipulation von Kauf- oder gar Wahlentscheidungen** durch Tracking und personalisierte Werbung
6. **Identitätsdiebstahl oder -betrug,** indem Kriminelle mit fremden Namen einkaufen oder Verträge abschließen. Bekannte Delikte des Identitätsbetrugs sind der Enkeltrick 2.0, der CEO-Fraud oder sexuelle Erpressung (Sextortion).
7. **Diskriminierung** aufgrund von z.B. Herkunft, persönlicher Überzeugungen oder Vorlieben
8. **Rufschädigung, wirtschaftliche oder gesellschaftliche Nachteile** bis hin zur Existenzgefährdung
9. Scoring: Bewertung von Arbeitsleistungen, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben und Interessen
10. **Verlust der Vertraulichkeit von Berufsgeheimnissen**

MYTHOS 2: COOKIE-BANNER SIND DOCH NUR KOMPLIZIERT! EINFACH ALLES AKZEPTIEREN UND GUT IST!

Falsch! Um zu verstehen, warum es diese Cookie-Banner gibt und wie sie uns helfen, sei zunächst einmal erklärt, was Cookies sind und welche Funktion sie haben.

Was sind Cookies?

Cookies sind Informationen, die beim Aufruf einer Webseite im Internetbrowser eines Nutzenden gespeichert werden, um diese Person zu einem späteren Zeitpunkt wiedererkennen zu können. Sie werden direkt vom Webseitenbetreiber oder von Dritten gesetzt, die der Webseitenbetreiber in sein Angebot integriert.

Notwendige Cookies

Einige Cookies sind notwendig, um wichtige Funktionen einer Website zu ermöglichen. Solche Cookies speichern z. B. Login-Daten, den Inhalt eines Warenkorbs oder helfen bei der Gewährleistung der Sicherheit. Das ist auch für den Webseiten-Nutzenden von Vorteil, da Informationen wie die Sprache, das Ausfüllen von Feldern zur Dateneingabe (Personalien, Nutzungskonto, E-Mail-Adresse) oder personalisierte Produktvorschläge gespeichert werden.

Nicht notwendige Cookies

Andere Cookies sind hingegen nicht notwendig für den Betrieb der Webseite. Darunter fallen insbesondere Cookies von Werbetreibenden, Tracking- und Analysediensten, sogenannte Drittanbieter-Cookies. Diese werden genutzt, um das Verhalten der Nutzenden zu verfolgen und detaillierte Profile von ihnen zu erstellen.

Ob das Setzen nicht erforderlicher Cookies zugelassen werden sollte oder nicht, hängt davon ab, was jedem Einzelnen persönlich wichtig ist.
Als Eltern mit Vorbildfunktion sollte die eigene Internetnutzung jedoch datenschutzbewusst gestaltet werden, auch wenn dies nicht immer der einfachste und bequemste Weg ist.

Tipp 1: Die Browser-Erweiterung **Lightbeam** für Mozilla Firefox und Chrome visualisiert, wie mit Cookies von Dritten das Benutzerverhalten aufgezeichnet wird.

Tipp 2: Cookies können über viele Jahre bestehen bleiben. Das regelmäßige Löschen des Browserverlaufs und abgelegter Cookies in den Browser-Einstellungen und die Nutzung des privaten Modus bzw. strenger Tracking-Einstellungen erschwert das Anlegen eines Nutzerprofils.

Einwilligungserfordernis nicht notwendiger Cookies

Solche Cookies dürfen **nur mit Einwilligung des Nutzenden** verwendet werden. Webseitenbetreiber sind verpflichtet, mithilfe des Cookie-Banners anzugeben, welche Cookies verwendet werden. Sie fragen außerdem ab, ob neben den technisch erforderlichen auch weitere, **nicht** notwendige, Cookies gesetzt werden dürfen.

Warum ist >alle akzeptieren< nicht die beste Wahl?

Um die eigene Privatsphäre zu schützen und die Datenspuren im Netz überschaubar zu halten, ist es ratsam, den **Ablehnen-Button** bei Cookie-Bannern zu wählen oder sich die speziellen Cookies anzuschauen und separat auszuwählen. Mit sogenannten **Tracking-Cookies** lässt sich das **Nutzerverhalten auf Webseiten** erfassen: Was wird auf der Website wie lange angeschaut? Wie oft wurde die Seite bisher besucht und was angeklickt? Auf welchen Seiten ist die Person bereits vorher oder hinterher unterwegs?

Das seitenübergreifende Zusammenführen gesammelter Informationen lässt zusammen mit der IP-Adresse und Informationen zu genutzten Geräten eine **eindeutige Identifikation des Users** zu.
Die Möglichkeit des **Datenabgriffs** durch den Einsatz von Cookies ist das größte Risiko. Fehlerhafte oder nicht genügend geschützte Cookies können solch einen Datenklau ermöglichen.[1]





MYTHOS 3: ES IST DOCH KEIN PROBLEM, ÜBERALL DIESELBEN PASSWÖRTER ZU NUTZEN!

Doch, das ist definitiv ein Problem!
Wird ein Konto gehackt und es wurde für mehrere Dienste das gleiche Passwort in Verbindung mit einer E-Mail-Adresse genutzt, lassen sich damit leicht andere Konten hacken. Dies erhöht das Risiko von Identitätsdiebstahl, Datenverlust und unbefugtem Zugriff auf persönliche und sensible Informationen.

Was macht ein sicheres Passwort aus?

Ein gutes Passwort besteht aus mind. **12 Zeichen** und ist ein guter **Mix aus Sonderzeichen, Ziffern, Groß- und Kleinbuchstaben**. Zahlenreihenfolgen wie 1234 oder Namen des Haustieres oder Umlaute wie ä,ö, ü sind dabei nicht empfehlenswert.



Wie lassen sich Passwörter merken?

Tipp 1: Bilde einen Satz und verwende von jedem Wort jeweils den Anfangsbuchstaben in entsprechender Groß- & Kleinschreibung. Ersetze bestimmte Buchstaben durch Zahlen oder Sonderzeichen, z.B. E = 3, i = !

Tipp 2: Ein Passwortmanager hilft bei der Verwaltung der unterschiedlichen Passwörter.[2]

Tipp 3: Denke dir einen Satz inkl. Sonderzeichen aus und ergänze ihn bei jedem neuen Account mit der Abkürzung des Anbieters: z.B. Wirklichistgut!0815Insta

[1] vgl. N. 2024
[2] vgl. BSI 2024: Sichere Passwörter erstellen
[3] vgl. Wolfer 2024
[4] vgl. Welchering 2024

MYTHOS 4: MEIN SMARTPHONE HÖRT MIT.



Vermutlich nicht! Es gibt das Gerücht, dass Smartphones Gespräche mithören, um gezielte Werbung anzuzeigen.

Diese Gründe sprechen dagegen

1. Smartphone-Apps benötigen eine **ausdrückliche Erlaubnis**, um das Mikrofon nutzen zu dürfen.
2. Betriebssysteme ab Android 12 und iOS 14 lassen einen unbemerkten Zugriff auf Mikrofon und Kamera durch im Hintergrund laufende Apps nicht mehr zu. Sie informieren mithilfe eines **Privacy Indicators** darüber, wenn eine App das Mikrofon oder die Kamera benutzt.
3. Würde das Smartphone tatsächlich dauerhaft mithören und Gespräche übermitteln, müsste dies am Stromverbrauch und dem **verbrauchten Datenvolumen** zu erkennen sein.

Warum uns trotzdem personalisierte Werbung angezeigt wird

1. Werbeanzeigen basieren auf dem **Onlineverhalten des Nutzenden**. Suchanfragen, Browserverlauf und andere Daten helfen Werbefirmen, passende Anzeigen zu erstellen. Algorithmen nutzen die Daten, die ohnehin geteilt werden.
2. Auch persönliche Treffen können durch die **Kombination unseres Freundschaftsstatus** in sozialen Medien **mit unseren Standortdaten** dazu führen, dass uns dieses Produkt, über das sich vielleicht auch persönlich unterhalten wurde, im persönlichen Feed angezeigt wird.[3]
3. Tatsächlich gibt es eine **KI-basierte Technologie** namens „**Active Listening**". Sie ermöglicht es Werbefirmen, Gespräche in Echtzeit auszuwerten, um in Kombination mit anderen Verhaltensdaten der Person zielgerichtet Werbung auszuspielen. Ob diese in Deutschland verbotene Technologie in der Vergangenheit jedoch angewandt wurde, ist zum jetzigen Zeitpunkt nicht bewiesen.[4]



Wer nichts zu verbergen hat, hat auch nichts zu befürchten, oder?



LINKTIPPS



Mit dem HPI Identity Leak Checker kann geprüft werden, ob die eigene E-Mail-Adresse bereits in einem Datenleck gefunden wurde

↗ https://sec.hpi.de/ilc/

#DigitaleVorbilder

DIE 10 GRÖßTEN DATENSCHUTZMYTHEN

juuuport.de

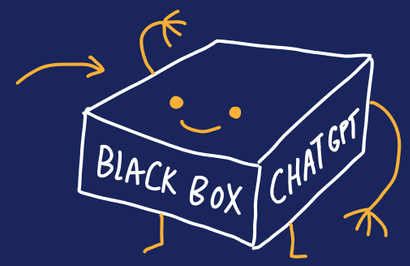
GRAPHIC RECORDING @elibrewing



































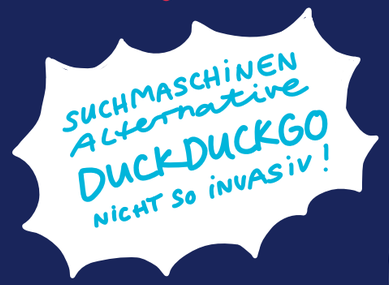


















Über die Moderatorin

Verena Gonsch
Journalistin, Autorin und Coach

Über die Referenten

Dr. Jens Ambrock
Referatsleiter Wirtschaft und Behörden beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI)
↗ datenschutz-hamburg.de

Ulrich Kühn
Stellvertr. Leitung beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) und Referatsleiter e-Privacy, Medien, Europa, Soziale Netzwerke
↗ datenschutz-hamburg.de

RECHTE, PFLICHTEN & VERANTWORTUNG IM DIGITALEN RAUM

Erziehungsberechtigte tragen Verantwortung für ihre Kinder, insbesondere auch im unübersichtlichen digitalen Raum. Zur Aufsichtspflicht gehört es, Kinder über Gefahren aufzuklären, sie über angemessenes Verhalten zu informieren, sichere Strukturen durch individuelle Schutzmaßnahmen zu schaffen und die Mediennutzung zu begleiten.

DARUM IST DAS FÜR FAMILIEN RELEVANT

Streit und Diskussionen wegen digitaler Medien? Das ist Alltag in den meisten Familien. Ob es die Bildschirmzeiten des Kindes sind, die Frage, welche Spiele gespielt werden oder wo Accounts angelegt werden dürfen.

Hilflosigkeit macht sich bei vielen Eltern breit, die sich fragen:

- Wie funktioniert eine entspannte und sichere Mediennutzung in unserem Familienleben?
- Welche Verantwortung habe ich als Elternteil, wenn mein Kind im digitalen Raum zunehmend selbstständiger agiert?
- Wie kann es gelingen, Kindern Medienkompetenz im stressigen Familien- und Berufsalltag zu vermitteln?

Unter **Medienkompetenz** wird die Fähigkeit verstanden, selbstbestimmt, kritisch und aktiv mit Medien umgehen zu können.

DAS HAT MEDIENERZIEHUNG MIT DATENSCHUTZ ZU TUN

Das Wissen darüber, wie man seine privaten Daten schützt, gilt als Teil der **Medienkompetenz**. Kinder sollten dazu befähigt werden, selbst zu bestimmen, wer ihre Daten erhält oder einsehen kann. Genauso wichtig ist es aber auch, die entsprechenden Rechte anderer zu respektieren und zu wahren.

Zu den zu vermittelnden Datenschutz-Kenntnissen gehören beispielsweise:

- Wissen um **sichere Passwörter** und **Privatsphäre-Einstellungen**
- bewusster Umgang **mit eigenen und fremden Bildern**
- Wissen über Geschäftsmodelle von Großkonzernen (**Datenhandel**)
- **Folgen von Digitalisierungsprozessen** auf die Gesellschaft (“der gläserne Mensch”) und die Politik (Wahlmanipulation)[1]

DIESE RECHTE GELTEN AUCH IM NETZ

Kinderrechte gemäß UN-Kinderrechtskonvention[2]

Nahezu alle **Rechte des Kindes** werden auch im **digitalen Raum** berührt:

- Zugang zu Medien
- Schutz der Daten und der Privatsphäre
- Schutz vor Gewalt und Ausbeutung
- Meinungs- und Informationsfreiheit
- Vereinigung und friedliche Versammlung
- Teilhabe und Spiel
- Bildung und Medienkompetenz

Altersgrenzen für straf- und zivilrechtliche Haftbarkeit

Laut § 19 Strafgesetzbuch (StGB) werden **Kinder unter 14 Jahren als nicht schuldfähig** angesehen. Davon zu unterscheiden ist die **Deliktsfähigkeit**, also die zivilrechtliche Verantwortung für angerichtete Schäden.[3] Dies geht mit einer Schadensersatzpflicht einher. Unter der Voraussetzung des **Vorsatzes** oder der **Fahrlässigkeit** können Kinder bereits ab dem vollendeten **7. Lebensjahr** deliktfähig sein. So wurde 2015 eine Sechstklässlerin, die einen Mitschüler mobbte, vom Landgericht Memmingen zu 1500 € verurteilt.[4] Im Falle von zivilrechtlichen Schadensersatzansprüchen kann somit bereits in jungen Jahren ein Schuldtitel ausgestellt werden, der bis zu 30 Jahren bestehen bleibt.

Aufsichtspflicht im Netz

Zu den elterlichen Pflichten gehört nicht nur die **Aufsicht**, sondern auch die **Aufklärung im Zusammenhang mit bestimmten Gefahren** sowie **Belehrungen**, bevor sie Kindern digitale und internetfähige Geräte zur Nutzung überlassen.[5] Wenn Eltern dieser Aufsichtspflicht nachgekommen sind, haften sie nicht automatisch für das Handeln der Kinder.[6]

Eltern haben einen **Förderungs- und Erziehungsauftrag** und sollten daher über datenschutzrechtliche Grundlagen informiert sein.[7]

„Spiel, Privatsphäre, Bildung: Kinder haben Rechte, auch im digitalen Raum! Erwachsene müssen Kinder auf ihrem Weg in digitale Welten begleiten und fördern. Entscheidungen im besten Sinne des Kindes zu treffen bedeutet, den Willen des Kindes zu berücksichtigen und gleichzeitig Schutz, Teilhabe und Förderung zu gewährleisten.”

Clara von der Heydt, #Kinderrechte digital leben!, Der Kinderschutzbund LV Thüringen e.V.

[1] vgl. Wawrzyniak 2020
[2] vgl. DKHW 2024
[3] §§ 823 ff. Bürgerliches Gesetzbuch (BGB)
[4] LG Memmingen, Urteil vom 03.02.2015, Az. 21 O 1761/13
[5] vgl. AG Bad Hersfeld Familiengericht, F 120/17 EASO
[6] § 832 BGB Haftungsausschluss
[7] § 1626 Abs. 1 BGB

Aufsicht oder Überwachung?

Trotz Aufsichtspflicht: Im Hinblick auf das **allgemeine Persönlichkeitsrecht** und die Menschenwürde des Kindes verbietet sich in der Regel sowohl die **anlasslose Kontrolle** der privaten Nachrichten über Messengerdienste als auch die anlasslose Überwachung durch GPS-Tracking.

Das bedeutet, dass es zwischen Kontrolle und Überwachung und der wachsenden Selbstständigkeit der Kinder und Jugendlichen ein gesundes Mittelmaß geben muss. Bei konkreten Anhaltspunkten für kritische Situationen sollten Eltern die Geräte der Kinder immer im direkten Austausch kontrollieren, um ihrer elterlichen Sorge nachzukommen.

Tipps für ausgewogene Mediennutzungszeiten

- Festlegung eines Tages- oder Wochenkontingents
- Einschränkung der Nutzungszeiten durch Einstellungen am Router, über Kindersicherungs-Apps oder am Gerät selbst
- Absprache medienfreier Zeiten und Orte
- Vorleben eines ausgewogenen Mediennutzungsverhaltens



DAS KÖNNEN ELTERN PRÄVENTIV TUN

Geschützte Online-Umgebung einrichten

- Nutzung von Messengern, Apps und Spielen unter Beachtung des **Mindestalters**
- Orientierung an den Empfehlungen der USK
- technische Sicherheitseinstellungen vornehmen, wie Drittanbietersperre, Unterbinden von In-App-Käufen, Ad-Blocker, Passwortschutz für das Herunterladen von Apps, Sperre jugendgefährdender Seiten im Browser

Aufklärung von Kindern über die drohenden Gefahren und Konsequenzen durch eigenes strafbares Handeln

- Verletzen von Urheberrechten Dritter
- Verbreitung von beleidigenden oder bedrohenden Inhalten (Cybermobbing)
- Verbreitung von Fake News (z.B. Kettenbriefe)
- Sexting mit Minderjährigen
- Verschicken von pornografischen Inhalten oder verfassungsfeindlichen Stickern/Symbolen
- Verletzung des Rechts am eigenen Bild anderer

Aufklärung von Kindern über die drohenden Gefahren durch Andere

- jugendgefährdende Inhalte
- Kostenfallen durch In-App-Käufe, Abofallen, Fake-Shops, Werbefallen, Trickbetrüger
- Aufklärung zu Geschäftsmodellen von App-Anbietern, Social Media, Sprachassistenten
- Cybergrooming: Cybermobbing, Deep Fake, Identitätsklau

WAS KÖNNEN ELTERN SONST NOCH TUN?

- Informieren über neue Apps, Spiele und technische Entwicklungen
- regelmäßige Gespräche zu Erfahrungen im digitalen Raum führen
- auf Warnzeichen achten
- wiederholtes Thematisieren, wenn das Kind trotz Absprachen/ Sicherheitseinstellungen auf bedenkliche Inhalte stößt oder Kosten entstehen
- Medienkonsum weder als Belohnung, noch als Bestrafung einsetzen
- Regeln und dazugehörige logische Konsequenzen aufstellen

Anregungen, um sich gemeinsam als Familie dem komplexen Thema der Medienerziehung zu nähern, kann ein **Mediennutzungsvertrag** geben.

Differenziert nach Altersgruppen gibt dieser Vorschläge für **Regeln** sowohl **für Eltern** als auch **Kindern** vor und ist individuell anpassbar. Der Mediennutzungsvertrag eignet sich, um sich über die eigenen Vorstellungen und Werte in Bezug auf die gewünschte Mediennutzung in der Familie im Klaren zu werden und gemeinsame Regeln zu finden. Wenn allen Seiten klar ist, was erlaubt ist und was nicht, kann dies unnötige Diskussionen und Streit verhindern.





Mit einem frühzeitig erstellten Mediennutzungsvertrag ist allen Seiten klar, was erlaubt ist und was nicht.

aus dem Flyer zum Mediennutzungsvertrag, **Hg. klicksafe & internet-abc**

LINKTIPPS

Orientierung bei der familiären Medienerziehung

- www.mediennutzungsvertrag.de
- www.klicksafe.de/eltern
- www.internet-abc.de/eltern

Informationsportale zu rechtlichen Grundlagen im digitalen Raum

- https://irights.info/
- www.safe-im-recht.de
- https://kinderrechte-digital-leben.de/

Medienpädagogische Online-Ratgeber für Computerspiele und neue Medien

- https://spieleratgeber-nrw.de/

Schritt-für-Schritt-Anleitungen zum technischen Jugendmedienschutz

- www.medien-kindersicher.de

#DigitaleVorbilder

RECHTE, PFLICHTEN & VERANTWORTUNG IM DIGITALEN RAUM

TIPP: ELTERN-RATGEBER-SEITEN NUTZEN

UN-KINDERRECHTS-KONVENTION

GILT AUCH DIGITAL

3 Rechtskategorien
§ SCHUTZRECHTE
§ TEILHABERECHTE
§ FÖRDERRECHTE

WIR HABEN RECHTE!

EXPERTIN: CLARA VON DER HEYDT

FSK & USK

SPIELE-RATGEBER (PSYCH. EINSCHÄTZUNG)

USK 16

WAS WÜNSCHEN SICH KINDER?

INTERESSE, VERSTÄNDNIS & BEGLEITUNG

?!

click

TIPP: GEMEINSAMER, REGELMÄßIGER TERMIN

1. MAI

GEMEINSAM DIGITALE GERÄTE EINRICHTEN EINSTELLUNGEN VORNEHMEN!

"WIR WOLLEN KEINE WERBUNG!"

MOTZ monster & WUNSCH Einhorn

"Wir wollen mitreden dürfen!"

MODERATION: KATHARINA KRÜGER

IM GESPRÄCH BLEIBEN!

AB 13 Jahren

AB 13 Jahren

AB 13 Jahren

KLICKSAFE.DE SCHAUHIN.INFO

TIPP: MESSENGER ALTERNATIVEN BESPRECHEN

FRÜH DIE ERSTEN SCHRITTE GEMEINSAM GEHEN!

TIPP: FLIMMO.DE PÄDAGOGISCHE EMPFEHLUNGEN FÜR TV&STREAM

medien-nutzungs-vertrag!

ÜBERTRAG

REGELN & KONSEQUENZEN FÜR ELTERN & KINDER?

RECHT AM EIGENEN BILD!

DATENSCHUTZ & PERSÖNLICHKEITSRECHTE ACHTEN!

KLASSENCHATS

ZIVILRECHTLICH STRAFBAR AB 7 JAHREN

STELL EINE FRAGE & ERHALTE EINE PERSÖNLICHE ANTWORT IN MAX 24 STD.!

TIPP: FRAGZEBRA.DE FRAGFINN.DE

KINDER-SUCHMASCHINE

EXPERTIN: ANTJE KAISER

GRAPHIC RECORDING @elibreuing

Über die Moderatorin

Katharina Krüger
Journalistin & Projektmanagerin für die ARD Kinderangebote

Über die Referentinnen

Antje Kaiser
Projektleitung **#DigitaleVorbilder** & Referatsleitung Presse, Kommunikation und Medienbildung beim LfDI MV

↗ datenschutz-mv.de

Clara von der Heydt,
Medienpädagogin Kinder- und Jugendmedien, Projektleitung #Kinderrechte digital leben!, Der Kinderschutzbund Landesverband Thüringen e.V.

↗ kinderrechte-digital-leben.de/das-projekt

KINDERBILDER IM NETZ

PRIVATSPHÄRE FÜR KLEINE PERSÖNLICHKEITEN



Kinderbilder im Netz sind Fotografien oder Videos, die im Internet hochgeladen oder über Messengerdienste geteilt werden. Es liegt in der Verantwortung der Erziehungsberechtigten, die Privatsphäre der Kinder zu schützen sowie deren Persönlichkeitsrecht am eigenen Bild und auf Selbstdarstellung zu wahren.

DARUM IST DAS FÜR FAMILIEN RELEVANT

Kinderbilder auf sozialen Netzwerken sind allgegenwärtig. Nicht nur Kinder und Jugendliche, sondern auch Eltern, Großeltern und Freund:innen verbreiten digitale Fotos und zeigen damit Einblicke in das Privatleben von allen Familienangehörigen. In vielen Familien gehören soziale Netzwerke und mobile Geräte selbstverständlich zur Kommunikation und zum Austausch von Fotos dazu, wie eine Studie des Deutschen Kinderhilfswerks[1] zeigt. Dank der hochwertigen Kameras in Smartphones können sehr schöne, teils professionelle Bilder entstehen. Diese digitalen Bilder lassen sich unkompliziert an weit entfernte Familienmitglieder schicken und erinnern an wichtige Lebensphasen der Kinder.

Es gibt das sogenannte **Phänomen** Sharenting, bei dem Eltern regelmäßig Bilder und persönliche Informationen ihrer Kinder in sozialen Medien und auf digitalen Plattformen teilen (Stichwort: Momfluencer).

DAS HABEN KINDERBILDER IM NETZ MIT DATENSCHUTZ ZU TUN

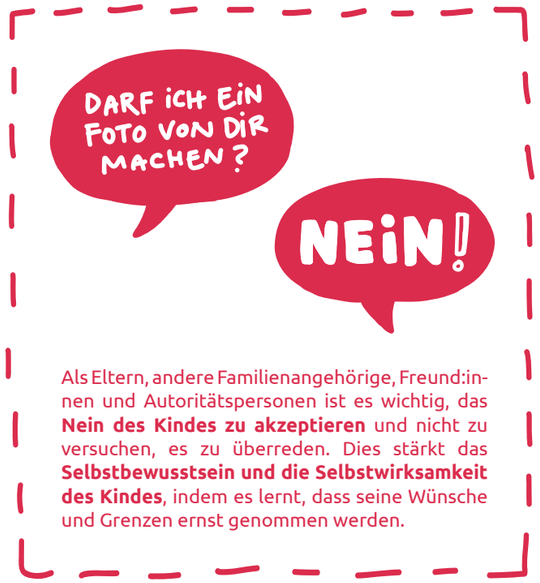
Kinderbilder im Netz können **persönliche und sensible Informationen** preisgeben, welche die **Privatsphäre** der Kinder betreffen. Kinderbilder zeigen nicht nur das Aussehen eines Kindes (biometrische Daten), sondern können auch indirekt Informationen über **Identität, Wohnort, Schule, Interessen und soziale Umgebung** preisgeben. Diese Informationen sind **schützenswerte personenbezogene Daten**. Werden diese von öffentlichen Stellen verwendet, wie bspw. der Kita, der Schule oder einem Verein, müssen diese sich dabei an die Grundsätze der DSGVO halten und bspw. eine Fotoeinwilligung einholen, Eltern jedoch nicht.

Beim Teilen von Kinderbildern im privaten und familiären Kreis findet die DSGVO keine Anwendung. Trotzdem ist das **Recht am eigenen Bild** zu berücksichtigen. Deswegen ist es auch dort wichtig zu hinterfragen, welche Bilder mit wem geteilt werden.

§ KINDER RECHTE

Vorsicht ist geboten beim Teilen von privaten Bildern über einen öffentlichen Social Media-Account. Denn damit werden Kinder- und Familienfotos einem großen Empfängerkreis zur Verfügung gestellt. Wie mit dem heutigen Stand der Technik z.B. mit KI Kinderbilder verändert werden können, zeigt das Video „Nachricht von Ella“[2] sehr anschaulich.

Ende-zu-Ende-verschlüsselte Messengerdienste bieten mehr **Privatsphäre** und **Kontrolle** als soziale Medien. Noch sicherer sind datenschutzkonforme Clouddienste, auf denen einzelne Alben nur einem begrenzten Kreis freigegeben werden können. Generell sollte darauf geachtet werden, dass die benutzten Plattformen und Apps ihren Unternehmenssitz im Geltungsbereich der DSGVO haben und sich somit an bei uns geltendes Datenschutzrecht zu halten haben.



Als Eltern, andere Familienangehörige, Freund:innen und Autoritätspersonen ist es wichtig, das **Nein des Kindes zu akzeptieren** und nicht zu versuchen, es zu überreden. Dies stärkt das **Selbstbewusstsein und die Selbstwirksamkeit des Kindes**, indem es lernt, dass seine Wünsche und Grenzen ernst genommen werden.

[1] vgl. DKHW 2018: 81
[2] vgl. Telekom 2024
[3] vgl. BMFSFJ 2024

DIESE RECHTE GELTEN AUCH IM NETZ

Art. 16 der UN-Kinderrechtskonvention: **Recht auf Privatsphäre**. Kinder haben ein Recht darauf, dass ihre Ehre nicht verletzt wird und nicht ohne Erlaubnis Bilder von ihnen im Internet landen.[3]

Genau wie Erwachsene haben Kinder ein **Recht am eigenen Bild**. Mit zunehmendem Alter entwickeln Kinder ein eigenes Bewusstsein, ob Fotos von ihnen gemacht werden dürfen. Bei der Verbreitung von Kinderbildern müssen sich Eltern grundsätzlich hinterfragen, ob sie es wollen, wenn bestimmte Bilder im Netz landen würden. Dieses Recht ist Teil des **allgemeinen Persönlichkeitsrechts** und im **Kunsturhebergesetz** (KunstUrhG) geregelt. Bei gemeinsamem Sorgerecht sollten beide Elternteile der Veröffentlichung von Fotos des Kindes, wie z.B. Kita-, Schul- oder Urlaubsfotos, gemeinsam zustimmen und eine Regelung treffen, die dem Wohl des Kindes entspricht.

Bei der Veröffentlichung von Bildern haben grundsätzlich die Sorgeberechtigten die Entscheidungsmacht und müssen der Veröffentlichung von Fotos oder Videos zustimmen. Ab etwa 14 Jahren geht das KunstUrhG jedoch von einer sogenannten **Einsichtsfähigkeit** des Jugendlichen aus. Das bedeutet, dass Jugendliche selbst einschätzen können, welche Risiken mit der Veröffentlichung verbunden sind, und daher entscheiden dürfen, ob ein Foto gepostet werden darf. Ein Jugendlicher kann somit einer Veröffentlichung durch Freund:innen zustimmen, auch wenn die Eltern dagegen wären. Umgekehrt gilt dies auch: Wenn die Eltern die Erlaubnis zur Veröffentlichung gegeben haben, das Kind jedoch dagegen ist, zählt der Wunsch des Kindes.

§ RECHT AUF Löschung §

Insgesamt sollten Eltern sich dabei ganz genau überlegen, wo sie die Bilder teilen. Selbst bei einem Status eines Messengerdienstes können beispielsweise Arbeitskolleg:innen die Kinderbilder sehen, wenn man es nicht vorher anders einstellt. Und Eltern sollten sich immer fragen, ob alle Kontakte in ihrem Telefon so einen Status sehen sollten.

DAS KÖNNEN ELTERN PRÄVENTIV TUN

Bevor das Foto gemacht wird

- Kinder / Erziehungsberechtigte fragen, ob ein Foto gemacht werden darf
- Standortfunktion der Kamera-App deaktivieren (oftmals auch Standortangaben in den Metadaten der Fotos)
- Fotografie von Nacktheit und Unterwäsche ist tabu
- Clouddienste auf ihre Sicherheit prüfen
- intime Orte und Situationen nur für private Zwecke fotografieren

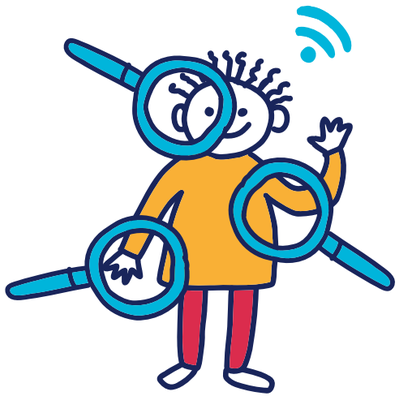
Bevor das Foto im Netz hochgeladen wird

- **Zustimmung des betroffenen Kindes** (bzw. der Erziehungsberechtigten) einholen, ob das Foto gepostet werden darf
- Kinder altersangemessen über **Risiken der Veröffentlichung von Bildern im Internet aufklären**
- **persönliche Daten**, wie Name, Geburtsdatum, Schule oder Wohnort, **vermeiden**
- **Zugriffsrechte** und **Privatsphäreeinstellungen** bei Plattformen überprüfen (auch bei Statusmeldungen)
- Gesicht des Kindes, persönliche Details und identifizierbare Merkmale **nicht veröffentlichen**
- Bilder nur **in vertrauensvollen Gruppen** mit Ende-zu-Ende-Verschlüsselung teilen
- ggf. Funktionen zum automatischen Löschen der Bilder nach dem Ansehen verwenden

NOTFALLTIPPS

Wenn Bilder von Kindern ohne Erlaubnis im Internet auftauchen, können Eltern Folgendes tun:

- Person oder Website kontaktieren und um **Entfernung der Bilder** bitten
- **Meldefunktion von Plattformen nutzen** und Bilder als unangemessen kennzeichnen
- bei unkooperativen Websites oder schwerwiegenden Verstößen juristische Schritte einleiten (zivilrechtlich)
- wenn im Geltungsbereich der DSGVO (z.B. Vereine) sich an die **Datenschutzaufsichtsbehörde** wenden



„Privatsphäre ist nicht nur ein Bild. Ich weiß von vielen Family-Influencerkindern viel mehr, als von den Kindern meiner besten Freunde: wann sie aufwachen, wann sie genervt sind, was sie zum Geburtstag bekommen, was ihre Sorgen sind usw.“

Sara Flieder, Kinderrechtsaktivistin

WUSSTEST DU, DASS ...?

... es nicht reicht, ein Smiley über das Gesicht eines Kindes zu legen? Orte und/oder Merkmale wie Kleidung lassen sich meist trotzdem erkennen. Das Foto ist zudem auf dem Server der Plattform-Betreiber und kann bspw. bei Cyberangriffen **geleaked** werden. Darüber hinaus gibt es Bildbearbeitungssoftware, die Smileys wieder entfernen kann.

... du auch **Großeltern** über **Datenschutzrisiken aufklären** solltest? Viele nutzen Smartphones oder Tablets, sind jedoch ohne Internet aufgewachsen und sich der Gefahren nicht bewusst.





LINKTIPPS

Mehr Tipps für Eltern zum Thema Kinderbilder im Netz

↗ www.schau-hin.info/sicherheit-risiken/kinderfotos-im-netz-darauf-sollten-eltern-achten

Studie vom Deutschen Kinderhilfswerk
„Kinder. Bilder. Rechte. Persönlichkeitsrechte von Kindern im Kontext der digitalen Mediennutzung in der Familie”

↗ www.dkhw.de/filestorage/1_Informieren/1.1_Unsere_Themen/Kinder_und_Medien/Studien/DKHW_Schriftenreihe_4_Kinder-BilderRechte.pdf

#Digitale Vorbilder

KINDERBILDER IM NETZ

PRIVATSPHÄRE FÜR KLEINE PERSÖNLICHKEITEN

TIPP: EIGENE WERTEHALTUNG MIT KINDERN KOMMUNIZIEREN!

DATEN LÖSCHEN?

ACHTUNG: ZWEITVERWERTUNGSRECHTE DER ANBIETER

RISIKO SOCIAL MEDIA DER ZUGRIFF AUF MEDIEN IST MÖGLICH

TIPP: MÖGLICHST FRÜH MIT KINDERN INS GESPRÄCH KOMMEN!

AB DEM KINDERGARTEN VON ANFANG AN!

ACHTET DIE PERSÖNLICHKEITSRECHTE EURER KINDER!

WENIGER IST MEHR!

click

EXPERTIN: SOPHIE POHLE

TIPP: STICKER NICHT ERST IN DER APP HINZUFÜGEN!

ERSTE LIEBE & PORNOGRAFIE ÜBER WHATSAPP

MODERATION: NICOLE AHLES

DAS INTERNET VERGISST NICHT!

DIGITALER STECKBRIEF

- FOTOS / GESICHTER
- PRIVATE INFOS
- HOBBIES & VORLIEBEN

EINVERSTÄNDNISERKLÄRUNG

SICHER SURFEN

KINDERWEBSITES+ SUCHMASCHINEN

ELTERN MEDIEN LOTS:INNEN (FÜR MEDIENPÄDAGOGISCHE ELTERNABENDE)

SAMMLUNGEN VON KINDERBILDERN AUF DEM PC FREMDER? NEIN DANKE!

ELTERNRATGEBER

[!]SCHAU HIN

TIPP: WAS FÄND ICH SELBST NICHT SCHÖN & WÜRDE ES ÜBER MICH NICHT PREISGEBEN?

JUGENDLICHE HELFEN JUGENDLICHEN

juuuport.de
- ANONYM
- KOSTENFREI
- GLEICHALTRIGE

CHATANFRAGE

Hi! ICH HAB DICH HEUTE OO GESEHEN!

WIR SIND JA QUASI NACHBARINNEN

EXPERTE: WIRO NESTLER

KINDER RECHTE

- RECHT AM EIGENEN BILD
- AB DEM 8. LEBENSJAHR MÜSSEN KINDER EINBEZOGEN WERDEN
- AB 14 JAHREN AKTIVE EINWILLIGUNG

SCHAM

Mama, Papa, das ist mir peinlich!

EXPERTIN: SARA FLIEDER

SHARENTING

Meine ELTERN = MEIN ARBEITGEBER

INFLUENCER KIDS

TIPP: KINDER SENSIBILISIEREN! FRAGEN, BEVOR MAN EIN FOTO MACHT.

ZIELE
- UN KINDERRECHTSKONVENTION INS GESETZ!
- MEDIENKOMPETENZ VON LEHRPERSONAL & ELTERN FÖRDERN!

Medienerziehung

GRAPHIC RECORDING @elibrewing

Über die Moderatorin

Nicole Ahles
Moderatorin & Journalistin

Über die Referent:innen

Wiro Nestler
LKA Hamburg
polizei.hamburg.de

Sara Flieder
Kinderrechtsaktivistin

Sophie Pohle
Referentin der Koordinierungsstelle Kinderrechte des Deutschen Kinderhilfswerkes
dkhw.de

TikTok, Instagram, Snapchat & Co



Soziale Netzwerke sind Internetdienste, die es ermöglichen, mit Freund:innen, Bekannten oder auch Fremden in Kontakt zu treten, sich auszutauschen, aber auch sich selbst zu inszenieren und Informationen zu teilen. Je nach Netzwerk treffen die Nutzenden auf unterschiedliche Altersgruppen. Während Facebook bei den über 30-Jährigen seit vielen Jahren der beliebteste Dienst ist, sind jüngere Menschen eher bei Instagram, Snapchat und TikTok anzutreffen.[1]

DARUM IST DAS FÜR FAMILIEN RELEVANT

Von den durchschnittlich 224 Minuten täglicher Onlinezeit verbringen Jugendliche besonders viel Zeit auf Social Media. So wird Instagram von 62 % der 12 - 19-Jährigen regelmäßig genutzt, 59 % nutzen TikTok und 49 % sind bei Snapchat aktiv.[2]

Warum sind diese Social Media-Angebote bei Jugendlichen so beliebt?

Die unterschiedlichen Social Media-Plattformen bieten Jugendlichen vielfältige Angebote und gehen damit auf spezielle Bedürfnisse und Entwicklungsphasen ein.

Dazu zählen nach Havighurst[3] die Entwicklung:

- von Autonomie durch die Ablösung von den Eltern
- der eigenen (sexuellen) Identität
- eines Moral- und Wertesystems
- einer Zukunftsperspektive

Social Media hat einen hohen Unterhaltungswert, denn Algorithmen zeigen spannende Informationen im persönlichen Feed des Nutzenden, die an die Interessen und Vorlieben angepasst sind. Gleichzeitig ermöglicht Social Media den **Erfahrungsaustausch** unter Gleichgesinnten weltweit (**Selbsthilfe**) und trägt auch zur **Meinungsbildung und Interessensentwicklung** bei.

Ein eigenes Social Media-Profil bietet Jugendlichen die Möglichkeit der **positiven Selbstdarstellung.** Egal ob Alltagssituationen, Tanz, Karaoke, Let's Plays, Pranks oder Duette: Durch intuitiv bedienbare, professionelle Tools für Schnitt-, Sound- und Filtereffekte war es noch nie so einfach, selbst kreativ zu werden. Der entstandene Content wird genauso schnell geteilt. Dies fördert zum einen die **Selbstwirksamkeit** und kann, bestärkt durch Likes und positive Kommentare, ebenso zur **Steigerung des Selbstwerts** beitragen. Nicht zuletzt animieren soziale Netzwerke dazu, sich in Challenges gegenseitig herauszufordern und an seine Grenzen zu gehen.

ALLGEMEINE RISIKEN SOZIALER PLATTFORMEN

Den positiven Aspekten von sozialen Medien stehen ebenfalls Risiken gegenüber, derer sich Eltern und Jugendliche bewusst sein sollten:

- **Gefahr** von Mediensucht
- Verringerung der Aufmerksamkeitsspanne durch Gewöhnung an kurze Clipdauer
- **Vereinsamung** in der „realen" Welt
- **psychische Probleme** und Schlafstörungen durch nicht kindgerechte Inhalte und fehlende Alterskontrolle (Gewalt, extreme politische Ansichten, Pornografie)
- (lebens-)gefährliche Challenges und Pranks
- **sozialer Druck** durch das Anstreben von Likes, Flammen, Feedback auf gepostete Sachen
- **FOMO** (engl. Fear of missing out): die Angst, etwas zu verpassen, verstärkt durch Push-Nachrichten
- Bevorzugung sexualisierter, freizügiger Darstellungen sowie Inszenierung stereotyper Rollenbilder durch die Communitiy (mehr Likes/Reichweite)
- Einblicke in höchst private Räume, wie Kinderzimmer
- unüberschaubare Reichweite bei öffentlichen Profilen
- einfache Verbreitung von Fake News
- **Fake-Profile**



[1] vgl. Statista 2024
[2] vgl. JIM 2023
[3] vgl. Havighurst 1953



- **Kostenfalle** durch virtuelle Geschenke im Livestream (z.B. bei TikTok)
- **Abgabe von Rechten** an hochgeladenen Bildern und Videos an die Plattformbetreiber
- Möglichkeit, sich selbst rechtswidrig zu verhalten durch die **Verletzung von Urheberrechten**, **Rechten am eigenen Bild** und anderen Persönlichkeitsrechten

Auch Jugendliche, die sich mit Smartphones, Sozialen Netzwerken und Apps gut auskennen, können die damit verbundenen Risiken nicht zwangsläufig richtig einschätzen und benötigen Unterstützung bei der Einordnung und Verarbeitung des Gesehenen.

DAS HABEN SOZIALE PLATTFORMEN MIT DATENSCHUTZ ZU TUN

Soziale Netzwerke zielen darauf ab, sich mit möglichst vielen Personen zu verbinden oder besonders viel Aufmerksamkeit von anderen Nutzenden zu erhalten. Dies ist mit dem Grundgedanken des Datenschutzes, die Kontrolle über die eigenen Daten nicht aus der Hand zu geben, nur schwer in Einklang zu bringen.

Wer soziale Netzwerke nutzt, sollte sich bewusst sein, dass die Verpflichtung zu datenschutzfreundlichen Voreinstellungen (Privacy by default) von den meisten sozialen Plattformen nur ungenügend umgesetzt wird. Oftmals gibt man die Rechte an hochgeladenen Inhalten (auch auf privaten Profilen) an die Plattformbetreiber ab. Erziehungsberechtigte tragen dabei Sorgepflicht für die Persönlichkeitsrechte ihrer minderjährigen Kinder.

Vor allem öffentliche Profile bergen die Gefahr, dass sich gepostete Inhalte unkontrolliert im Netz verbreiten. Diese Profile sind durch Suchmaschinen auch für Menschen auffindbar, die keinen Social Media-Account besitzen. **Was einmal im Netz ist, bleibt auch da!** Selbst wenn Stories oder Nachrichten nach einer bestimmten Zeitspanne automatisch verschwinden, können diese Beiträge durch Screenshots gesichert und weiterverbreitet werden.

Die Anbieter von sozialen Netzwerken verdienen mit den angegebenen Daten ihr Geld. Die **kostenlose Nutzung wird mit der Preisgabe der eigenen Daten bezahlt**. Dafür wird oft der Satz verwendet: “Wenn du nicht für ein Produkt zahlst, bist du das Produkt.”

Diese Daten werden genutzt, um ein **individuelles Nutzerprofil** anzulegen und möglichst effektiv Werbung und Inhalte ausspielen zu können. Personalisierte Inhalte lassen Nutzende länger auf Seiten verweilen.

Aber auch die Daten persönlicher Kontakte werden oft ungefragt abgegriffen.

Um Nutzenden Freund:innen und Familie vorschlagen zu können, werden die Kontakte im eigenen Telefonbuch automatisiert ausgelesen. Dies kann unterbunden werden, indem Nutzende dies proaktiv in den Einstellungen ablehnen.

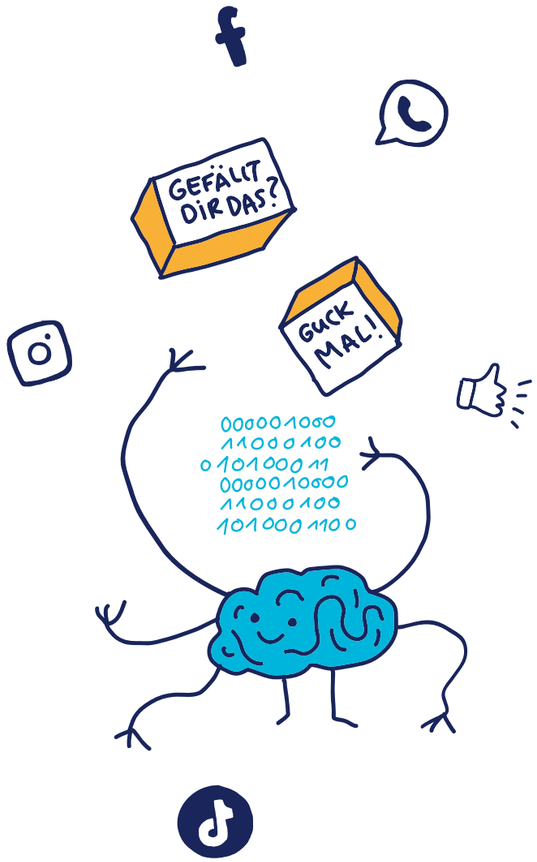
„Der Algorithmus von TikTok funktioniert besonders gut, in dem er uns zielgerichtet Sachen anzeigt, die wir interessant finden. Wir bekommen das Gefühl, dass er uns besser kennt, als wir uns selber. Das kann dazu führen, dass wir dort mehr Zeit verbringen, als wir es eigentlich vorhatten.“

Martin Bregenzer

DAS KÖNNEN ELTERN PRÄVENTIV TUN

Um die Nutzung von Social Media möglichst sicher zu machen, gibt es verschiedene Einstellungsmöglichkeiten:

- Konto auf privat stellen (trotzdem können Profilbild, Name und ggf. optionale Profilinformation, Bio, für alle Nutzenden sichtbar sein)
- sich informieren, wo Beiträge, Kommentare, Direktnachrichten (DN) und Benutzer:innen gemeldet und blockiert werden können (alles, was gegen die Community-Richtlinien verstößt)
- gemeinsam mit dem Kind Community-Richtlinien lesen
- Benutzerkreis einschränken, der per Direktnachricht Kontakt aufnehmen kann
- Kommentarfunktion deaktivieren, filtern, verbergen
- Likes, Views einschränken
- Überprüfen, wer das Profil erwähnen darf
- Einstellungen für Stories verwalten: sehen, antworten, teilen nur für enge Freunde
- Bildschirmzeit: Zeitlimits festlegen, an Pausen erinnern, Push- oder Email-Benachrichtigungen über Aktivitäten deaktivieren
- eingeschränkten Modus für jüngere Kinder einrichten, um bedenkliche Inhalte auszublenden
- ggf. den Elternmodus / Supervision / Family Center nutzen
- Standortfreigabe deaktivieren



LINKTIPPS

Flyer von Klicksafe zu verschiedenen Social Media Plattformen

↗ www.klicksafe.de/materialien/

Informationen zu diversen Sozialen Netzwerken von SchauHin!

↗ www.schau-hin.info/soziale-netzwerke

Anleitungen zum datenschutzfreundlichen Gebrauch verschiedener Social Media-Plattformen

↗ www.internetmatters.org/de/resources/social-media-advice-hub/



Über die Moderatorin

Katharina Krüger
Journalistin & Projektmanagerin für die ARD Kinderangebote

Über die Referenten

Martin Bregenzer
Referent für Medienkompetenz bei der EU-Initiative klicksafe, Medienanstalt Rheinland-Pfalz

↗ www.klicksafe.de

Dr. Phil. Detlef Scholz,
Erziehungswissenschaftler, Systemischer Therapeut (SG), Medienpädagoge, Psychologischer Berater; Leiter des Kompetenzzentrums und Beratungsstelle für exzessiven Mediengebrauch und Medienabhängigkeit

↗ www.suchthilfe-mv.de/kompetenzzentrum-fuer-medienabhaengigkeit.html

MEDIENNUTZUNG
IN DER FAMILIE



Mediennutzung in der Familie bezieht sich auf die Art und Weise, wie Familienmitglieder digitale Medien konsumieren und nutzen. Dies umfasst eine Vielzahl von Aktivitäten, bei denen Technologien und Medien in den Alltag der Familie integriert sind. Dazu gehören sowohl die individuelle Nutzung durch einzelne Familienmitglieder als auch gemeinsame Aktivitäten, die mit Medien verbunden sind.

Dabei ist es von großer Bedeutung, dass für alle Familienmitglieder ein kritischer und reflektierter Umgang mit den Daten und Informationen im Netz die Grundlage bildet.

DARUM IST DAS FÜR FAMILIEN RELEVANT

In den meisten Familien findet sich eine bunte Vielfalt an technischer Ausstattung und medialen Nutzungsgewohnheiten.

Die Ausstattung mit den neuesten technischen Geräten und Anwendungen, häufig versehen mit **smarten Geräten**, wie Sprachassistenten, ist in vielen Haushalten bereits Standard. Von der Bedienung des Lichtschalters, der Kaffeemaschine, des Türöffners bis zum Saugroboter wird vieles **automatisiert (fern-)gesteuert**.

Auch für die **Organisation des Familienlebens** u.a. durch geteilte Kalender, Einkaufslisten oder den **Austausch** mit den Verwandten **über Ländergrenzen** hinweg sind die Vorzüge des Internets unstrittig. Verstärkt wird dies zum Beispiel **durch digitale Spiele**, **Erleichterung beim Lernen** in Schule und Studium durch KI, Lern Apps oder **Inspiration durch Influencer:innen** in den sozialen Medien.

Die KIM-Studie 2022 zeigt, dass immer mehr Kinder digitale Medien selbstständig und ohne Begleitung von Erwachsenen nutzen. 48 % der befragten Eltern von Kindern im Alter von 6 bis 12 Jahren gaben dies an. Während mit zunehmendem Alter immer mehr Kinder online sind, werden technische Möglichkeiten und Dienstleistungen zum Schutz vor ungeeigneten Inhalten im Netz nur von einem Drittel der Eltern verwendet. Dies ist ein erstaunliches Ergebnis vor dem Hintergrund, dass 80 % der Erziehungsberechtigten durchaus die Gefahren für Kinder im Netz sehen.[1]

DAS HAT MEDIENNUTZUNG IN DER FAMILIE MIT DATENSCHUTZ ZU TUN

Datenschutz in der Familie ist ein entscheidender Aspekt der Mediennutzung, der proaktives Handeln von Eltern erfordert, um die **Privatsphäre und Sicherheit** aller Familienmitglieder im **digitalen Raum** zu gewährleisten. Alle erwachsenen Familienmitglieder sind aufgefordert, als Vorbild zu zeigen, wie **Datenschutz** gut umgesetzt wird, und warum er so wichtig ist. Sie übernehmen die Verantwortung dafür, welchen **digitalen Fußabdruck** Kinder bereits in jungen Jahren im Netz hinterlassen.

Dabei sollten Eltern darauf achten, dass die von der Familie genutzten Geräte sicher sind, bspw. durch regelmäßige Updates, Firewalls und sichere Passwörter.

Während elterliche Kontrolle wichtig ist, müssen Eltern auch das **Recht ihrer Kinder auf Privatsphäre** respektieren und sensibel mit deren Daten umgehen.



[1] vgl. KIM 2022
[2] ebd.



„Es kann vorkommen, dass Kinder eine Art eifersüchtiges Verhalten entwickeln oder digitale Geräte als Konkurrenz sehen, wenn Eltern zu viel Zeit damit verbringen. Es ist wichtig, dass Eltern digitale Geräte bewusst weglegen, um Zeit mit dem Kind zu verbringen, sonst leidet die Bindung darunter.“[2]

DIESE RECHTE GELTEN AUCH IM NETZ

Für dieses Kapitel ist besonders das **Kinderrecht auf eine Familie, elterliche Fürsorge und ein sicheres Zuhause** relevant. Denn daraus lässt sich der Anspruch ableiten, dass Eltern ihre Kinder in der Medienwelt begleiten und vor ungeeigneten Inhalten oder Kontakten schützen müssen, beispielsweise durch entsprechende Sicherheitseinstellungen. Dazu zählt aber auch die reflektierte und sichere Nutzung von smarten Technologien zu Hause.

"**Medienerziehung** bedeutet, den Kindern beim **Aufbau von Medienkompetenz** sowie bei der **Verarbeitung ihrer Medienerlebnisse** unterstützend zur Seite zu stehen."[1]

„Eltern haben die Aufgabe, ihren Kindern bei der **Auswahl von Medien** Orientierung zu geben und sie ebenso während der Nutzung zu unterstützen. Schließlich sind sie es, die den Kindern den Zugang zu bestimmten Medienangeboten ermöglichen oder verbieten (können). Dabei müssen auch die Wünsche und Bedürfnisse der Kinder Beachtung finden."[2]

Tipp: Es ist sinnvoll, sich in regelmäßigen Abständen mit Suchmaschinen und in sozialen Medien selbst zu suchen, um zu schauen, wie es um den eigenen Ruf im Internet bestellt ist. Befinden sich falsche Informationen über die eigene Person im Umlauf? Sind persönliche Informationen ohne die wissentliche Zustimmung veröffentlich worden? Wenn ja, gilt es, dem durch proaktive Maßnahmen entgegenzutreten und die Löschung von falschen oder ggf. unrechtmäßig veröffentlichten Informationen bei den Verantwortlichen zu verlangen.

DAS KÖNNEN ELTERN PRÄVENTIV TUN

Eine eigene Haltung zu digitalen Medien entwickeln

- **Handlungs- und Entscheidungsgrundlage in der Medienerziehung** sollte ein Zusammenspiel aus Werten, Zielen, Überzeugungen, Erfahrungen und Erkenntnissen sein
- Herausforderung der heutigen Elterngeneration, Technologien und sicheren Umgang mit digitalen Medien selbst erst kennenlernen
- entspannter Umgang und eine **offene Grundhaltung** sowie **Vertrauen** in das Lernen der Kinder durch eigene Erfahrungen (positive wie negative)
- **Chancen statt primär Risiken** zu sehen
- **konstruktives Gespräch**, als Basis für eine begleitende und wertschätzende Medienerziehung[3]

Vorbild sein

- im Umgang mit (Kinder)Fotos, beim Erstellen und Teilen
- mit der eigenen digitalen Balance im Privatleben, insbesondere während der Eltern-Kind-Zeit
- im Homeoffice/ als Selbstständige:r vor dem Kind Prioritäten setzen in der eigenen Aufmerksamkeit
- im Umgang mit der eigenen Privatsphäre: Wie viel gebe ich auf sozialen Netzwerken/im Netz von mir preis?
- Wie oft wähle ich in der Cookie-Abfrage "Alle erlauben" statt "nur die technisch erforderlichen Cookies"?
- Wie unbedarft gebe ich meine Kontaktdaten für Gewinnspiele raus oder erlaube es Anbietern von Bonusprogrammen, wie z.B. Punkte sammeln, Apps von Supermarkt- oder Drogerieketten, Daten von mir zu sammeln, um daraus Nutzungs-, Gesundheits-, Kauf- oder Bewegungsprofile zu erstellen?
- Nehme ich mir die Zeit, AGB zu lesen, um mich über App-Berechtigungen zu informieren?
- Lege ich Wert auf Datenschutzeinstellungen an meinen Endgeräten?

Aufklären und Regeln aufstellen

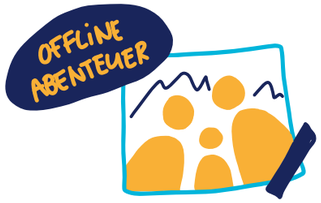
- **Medienführerschein** für das Kind als Voraussetzung für ein eigenes Smartphone
- Kinder brauchen auch im Netz Regeln und Grenzen
- gemeinsame Vereinbarung eines **Mediennutzungsvertrages**
- im Gespräch altersangemessene **Gefahren** und **Lösungsstrategien thematisieren** sowie **Anlaufstellen** aufzeigen
- zur **konsequenten Umsetzung** vereinbarter **Mediennutzungsregeln, technische Schutzmaßnahmen** nutzen

Sich als Vertrauensperson etablieren

- **Interesse** an den Sorgen und Bedürfnissen des Kindes **zeigen**
- sich die **Faszination von Online-Games erklären lassen** und selber mitspielen
- nicht mit Medienentzug strafen

Alternativen zur digitalen Mediennutzung aufzeigen

- **Abenteuer außerhalb der digitalen Welt zeigen**: z. B. im Wald, beim Wandern oder Baden, Rollenspiel mit Verkleiden, Geo Caching usw.
- **Lust machen auf analoge Medien**, wie Bücher oder Brettspiele
- "**Bibliothek der Dinge**" erkunden



"Wenn wir mehr mit unseren Kindern spielen würden, wären vielleicht digitale Spiele gar nicht so wichtig!"

Thomas Feibel, Gründer des TOMMI-Softwarepreis

[1] Medienkindergarten, Wien
[2] Wiener Bildungsserver 2024
[3] vgl. PROJUVENTUTE 2024

LINKTIPPS

24 Ideen, wie dein Kind freiwillig vom Bildschirm wegkommt

↗ https://medienmentorin.de/blog/portfolio/kleine-sendepause/

Medien-Führerschein für Kinder

↗ https://www.internet-abc.de/surfschein/

Familien-Checkliste zum Datenschutz

↗ www.klicksafe.de/materialien/so-sind-eure-daten-besser-geschuetzt

Kinder sicher im Netz begleiten – Leitfaden für Eltern

↗ https://www.klicksafe.de/materialien/internetkompetenz-fuer-eltern-kinder-sicher-im-netz-begleiten

#Digitale Vorbilder
MEDIENNUTZUNG
IN DER FAMILIE



























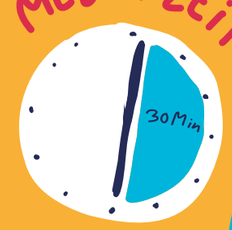




























GRAPHIC RECORDING @elibrewing

Über die Moderatorin

Katharina Krüger
Journalistin & Projektmanagerin für die ARD Kinderangebote

Über die Referent:innen

Thomas Feibel
Journalist, Leiter Büro für Kindermedien, Organisator & Gründer Dt. Kindersoftwarepreis TOMMI, Autor von Medienerziehungsratgebern & Kinder-/Jugendbüchern über Aufwachsen in der digitalen Welt. Referent
↗ https://feibel.de/

Katherine Zimmermann
Medienpädagogin & Kinder- und Jugendmedienautorin
↗ https://medienmentorin.de/

GAMING

SPIELEND SICHER!

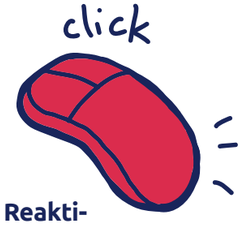


Mit Gaming ist das Spielen von digitalen Spielen auf elektronischen Geräten, wie der Spielkonsole, dem Rechner, dem Notebook, dem Tablet oder dem Smartphone, allein oder mit anderen, gemeint. Digitale Spiele können in verschiedene Genres unterteilt werden, die sich vor allem in ihren Spielmechaniken unterscheiden. Dabei handelt es sich entweder um abstrakte Vorgänge und Aufgaben, Nachahmungen von konventionellen Spielen und Sportarten oder Anwendungen mit virtueller Realität. Dies verlangt den Spielenden Ausdauer, Geschicklichkeit, Schnelligkeit, Taktik oder Raffinesse ab.

DARUM IST DAS FÜR FAMILIEN RELEVANT

Digitale Spiele sind aus vielen Haushalten nicht mehr wegzudenken. Insgesamt spielen 72 % der Jugendlichen regelmäßig. Das ist unabhängig davon, ob sie am **Computer, der Konsole, dem Tablet oder dem Smartphone** spielen. Dabei unterscheiden sich die Nutzungsgewohnheiten zwischen den Geschlechtern. Jungs sind mit 119 min/Tag doppelt so aktiv wie Mädchen mit nur 61 min/Tag. Zu den Favoriten der Jungen gehören „Minecraft“, „FIFA“, „Fortnite“ und „GTA – Grand Theft Auto“. Mädchen hingegen zählen „Die Sims“, „Hay Day“, „Mario Kart“, „Candy Crush“, „Roblox“, „Subway Surfer“, „Super Mario“ und „Hogwarts Legacy“ zu ihren liebsten Spielen.[1]

Es gibt viele **positive Aspekte**, warum digitale Spiele für Kinder und Jugendliche empfehlenswert sind:



- Förderung von Fähigkeiten, wie **Reaktionsgeschwindigkeit, Hand-Auge-Koordination, visuelle Aufmerksamkeit** sowie **logisches, räumliches Denken**
- Förderung von **Kreativität**
- durch knifflige Aufgaben **Motivation** schwierige Situationen zu meistern
- Steigerung des **Durchhaltevermögens**
- Förderung von historisch-politischer **Bildung**
- Entstehen und Pflege von **Freundschaften** durch Chats oder das gemeinsame Spiel
- Vertiefung von Fremdsprachenkenntnissen





Es gibt aber auch **negative Aspekte**, die Schaden beim Kind anrichten können:

- durch **übermäßiges Spielen** Probleme, wie **Schlafmangel, Konzentrationsschwierigkeiten und Vernachlässigung anderer Aktivitäten**
- mögliche Zunahme von **aggressiven Verhaltensweisen**
- gesundheitliche Probleme durch **Bewegungsmangel und Sitzhaltung**
- Unterwanderung von Spiele(chats) durch **Extremisten**, die diese für ihre Propaganda nutzen
- Unterwanderung durch Erwachsene zur Anbahnung sexueller Kontakte mit Kindern und Jugendlichen (Cybergrooming)

Für Eltern gilt es daher, Vor- und Nachteile abzuwägen und einen Blick darauf zu haben, welche digitalen Spiele das Kind aktuell spielt und notfalls einzugreifen, wenn Überforderungen oder Gefahren lauern.

„Verwende einen Nickname, der keine Rückschlüsse auf das Alter, Geschlecht oder den Wohnort zulässt.“

Thomas Freitag, Landeskriminalamt M-V



[1] vgl. JIM 2023
[2] vgl. BSI 2024: Gaming
[3] ebd.
[4] vgl. EVZ 2021





DAS HABEN GAMES MIT DATENSCHUTZ ZU TUN

Um Hard- und Software kaufen, Spiele herunterladen, Updates installieren und online gegeneinander antreten zu können, benötigt es einen Account. In diesem werden die **Kontaktdaten, E-Mail-Adresse, Passwörter, Sicherheitsfragen, Geburtsdatum, Kreditkartendaten, die Kontoverbindung** sowie die eingekauften Spiele hinterlegt.[2]

Darüber hinaus sammeln Spielebetreiber und Plattformen biometrische Daten, Informationen über das individuelle Spielverhalten und über Interaktionen mit anderen Spielenden. Diese Daten werden verwendet, um das **Spielerlebnis zu personalisieren**, um ein **Nutzerprofil zu erstellen** und um **personalisierte Werbung** anzeigen zu können.

Seit dem Aufkommen von Augmented Reality-Technologien werden auch die **Geolokalisierungsdaten** der Spielenden gespeichert. Anhand dieser kann sowohl der Standort der Spielenden bestimmt werden als auch die Zeit und sogar die Anzahl an Kalorien, die Benutzer:innen während einer Spielsitzung verbrauchen. “Insgesamt betrachtet, können diese Geolokalisierungsdaten ein genaues Bild der täglichen Routinen eines Spielers erzeugen, etwa seiner Privatadresse, seines Arbeitsplatzes und anderer Freizeit-Hotspots”.[3]

In Europa auf dem Markt befindliche Spiele und Plattformen müssen sich dabei an die Vorgaben und Grundsätze der **DSGVO** halten. Laut dieser haben Spielende ein Recht darauf zu wissen, was mit ihren **personenbezogenen Daten** passiert. Der Verarbeitung und Weitergabe ihrer Daten müssen sie entweder durch den Abschluss eines **Kaufvertrages** und/oder einer **expliziten Einwilligung** zugestimmt haben.

Insbesondere bei Anbietern von Spielen und Plattformen außerhalb des Geltungsbereiches der **DSGVO** kann nicht mit absoluter Sicherheit gesagt werden, welche Daten tatsächlich erfasst, gespeichert und weiterverarbeitet werden.[4]

DIESE RECHTE GELTEN AUCH IM NETZ

Durch das **Jugendschutzgesetz** (JuSchG) ist geregelt, dass Computer- und Videospiele auf Trägermedien nur nach Prüfung und Freigabe durch die Unterhaltungssoftware Selbstkontrolle (USK) an Kinder und Jugendliche verkauft werden dürfen. Die jeweiligen Altersstufen sind 0, 6, 12, 16 und 18 Jahre. Spiele, die nicht bei der USK zur Prüfung vorgelegt wurden oder die von der USK kein Alterskennzeichen erhalten haben, dürfen nur an Erwachsene abgegeben werden. Es handelt sich bei den Altersstufen jedoch nicht um eine pädagogische Eignungsempfehlung.

Der **Jugendmedienschutz-Staatsvertrag** (JMStV) zwischen allen deutschen Bundesländern regelt den Jugendmedienschutz im Bereich des Rundfunks und der Telemedien (im Internet abrufbare Onlineangebote). Im Gegensatz zum JuSchG sieht der JMStV keine stufenweise Alterskennzeichnung vor. Trotzdem muss durch eine Beschränkung der Sendezeit oder durch technische Maßnahmen sichergestellt werden, dass entwicklungsbeeinträchtigende Angebote von Kindern der betroffenen Altersgruppe nicht wahrgenommen werden können.[1] Aus diesem Grund kann man bei Streaming- und Videoplattformen Alterseinstellungen finden.



[1] vgl. game 2024
[2] vgl. BzGA 2024: Kostenfallen

DAS KÖNNEN ELTERN PRÄVENTIV TUN

Auf die Sicherheit achten

- **Elternkontrollen und Sicherheitsfunktionen** auf den Geräten aktivieren, um den Zugang zu kostenpflichtigen und jugendgefährdenden Inhalten zu beschränken
- **Datenschutzeinstellungen** innerhalb der Spiele und auf den Plattformen überprüfen
- Möglichkeit zur **Kontaktaufnahme mit Fremden** im Chat **deaktivieren**
- keinen Klarnamen sondern einen Nickname benutzen, der keine Rückschlüsse auf Alter, Geschlecht, Wohnort zulässt
- **Altersfreigaben und Inhaltsbeschränkungen** beachten (Kind über die Notwendigkeit dieser Schutzeinstellungen aufklären, diese kann durch eine fehlende Altersprüfung durch den Anbieter leicht umgangen werden)
- **Programme zur Kindersicherung und Schutzsoftware** nutzen

Eltern-Kind-Gespräche zur Nutzung von Online-Games

- **Account gemeinsam anlegen**
- abwägen, welche persönlichen Angaben und App-Berechtigungen notwendig sind
- sich **über Spiele informieren (Inhalte,** Sicherheitsfeatures **verstehen)**
- klare **Regeln für die Spielzeit** aufstellen (technische Kontrolle durch Einstellungen in der App)
- **Aufklärung über** mögliche **Gefahren**, wie personalisierte Werbung, unangemessene Inhalte, Missbrauch von persönlichen Daten, Cybergrooming
- **Kostenfallen** thematisieren

Kostenfallen kennen

- vermehrte Einkäufe durch **Lootboxen, zusätzliche** Skins & Outfits
- Gefahr von Abo-Fallen
- teure **Spielerweiterungen auf Internet-Märkten**[2]
- **Play to earn** (engl. Spielen, um zu verdienen) verspricht Kindern, während des Spielens Geld zu verdienen, ist oftmals aber mit einem hohen Startkapital verbunden.

Kostenfallen vermeiden und Handlungstipps für Notfälle

- **Einschränkung** und Deaktivierung **von Zahlungsmethoden** und In-App-Käufen auf den Geräten des Kindes (passwortgeschützt)
- Angabe von **Kreditkartendaten** oder **Bankkonten vermeiden**
- **Bezahlung über Aufladekarten**, wie paysafe, google play/apple cards (Vereinbarung fester Beträge)
- **Kontrolle der Kaufhistorie** auf den Geräten des Kindes (Identifizierung von ungewollten oder unerlaubten Käufen)
- **Kundenservice** der entsprechenden Plattform oder des Spieleentwicklers **kontaktieren** für Rückerstattungen unautorisierter Käufe

***Tipp für Eltern:**
Aufpassen bei Lootboxen!

In manchen Spielen und besonders bei kostenlosen Spiele-Apps finden sich Lootboxen. Lootboxen, abgeleitet vom englischen „to loot" (einsammeln), versprechen nützliche Inhalte, wie Waffen, Ausrüstung oder Geldeinheiten für das Weiterkommen im Spiel. Die Inhalte kommen per Zufallsprinzip und sollen anregen, weitere Lootboxen zu kaufen. Da Lootboxen mit echtem Geld bezahlt werden, sind sie besonders lukrativ für Spieleanbieter.

Empfehlung für Eltern und Pädagog:innen: „Spielt doch einfach mal selber, sammelt Praxiserfahrungen mit dem Medium, erstellt euch eigene Accounts und geht mit (euren) Kindern ins Gespräch, was da so erlebt wird!"

Mick Prinz, Amadeu-Antonio-Stiftung

LINKTIPPS

Einordnung zu Lootboxen: „Analyse der viel diskutierten Beutekisten unter Jugendschutzgesichtspunkten"

↗ www.jugendschutz.net/fileadmin/daten/publikationen/praxisinfos_reports/report_lootboxen.pdf

Übersicht über Eignung von Spielen nach pädagogischen Kriterien

↗ https://spieleratgeber-nrw.de/

Tipps für Eltern, um Kinder beim Gaming zu begleiten und zu den Sicherheitstipps

↗ www.klicksafe.de/digitale-spiele

↗ www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Gaming/gaming_node.html

Überblick über Anlaufstellen bei Medien-(Spiel)-Sucht

↗ www.ins-netz-gehen.info/beratungsstellendatenbank/

HERZLICH Willkommen!

ANTJE KIEßLER Moderation

AUFKLÄRUNG & HILFESTELLUNGEN FÜR ELTERN

RUNDUM Sicherheit IM NETZ

DIGITALE VORBILDER PODCAST & VIDEO

DATENSCHUTZ

DSGVO

Drittanbieter?

Löschbar?

Tipp: APPS selbst TESTEN!

TV? Ne!

VIDEO ON DEMAND YOUTOUBE

GAMING

Zielgruppe 12-16Jahre

USK 6

USK 16

MINECRAFT

FORTNITE

FIFA

KONSOLE

Tipp: VERBRAUCHER-ZENTRALE klicksafe.de SPIELERATGEBER NRW CHAOSCOMPUTERCLUB

TIPP: GESPRÄCH SUCHEN!

#DigitaleVorbilder

GAMING

SPIELEND SICHER!

ACHTUNG!

HALLO

KI-STIMMEN ERWACHSENE mit Kinderstimmen in Gaming Sprachchats

DIGITALES VORBILD SEIN!

GEMEINSAMER Medientag

Fluchtpunkt & ABLENKUNG?

MOBIL + ohne

Würdest du einen Flyer mit deinen Daten verteilen?

FLYER TEST

KINDER IN DIE REALITÄT HOLEN

KAUF mich! JETZT

VERMEINTLICH "KOSTENLOSE" APPS

TRIGGER

UMSÄTZE durch IN APP Käufe

PAY NOW

HOBBY BANKDATEN WOHNORT

DATENSCHUTZ

- PASSWÖRTER!
- 2-FAKTOR IDENTIFIZIERUNG
- AGBs LESEN

↓ mit CHAT GPT zusammenfassen

TIPP: DANEBEN SETZEN + VERSTEHEN

CRINGE

STRAFEN FÜR Unternehmen

UNTERNEHMEN DATENSAMMLER

DATEN BLACKBOX

LAUNCHER

MEIN DIGITALES PROFIL SPRACHCHATS

BENJAMIN HEINEMANN Experte

PREPAID KARTE

GRAPHIC RECORDING @elibrewing

Über die Moderatorin

Antje Kießler
Moderatorin & Journalistin

Über den Referenten

Benjamin Heinemann
Freier Medienpädagoge u.a. bei Creative Gaming e.V.

↗ creative-gaming.eu

CYBERMOBBING

#@?!%

2%!!!

>>>> AKTIV BEGEGNEN <<<<

Cybermobbing ist das absichtliche Beleidigen, Bedrohen, Bloßstellen, Ausgrenzen oder Belästigen anderer über das Internet durch einzelne oder mehrere Täter:innen, meist über einen längeren Zeitraum hinweg. Beleidigende Inhalte verbreiten sich rasend schnell im Netz und das Publikum kann bei Cybermobbing unüberschaubar groß sein.

DARUM IST DAS FÜR FAMILIEN RELEVANT

Aktuelle Studien belegen, dass mehr als **jeder zweite junge Mensch Cybermobbing** im direkten persönlichen Umfeld mit **erlebt hat**. Laut aktueller JIM Studie von 2023 haben zudem 14 % der befragten 12 bis 19-Jährigen im zurückliegenden Monat **persönliche Beleidigungen** oder **Anfeindungen** gegen sich selbst erfahren, weiteren 39 % sind **Hassbotschaften** im Netz begegnet.[1]

Cybermobbing kommt da vor, wo junge Menschen online am meisten aktiv sind: 52 % beim Messengerdienst **WhatsApp**, dicht gefolgt von den Social Media Plattformen **TikTok** mit 34 % und **Instagram** mit 33 %.[2]

[1] vgl. JIM 2023
[2] vgl. ebd.
[3] vgl. BSI 2024

DAS HAT CYBERMOBBING MIT DATENSCHUTZ ZU TUN

Beim Cybermobbing handelt es sich um ein Phänomen, bei dem **personenbezogene Daten**, wie Fotos oder Angaben zur Person, **missbräuchlich digital verbreitet werden**. Dabei wird von den Täter:innen gegen das Grundrecht auf informationelle Selbstbestimmung verstoßen.

In manchen Fällen geht Cybermobbing mit einem sogenannten **Identitätsdiebstahl** einher. Dem Opfer werden dabei die Zugangsdaten zum Nutzerprofil in einem sozialen Netzwerk entlockt. So können Täter:innen vermeintlich im Namen des Opfers Inhalte posten oder Nachrichten schreiben, um das Opfer in Misskredit zu bringen.[3]

DIESE RECHTE GELTEN AUCH IM NETZ

In Deutschland ist das Recht auf Meinungsfreiheit in Art. 5 des Grundgesetzes beschrieben. Manch eine:r meint, dass man sich dadurch alles erlauben darf. Dem ist jedoch nicht so!

Das Recht zur freien Meinungsäußerung gilt nicht uneingeschränkt. Es gerät da an seine Grenzen, wo die Menschenwürde und das Persönlichkeitsrecht anderer verletzt wird. Ebenso wenig sind strafbare Inhalte von der Meinungsfreiheit gedeckt. Obwohl Cybermobbing an sich in Deutschland kein eigener Straftatbestand ist, können damit folgende Tatbestände des Strafgesetzbuches (StGB) erfüllt sein:

§ 187 StGB Verleumdung
§ 185 StGB Beleidigung
§186 StGB üble Nachrede
§ 253 StGB Erpressung

Beim Cybermobbing gehen diese Taten oft mit der missbräuchlichen Verbreitung von Bildern oder Videos des Opfers einher, wodurch zusätzlich das Recht am eigenen Bild verletzt wird, was zivilrechtliche Konsequenzen nach sich ziehen kann. Es ist daher wichtig zu verstehen, dass die Meinungsfreiheit keine Rechtfertigung für respektloses oder schädigendes Verhalten im Internet bietet.



Zum Datenschutzbewusstsein gehört nicht nur die Vorsicht im Umgang mit den eigenen Daten, sondern auch die Achtung vor den Daten anderer.

Anzeichen Betroffener:

- Ein auffälliger Rückgang des Medienkonsums auf den üblichen Plattformen: der „Tatort“ wird gemieden
- Abfall schulischer Leistungen
- Konzentrationsprobleme
- Schulunlust & Schulverweigerung
- Isolation bzw. Ausgrenzung in Pausen, bei Gruppenarbeiten
- Depressionen & allg. psychische Probleme
- Müdigkeit durch Schlafstörungen

DAS KÖNNEN ELTERN PRÄVENTIV TUN

- Datenschutzbewusstsein schärfen: Vorsicht im Umgang mit eigenen Daten & Achtung vor fremden Daten vorleben
- Regeln für den Umgang mit den eigenen Daten und das Teilen von Bildern im Netz festlegen (siehe Kapitel „Kinderbilder im Netz“)

Geschützte Online-Umgebungen einrichten

- entsprechende **Privatsphäreeinstellungen**
- Nutzung des begleitenden **Elternmodus**, den viele Plattformen anbieten
- Beachtung der Altersangaben der Plattformen
- **wahrheitsgemäße Altersangabe** bei der Profilerstellung

Vertrauensvolle Eltern-Kind-Beziehung stärken

- Selbstwertgefühl & Resilienz **stärken**
- eine vertrauensvolle Beziehung pflegen, sich interessiert und **offen der Lebenswelt des Kindes/Jugendlichen gegenüber zeigen** und als Gesprächspartner:in zur Verfügung stehen
- Bewusstsein dafür vermitteln, **vor dem Posten nachzudenken**, ob man das so auch im 1:1-Setting sagen würde und möglichst verständlich zu formulieren (Emojis können dabei helfen)
- **Perspektivwechsel** ermöglichen: sich als Reflexionspartner:in anbieten und Empathie dafür vermitteln, wie Nachrichten oder Bilder in der geteilten Form (z.B. im Klassenchat) beim Betroffenen ankommen könnten
- einen respektvollen und wertschätzenden Umgangston **vorleben** und vermitteln

„Wenn du mitbekommst, wie jemand online gemobbt wird, bleib nicht stumm und unterstütze Betroffene bspw. durch eine liebe Nachricht.“

Melina Everhartz von der Online-Beratungsplattform JUUUPORT

Warum mobben Menschen andere?

Die Täter:innen mobben entweder aus Langeweile, weil sie sauer auf jemanden sind oder einfach, weil sie ein geringes Selbstwertgefühl haben. Einige Täter:innen wurden früher selbst gemobbt. Durch das Einschüchtern vermeintlich Schwächerer und entsprechend positiver Reaktionen eines „Publikums“ fühlen sie sich stark, witzig, beliebt und überlegen.

Etwas Gemeines über andere zu posten, fällt leicht, da demjenigen dabei nicht direkt in die Augen geschaut und dessen Betroffenheit ausgehalten werden muss. Manche mobben andere auch anonym, unter einem Pseudonym oder mittels eines Fake-Profils. Dadurch ist die Hemmschwelle nochmals gesenkt, sich respektvoll benehmen zu müssen.









NOTFALLTIPPS

Für Betroffene

- aktiv werden und sich Hilfe bei erwachsenen **Vertrauenspersonen/anonymen Beratungsstelle** holen
- Tat mit **Screenshots** und/oder einem **Mobbing-Tagebuch** dokumentieren
- **Nachricht** beim Seitenbetreiber **melden und löschen lassen**
- Täter:innen auffordern, das Foto/Video/Kommentar zu entfernen
- Täter:innen **blockieren**
- zusammen mit deinen Eltern **Strafanzeige** bei der Polizei stellen und zivilrechtliche Schritte prüfen

Für Eltern von Betroffenen

- **Gespräch** mit Kind suchen/nächste Schritte absprechen
- ggf. **Schule** und **Eltern der Täter:in** mit **einbeziehen**
- Betroffene darauf vorbereiten, dass Bilder/Videos immer wieder auftauchen können

Für Eltern von Täter:innen

- mit allen Beteiligten das Gespräch suchen und **Beweggründe hinterfragen**
- **Konsequenzen** für Täter:innen aufzeigen
- Gespräch zum Betroffenen/deren Eltern/der Schule suchen und eine Entschuldigung/einen Ausgleich/eine **Wiedergutmachung herbeiführen**
- Aufforderung zum umgehenden **Löschen** aller Bilder/Videos/Kommentare

Rechtssichere Screenshots

Ein zeitnah angefertigter, rechtssicherer Screenshot als Beweis einer Straftat ist wichtig, um den Behörden eine effektive Strafverfolgung zu ermöglichen. Dieser sollte folgendes beinhalten:

- den betreffenden Kommentar
- Datum und Uhrzeit des Kommentars
- (User-)Name des mutmaßlichen Täters
- Kontext, in dem der Kommentar gepostet wurde
- (User-)Name des Opfers

LINKTIPPS

Anlaufstellen für anonyme Onlineberatungen

- www.juuuport.de
- www.cybermobbing-hilfe.de/
- www.klicksafe.de/cmapp

Interaktiver Lernfilm für Grundschüler:innen

- www.planet-schule.de/schwerpunkt/elli-online/cybermobbing-film-100.html

Tipps für rechtssichere Screenshots auf unterschiedlichen Plattformen

- https://hateaid.org/rechtssichere-screenshots/

#Digitale Vorbilder

CYBERMOBBING

>>>> AKTIV BEGEGNEN



MODERATION: KATHARINA KRÜGER



EXPERTIN: ANN-KRISTIN GAUMANN



EXPERTE: LUKAS POHLAND

WO

TIPP: ANZEICHEN ERKENNEN! TATORT WIRD HÄUFIG GEMIEDEN!

SINUS-STUDIE 2024

52%

33%

34%

:(GROßE BELASTUNG FÜR BETROFFENE

AKTIV werden & NICHT mitmachen! BEITRÄGE MELDEN!

ERSTANLAUFSTELLE juuuport.de

ANGRIFFE RUND UM DIE UHR MÖGLICH

click

VERBREITUNG ÜBER WHATSAPP

SCHULE

VEREIN

TIPP: HILFE SUCHEN IST WICHTIG!

Hi

Hi!

TELEFON BERATUNG

ONLINE BERATUNG
- SCHNELL
- ANONYM

CYBERMOBBING-HILFE.DE

FOTOS

VIDEOS

TIPP
- SCREENSHOTS MACHEN!
- MOBBING TAGEBUCH ALS BEWEISMATERIAL!

TIPP: HEY, ICH BIN FÜR DICH DA!

KINDER AN DIE HAND NEHMEN! GEMEINSAM EINSTELLUNGEN VORNEHMEN!

mobbing

ON + OFFLINE

SCHAM GEFÜHLE

ERSTELLUNG VON FAKE PROFILEN

TIPP: BETROFFENE PERSON UNBEDINGT EINBEZIEHEN. AUSTAUSCH!

EMPATHIE

WIE WÜRDE ES MIR DAMIT GEHEN?

DISTANZ IM DIGITALEN RAUM

TÄTER·INNEN WAREN VORHER OFT SELBST BETROFFENE!

DROHUNGEN + VERÖFFENTLICHUNG VON KONTAKTDATEN & ADRESSEN

TIPP: ALS FREUND·IN DA SEIN, AGER AUCH FRAGEN UND AKTIV WERDEN!

ZIVILRECHT & STRAFRECHT ES GIBT NOCH KEIN EINDEUTIGES GESETZ!

§ - §

AN ELTERN VON TÄTER-INNEN:

DAS GESPRÄCH SUCHEN! KONSEQUENZEN KLAR MACHEN!

GRAPHIC RECORDING @elibrewing

Über die Moderatorin

Katharina Krüger
Journalistin & Projektmanagerin für die ARD Kinderangebote

Über die Referent:innen

Ann-Kristin Gaumann
Medienpädagogin & Kommunikationswissenschaftlerin, Medienpädagogisches Projektmanagement bei Juuuport e.V.
↗ www.juuuport.de

Lukas Pohland
Betroffener von Cybermobbing & Gründer der Online Beratungsplattform Cybermobbing Hilfe e.V.
↗ www.cybermobbing-hilfe.de

TATORT INTERNET

– Wie wir unsere Kinder vor Cybergrooming schützen

Cybergrooming ist eine Form von sexueller Gewalt, bei der Minderjährige gezielt über soziale Netzwerke und Online Games angeschrieben werden, um sexuelle Kontakte anzubahnen. Häufig geben sich Täter:innen in Chatforen oder auch mit Unterstützung von KI als Gleichaltrige aus und nutzen die kindliche Unbedarftheit, Vertrauensseligkeit und das mangelnde Risikobewusstsein aus, um zu ihren Opfern ein Vertrauens- oder Abhängigkeitsverhältnis herzustellen.

TÄTER:INNEN GEHEN HÄUFIG WIE FOLGT VOR

1. Kontaktaufbau

Der Kontaktaufbau zu Minderjährigen erfolgt häufig anonym auf sozialen Netzwerken, wie Instagram und TiKTok, Online-Spielen, wie Fortnite, oder Plattformen, wie YouTube oder Twitch.

2. Vertrauen gewinnen

Täter:innen versuchen zunächst Vertrauen aufzubauen. Sie zeigen sich interessiert, verständnisvoll und hilfsbereit, geben gleiche Interessen an und machen Komplimente oder (virtuelle) Geschenke. Oft drängen die Täter:innen an dieser Stelle schon auf einen Wechsel in unmoderierte Messengerdienste mit Kameraoption, wie WhatsApp oder Skype.



3. Sexuelle Übergriffe

Sobald sie das Vertrauen der Kinder oder Jugendlichen gewonnen haben, lenken die Täter:innen das Gespräch auf sexuelle Erfahrungen und Interessen der Minderjährigen. Sie senden ggf. selbst pornografisches Material und fordern intime Bilder oder Videos von dem Kind oder Jugendlichen an. Manchmal kommt es dabei sogar zum Vorschlag persönlicher Treffen, um offline in einen sexuellen Kontakt zu kommen.[1]

Wer und warum?

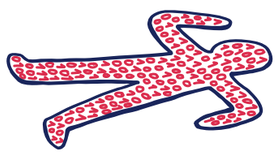
Sexueller Missbrauch findet in etwa 80 % bis 90 % der Fälle durch Männer und männliche Jugendliche statt, zu etwa 10 % bis 20 % durch Frauen und weibliche Jugendliche. Vielfältige Studien und Betroffenenberichte zeigen, dass es keine einheitliche Täterpersönlichkeit gibt. Allein der Wunsch, Macht auszuüben und durch die Tat das Gefühl von Überlegenheit zu erleben, eint sie.

DARUM IST DAS FÜR FAMILIEN RELEVANT

Sexuelle Belästigung Minderjähriger im Netz ist keine Seltenheit. Im Rahmen der JIM-Studie gaben 30 % der befragten 12- bis 19-jährigen Jugendlichen an, im Netz schon mal sexuell belästigt worden zu sein. Mädchen mit 36 % deutlich häufiger als Jungen mit 24 %, 6 % sogar regelmäßig pro Woche. Dies geschieht vor allem auf den Plattformen Instagram (35 %) und TikTok (20 %). Die von der Landesmedienanstalt NRW in Auftrag gegebene repräsentative Studie „Kinder und Jugendliche als Opfer von Cybergrooming“ von 2021 gibt genauere Einblicke: „Fast ein Viertel aller Kinder und Jugendlichen (24 %) wurde bereits im Netz von Erwachsenen zu einer Verabredung aufgefordert. Jedem sechsten Kind wurden von älteren Personen Gegenleistungen versprochen, wenn sie Bilder oder Videos von sich verschicken. Jedes siebte Kind wurde bereits aufgefordert, sich vor einer Webcam auszuziehen oder die Handykamera anzuschalten und etwa 15 % aller Kinder haben ungewollt Nacktbilder zugesendet bekommen.“[3]

DAS HAT CYBERGROOMING MIT DATENSCHUTZ ZU TUN

Das Risiko ungewollter Kontaktanbahnungen zu kriminellen Zwecken über Social Media-Kanäle oder Chatforen von Online Games kann durch datenschutzbewusstes Verhalten in Kombination mit geeigneten Privatsphäre- und Sicherheitseinstellungen vermieden werden. Die Aufklärung über potentielle Gefahren, wie das Verbreiten freizügiger Bilder von und durch Minderjährige in öffentlichen Profilen, sollte ein wichtiger Bestandteil der Medienerziehung sein.



DIESE RECHTE GELTEN AUCH IM NETZ

Cybergrooming als Form des sexuellen Missbrauchs von Kindern ohne Körperkontakt ist in Deutschland verboten gemäß § 176 StGB.

„Wer Kinder und Jugendliche im Internet mit sexueller Absicht bedrängt, muss mit Freiheitsstrafen von bis zu fünf Jahren rechnen“, so das Bundeskriminalamt.[4]

Folgende Handlungen fallen darunter:

- **Kontaktaufnahme zu Minderjährigen** mit beabsichtigten **sexuellen Handlungen***
- Zeigen von **pornografischem Material**
- **Motivation von Kindern zu sexuellen Handlungen**
- Herstellung von **Missbrauchsdarstellungen** (§ 184b)

Seit 2020 steht ebenfalls unter Strafe, wenn Täter:innen annehmen, mit einem Kind bis 13 Jahren zu schreiben, aber tatsächlich mit einem Erwachsenen, wie einem Elternteil oder mit verdeckten Polizeibeamt:innen, kommunizieren.

***Good to know:**

Zu „tatsächlichen“ sexuellen Handlungen muss es nicht kommen, auch muss das Kind nicht auf die Nachrichten reagiert haben. Für eine Strafbarkeit reicht es aus, dass das Kind eine solche Nachricht zur Kenntnis genommen hat.

[1] vgl. Klicksafe 2023: Cybergrooming
[2] UBSKM 2022
[3] Klicksafe 2023: Cybergrooming
[4] BKA 2024

DAS KÖNNEN ELTERN PRÄVENTIV TUN

Kindern altersangemessen Risiken verdeutlichen

- mit Kindern über die Absichten und das Vorgehen von Cybergroomern sprechen
- über Gefahren von Sexting aufklären
- Melde- und Sperrfunktionen zeigen
- über anonyme Anlaufstellen informieren (siehe Linktipps)

Regeln für den Umgang und das Teilen von Bildern und Daten im Netz festlegen

Tabu sind:

- Bilder von privaten und intimen Räumen, wie dem Kinderzimmer
- freizügige Fotos und Nacktbilder
- Bilder mit (möglicherweise versteckten) Hinweisen auf den Wohnort
- Profilbild mit identifizierbaren Personen
- Nickname mit Bezug zu Geschlecht, Wohnort oder Alter
- Einschalten der Kamera (Live-Cam), ohne Eltern um Erlaubnis zu fragen

Geschützte Online-Umgebungen einrichten

- für integrierten Kindersicherungsfilter wahrheitsgemäße Altersangaben machen
- Kontaktaufnahme durch Fremde unterbinden (Chat deaktivieren)
- Zugriff auf die Kamera deaktivieren, wenn sie nicht benötigt wird

Bei Treffabsicht mit einem Fremden aus dem Chat

- Chatverlauf zeigen lassen
- Treffen an einen öffentlichen Ort legen
- Treffen begleiten

„Höre auf dein Bauchgefühl! Wenn dir etwas unheimlich vorkommt, brich den Chat ab und blockiere den Kontakt."

Klicksafe, Kampagne gegen Cybergrooming

Diese ANZEICHEN sollten im Chat mit Fremden hellhörig machen:

- auffallend viele Komplimente
- sehr viel Zustimmung und Verständnis
- unglaubwürdiges Profil: keine Freunde, neu angelegt
- viele ähnliche Interessen
- Aufforderung, möglichst schnell in einen privaten Chat mit Video-Funktion zu wechseln
- Die Frage: „Bist du allein?"
- Täter verheimlicht eigene Identität (Verweigerung, Video anzuschalten)
- sexuelle Anspielungen
- unter Druck setzen
- Forderung, intime Bilder, Videos und persönliche Daten zu teilen
- Chat soll geheim bleiben, v. a. soll den Eltern nichts davon erzählt werden

NOTFALLTIPPS

Für Betroffene

- bei ungutem Gefühl sofort den Kontakt abbrechen
- sich einer erwachsenen Person anvertrauen
- Chatverlauf sichern
- eigenes Profil löschen und ein neues, sicheres Profil anlegen
- potenzielle Täter:innen verbal vertreiben, z.B. so:

„Lass mich in Ruhe!"

„Ich will das nicht!"

„Was du da machst, ist verboten. Ich melde das der Polizei und zeige dich an!"

„Ich erzähle weiter, was du da machst, damit du nicht andere Kinder belästigen kannst."

„Ich habe alles, was du gemacht hast, gespeichert. Ich habe Beweise!"

Für Eltern von Betroffenen

- Beweise sichern durch rechtssichere Screenshots
- Profil dem Seitenbetreiber melden und blockieren
- zeitnah Strafanzeige bei der Polizei / Onlinewache erstatten
- Hinweis an die Internet-Beschwerdestelle geben
- ggf. Hinzuziehen von Opferschutzexpert:innen





LINKTIPPS

Online-Meldestellen bei Cybergrooming

- www.polizei.de/Polizei/DE/Einrichtungen/Onlinewache/onlinewache_node.html
- www.soundswrong.de/melden/
- www.jugendschutz.net/verstoss-melden
- www.fragzebra.de/cybergrooming

Cybergrooming für Kinder erklärt

- kinderschutz-weimar.de/digitalisierte_gewalt/sexuelle-gewalt-im-internet/
- www.klicksafe.de/cybergrooming
- www.bka.de/DE/UnsereAufgaben/Aufgabenbereiche/Zentralstellen/Kinderpornografie/Cybergrooming/Cybergrooming_node.html

Anleitung zur Erstellung rechtssicherer Screenshots für unterschiedliche Plattformen und unterschiedliche Betriebssysteme

- https://hateaid.org/rechtssichere-screenshots/

ANONYME ANLAUFSTELLEN

Nummer gegen Kummer
für Kinder: 116111
für Eltern: 0800 – 111 0 550

Hilfetelefon Sexueller Missbrauch
0800-30 50 750

#DigitaleVorbilder

TATORT INTERNET

WIE KÖNNEN WIR UNSERE KINDER IM NETZ SCHÜTZEN?

MODERATION: KATHARINA KRÜGER



TIPP:
- KINDER BEGLEITEN
- IM GESPRÄCH BLEIBEN

DAS INTERNET IST **KEIN** RECHTSFREIER RAUM!!!

www.mediennutzungsvertrag.de

TIPP: MEDIEN-NUTZUNGS-VERTRAG

PERSÖNLICHE ENTSCHULDIGUNG

CYBER mobbing

juuuport.de

FUNKTIONEN PRÜFEN & EINSCHRÄNKEN
mikro - GPS-KAMERA

REGELN:
"DIGITALER FÜHRERSCHEIN"
KOMPETENZEN ENTWICKELN

TIPP: SPERR- & MELDE-FUNKTION

CYBER GROOMING
KONTAKTAUFNAHME ONLINE ÜBER CHATS
ZIEL: OFFLINE TREFFEN

EXPERTE: THOMAS FREITAG



DSGVO muss gelebt WERDEN!

ACHTUNG!!!
name@xx_de

EMAIL:
- OHNE NAMEN
- OHNE GEBURTS-DATUM

PERSONEN MELDEN

DIREKT ZUR POLIZEI

BEWUSSTSEIN FÜR EIGENE DATEN

VIRTUELLES GELD

MINECRAFT

ROBLOX

FORTNITE

GEFAHREN:
PHYSISCHER & PSYCHISCHER SCHADEN!

STRAFBARKEIT:
BEISPIEL: BESITZ VON KINDERPORNOGRAFIE ODER VERBOTENEN INHALTEN!



BESITZWILLE ZÄHLT!
NIEMALS TEILEN!!!

TIPP: MIT DER LEBENSWELT DER KINDER BESCHÄFTIGEN

click

12-19 JAHRE
FAST 4 Std
ONLINE PRO TAG

TIPP:
- KINDER BEGLEITEN
- SPIELE KENNEN

GROOMER
»DAS BLEIBT UNSER KLEINES GEHEIMNIS«

USK 16

WAS MACHT mein Gerät?

1. BEWEISE SICHERN!
2. SCREENSHOTS machen
3. STRAFANZEIGE
4. KINDERN DAS VORGEHEN ERKLÄREN

AB WANN IST MAN ZIVILRECHTLICH HAFTBAR IM DIGITALEN RAUM?
7 Jahre

EXPERTE: MARIO TSCHIRN



GRAPHIC RECORDING @elibrewing

Über die Moderatorin

Katharina Krüger
Journalistin & Projektmanagerin für die ARD Kinderangebote

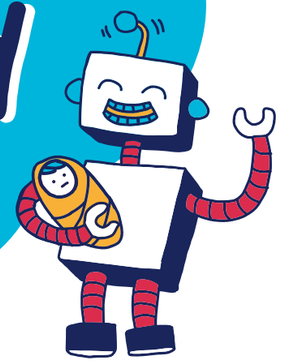
Über die Referenten

Mario Tschirn
Polizeiinspektion Anklam, Polizeiprävention a.D.

Thomas Freitag
Landeskriminalamt Mecklenburg-Vorpommern, Polizeiprävention

SMART FAMILY

KI ALS NEUES FAMILIENMITGLIED



Künstliche Intelligenz (KI) ist ein Bereich der Informatik, der sich mit der Entwicklung von Systemen beschäftigt, die menschenähnliche Intelligenz zeigen, wie z.B. das Lernen, Problemlösen und das Treffen von Entscheidungen. Diese Systeme nutzen Algorithmen und Modelle, um aus Daten zu lernen und Aufgaben autonom auszuführen. KI findet Anwendung in vielen Bereichen: von Spracherkennung über Bildverarbeitung bis hin zu autonomen Fahrzeugen und personalisierten Empfehlungen.

DARUM IST DAS FÜR FAMILIEN RELEVANT

Künstliche Intelligenz ist überall und bestimmt immer häufiger auch den Alltag von Familien. Manchmal ist es ihnen vielleicht gar nicht bewusst, dass es sich bei Anwendungen und Geräten um eine KI handelt. Es lohnt sich also, einen Blick darauf zu werfen, welche smarten Helfer für den Familienalltag sinnvoll sind, ob sie KI-basiert arbeiten und an welcher Stelle Vorsicht geboten ist, vor allem wenn es um sensible personenbezogene Daten geht.
Folgende smarte Geräte sind im Familienhaushalt denkbar:



Smarte Geräte

- Smarte Staubsauger
- SmartTV
- Smart Speaker
- Smarte Spielzeuge
- Smarte Überwachungskameras
- Fitnesstracker

Generative KI

- Übersetzungstools (DeepL, Google Translate)
- Bildgeneratoren (Luminar AI, Adobe Sensei, Canva)
- Chatbots bzw. Sprachmodelle (ChatGPT, Mistral AI)

KI als Ideengeber & Möglichmacher

Vor allem KI-Chatbots können im Schulalltag gut als **Ideengeber** genutzt werden. Es geht nicht darum, sich fertige Ergebnisse ausspielen zu lassen, sondern einen ersten Impuls zu bekommen und auf dieser Grundlage weiterzuarbeiten.

Als **Nachhilfelehrer** ist eine KI vielen Eltern eine gute Unterstützung. In Momenten, wo sie selbst keine Antworten oder Lösungen haben, können sie eine KI für die Recherche nutzen.

Generell ist es empfehlenswert, als Familie gemeinsam die KI auszutesten und zu verstehen, wo die Möglichkeiten und Grenzen sind.

Smarte Staubsauger oder Sprachassistenten können hier gute Alltagshelfer im Haushalt sein.

DAS HAT KI MIT DATENSCHUTZ ZU TUN

Beim Einsatz smarter Geräte und Anwendungen muss geprüft werden, ob sie mit personenbezogenen Daten arbeitet und wie diese zu schützen sind. KI-Systeme, die auf **maschinellem Lernen** basieren, benötigen für ihre Funktionsfähigkeit in der Regel sehr viele (ggf. auch personenbezogene) Daten. Dies bezieht sich insbesondere auf die Lern- und Betriebsphase. Wenn diese Daten nicht ordnungsgemäß geschützt sind, können unbefugte Personen oder Organisationen darauf zugreifen, was von unberechtigter Offenlegung über die (ungewollte) Verfälschung von Daten bis hin zum Identitätsdiebstahl gehen kann.

Insbesondere bei KI-Systemen, die **Technologien, wie Gesichtserkennung oder Fingerabdrücke**, nutzen, ist Vorsicht geboten. Diese sehr sensiblen Daten müssen besonders geschützt werden und dürfen nicht in falsche Hände gelangen.

Generative KI-Tools sammeln und speichern häufig Benutzeranfragen und -antworten. Unternehmen analysieren diese Interaktionsdaten dann und nutzen sie zum Trainieren zukünftiger Modelle.[1]

Hacker nutzen Systeme des maschinellen Lernens für Social-Engineering-Angriffe oder Phishing-Betrug. Sie tun dies, indem sie plausible E-Mails, Dokumente usw. generieren, die Malware einschleusen oder Anmeldeinformationen stehlen.[2]

DIESE RECHTE GELTEN IN BEZUG AUF KI IM NETZ

Die KI-Verordnung (Engl. Artificial Intelligence Act, kurz: **AI Act**) ist eine Verordnung der Europäischen Union zur Regulierung der Entwicklung und Nutzung von Künstlicher Intelligenz. Die Verordnung soll sicherstellen, dass KI-Systeme sicher, transparent und mit den Werten der Europäischen Union vereinbar sind.

So müssen künstlich erzeugte Inhalte, wie Videos oder Bilder, als solche gekennzeichnet werden.



***Good to know:**

Smart ist nicht KI. Smarte Geräte bieten oft automatisierte Funktionen und sind vernetzt, aber sie müssen nicht zwingend über KI verfügen.

[1] vgl. DSK 2024
[2] vgl. Ansario 2023

DAS KÖNNEN ELTERN PRÄVENTIV TUN

Sich vor dem Kauf über die KI-basierten Produkte und den Hersteller informieren

- In welchem Umfang werden Daten erhoben, gespeichert und an Dritte weitergegeben?
- Gibt es die Möglichkeit, am Gerät/Programm den Ruhemodus zu aktivieren?
- Welche Sicherheitseinstellung kann man am Gerät/Programm vornehmen?
- Kann man das KI-Training deaktivieren?
- Gibt es das Gerät ohne KI?
- Hat die KI in dem Gerät einen wirklichen Nutzen?

Sich über Gefahren informieren und darüber aufklären

- Suchtpotential prüfen, wenn KI-Anwendungen den Alltag bestimmen
- missbräuchlicher Einsatz durch das Imitieren der Stimme mithilfe von KI
- Bilder können einfach generiert werden und missbräuchlich benutzt werden: Deepfake
- KI kann Cybermobbing durch den Einsatz von automatisierten Bots verstärken

Tipps für die Verwendung von KI

- bei Eingabe von Arbeitsaufträgen (Prompts) keine sensiblen Informationen preisgeben (Passwörter, Namen, Geburtstag, Telefonnummern, Gesundheitsdaten usw.)
- Informationen, Quellen und Aussagen einer KI auf Richtigkeit prüfen
- Reflektionsfähigkeit des Nutzenden schärfen: Sind Bilder und Texte KI-generiert? Handelt es sich um Deepfakes?
- Nachhaltigkeit thematisieren: KI und Stromverbrauch
- erst selber lernen, dann KI nutzen
- Prompts bei Texten (sofern nicht individuell bearbeitet) und Bildern als Quelle angeben
- bei Besuch zu Hause über aktiven Sprachassistenten informieren und auf Wunsch ausschalten
- Zugriff auf die Kamera deaktivieren, wenn sie nicht benötigt wird

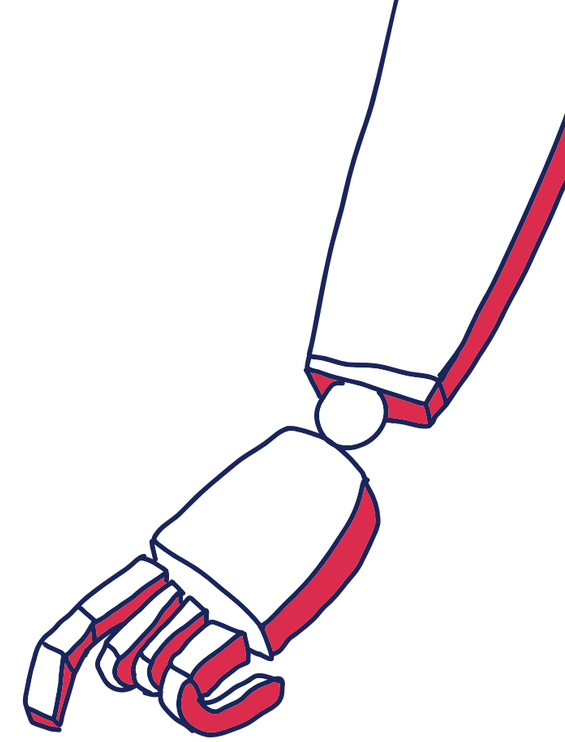


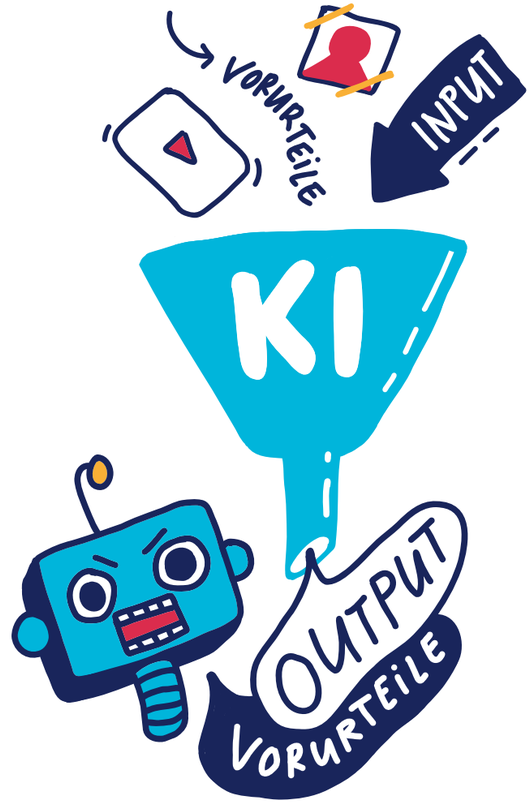
„Künstliche Intelligenz begegnet uns allen täglich. Deswegen sollten wir die Funktionsweise und den Einfluss auf unsere Entscheidungen besser verstehen lernen.“

Auszug aus dem Webinar „Smart Family“ vom 06.03.2024 von **Prof. Dr. Sandra Schulz**, Juniorprofessorin für Informatik und Didaktik an der Universität Hamburg

ETHISCHE PERSPEKTIVE

Eine KI kann in vielen Fällen durch neue Eingaben von Nutzenden stetig dazulernen. Das bedeutet, dass die Art der Eingaben und der verwendeten Inhalte, mit denen eine KI trainiert wird, ihre Ausgaben entsprechend beeinflussen kann. Wenn eine KI mit diskriminierenden Texten und Aussagen befüllt wurde, spielt sie diese entsprechend wieder aus, wodurch sich bestimmte Haltungen in der Gesellschaft verfestigen und verstärken können. Eine KI kann das Phänomen der Filterblasen verstärken, so dass bestehende Ansichten damit noch mehr verstärkt werden. Daher sind Antworten der KI immer kritisch zu betrachten und sollten nicht unreflektiert übernommen werden.





LINKTIPPS

- www.klicksafe.de/kuenstliche-intelligenz
- www.thats-ai.org/
- www.internetmatters.org/de/resources/parent-guide-to-artificial-intelligence-ai-tools/

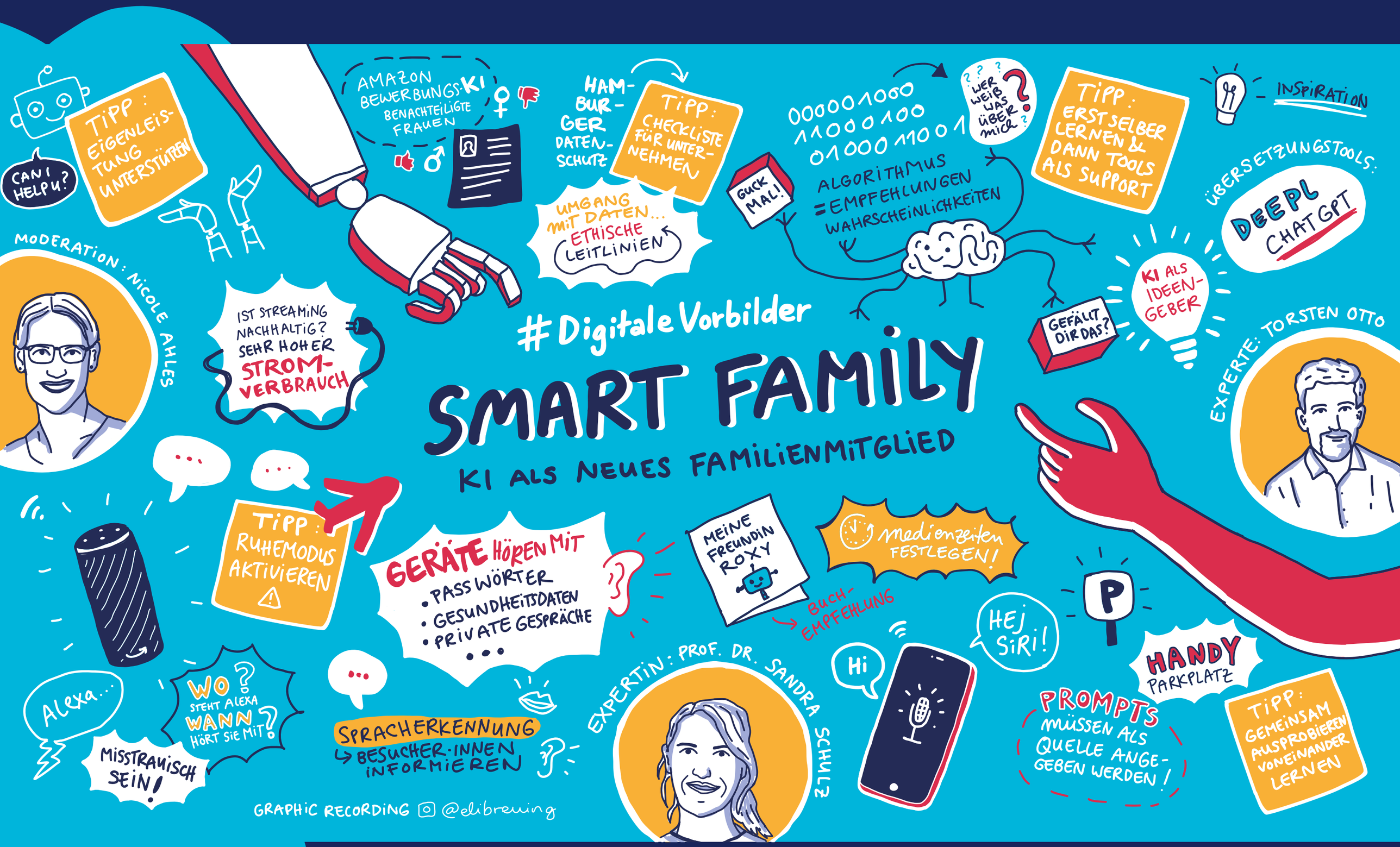
BUCHTIPP

Kenza Ait Si Abbou (2022)
„Meine Freundin Roxy“
Berlin: Tulipan-Verlag.

#Digitale Vorbilder

SMART FAMILY

KI ALS NEUES FAMILIENMITGLIED



GRAPHIC RECORDING @elibrewing

Über die Moderatorin

Nicole Ahles
Moderatorin und Journalistin

Über die Referent:innen

Prof. Dr. Sandra Schulz
Juniorprofessorin für Didaktik und Informatik
an der Uni Hamburg

Torsten Otto
Lehrer für Informatik am
Kurt-Körber-Gymnasium Hamburg

SMARTE SPIELZEUGE



Smarte Spielzeuge sind mit Bluetooth oder Internet verbunden und können mit ihrer Umgebung interagieren. Puppen, Roboter, Kuscheltiere, Drohnen oder Autos sind mit Sensoren, Mikrofonen oder Kameras ausgestattet, um ein spielerisches Erlebnis zu bieten, das sich an die Bedürfnisse und Vorlieben des Kindes anpasst.

DARUM IST DAS FÜR FAMILIEN RELEVANT

Die Familie bzw. das Zuhause ist ein besonders schützenswerter Ort. Hier werden private und sehr intime Gespräche geführt, die im besten Fall nicht nach außen gelangen. Smarte Spielzeuge, die immer beliebter werden, bieten interaktive und pädagogisch wertvolle Erfahrungen für Kinder.

Eltern sollten sich jedoch vor der Anschaffung eines smarten Spielzeuges darüber informieren, ob es Sicherheitsbedenken geben könnte und in welchem Umfang es eingesetzt werden kann.

Dabei ist es wichtig, ein Gleichgewicht zwischen innovativen Lernmöglichkeiten und dem **Schutz der Privatsphäre** zu finden.

DAS HABEN SMARTE SPIELZEUGE MIT DATENSCHUTZ ZU TUN

Smarte Spielzeuge verbinden sich mit dem Internet und passen sich individuell an die Bedürfnisse und Vorlieben der Kinder an. Dabei werden je nach Spielzeug Audioaufnahmen, Fotos, Videos, Standortdaten, Nutzungsdaten und Geräteinformationen gespeichert und zu einem **Verhaltensprofil** zusammengefügt. Dieses ermöglicht den Firmen, seinen Kund:innen personalisierte Erlebnisse zu bieten, die Interaktionen zu verbessern, Inhalte besser auf die Interessen der Kinder abzustimmen und **personalisierte Werbung** auszuspielen.[1]

Wie eine aktuelle Studie der Universität Basel belegt, ist neben der Erstellung von Verhaltensprofilen von Kindern auch **fehlende Transparenz** wegen unzureichender und schwer zugänglicher Informationen **über die Datenerhebung und -verarbeitung** unter Herstellern von smarten Spielzeugen weit verbreitet, zu dem diese laut Transparenz-Grundsatz der **DSGVO** verpflichtet sind.[2]

Familien, die sich für den Erwerb eines smarten Spielzeugs entscheiden, sollten sich im Vorfeld über die **Risiken** bewusst werden.

Potentielle Einfallstore für Kriminelle mit Interesse an den erfassten Datenmengen bieten zum einen **unzureichend gesicherte Übertragungswege** via Bluetooth oder WLAN und zum anderen auch **nicht DSGVO-konforme Speicherorte**.

So können Daten wie Namen, Kontaktdaten, Alter und Vorlieben des Kindes, Kontoverbindung auf nicht ausreichend gesicherten weltweiten Hersteller-Servern von Hackern unbefugt abgegriffen und zum Zwecke des **Identitätsdiebstahls** verwendet werden.

Wenn das Heimnetzwerk über das Hauptkonto gesteuert wird, sind bei solch einem **Datenhack** nicht nur die Daten und privaten Informationen der smarten Geräte in Gefahr, sondern möglicherweise auch Zugangsdaten von E-Mails, Social Media-Accounts und sogar Bankkonten.[3]

Nutzen smarte Spielgeräte bspw. **Bluetooth-Verbindungen ohne individuellen Passwortschutz**, könnte jeder Smartphone-Besitzer in Reichweite dieses Gerätes intime Momente aus dem Leben der Familie ausspionieren und theoretisch über das Mikrofon Kontakt zum Kind aufnehmen. Das Bewusstsein, dass das eigene Zuhause durch smarte Geräte überwacht wird, kann bei Eltern und Kindern zu **Verhaltensänderungen** führen und erhebliche **psychische Belastungen**, Angst und Unsicherheit hervorrufen.

Ohne geeignete Privatsphäreeinstellungen kann das durch einen GPS-Tracker erstellte **Bewegungsprofil** in einem smarten Gerät (z.B. Smartwatch) unbeabsichtigt in die Hände von Dritten gelangen. In Verbindung mit weiteren Profildaten des Kindes stellt dies ein Sicherheitsrisiko dar.

DIESE RECHTE GELTEN IN BEZUG AUF SMARTE SPIELZEUGE IM NETZ

Um die Sicherheit insbesondere von Kindern zu schützen, hat die Bundesnetzagentur 2017 Smart Toys mit Abhörfunktionen via Voice-Monitoring verboten. Dies betrifft Geräte und Spielzeuge, die heimlich Gespräche aufzeichnen oder ihre Besitzer:innen filmen und diese Aufnahmen kabellos an andere Geräte übertragen.

An den meisten Schulen in Deutschland ist die Nutzung von Smartwatches mit versteckter Abhörfunktion, zum Schutz der allgemeinen Persönlichkeitsrechte, untersagt.

Trotz geltenden **Grundrechts auf Freiheit und Privatsphäre** ist das Tracking der eigenen Kinder mittels GPS für Eltern oft selbstverständlich. Jedoch kommt es gleichzeitig einer **Dauerüberwachung** der Kinder gleich. Hier sollte vorher im Gespräch mit Eltern und Kindern geklärt werden, welche **Regelungen** es dazu **in der Familie** gibt.

Drohnen mit Kamerafunktion sind EU-weit für Kinder unter 16 Jahren verboten, wenn sie nicht unter die 2009/48/EG-Spielzeugrichtlinie fallen.[4]



[1] vgl. Verbraucherzentrale 2023

[2] vgl. heise online 2024

[3] vgl. BSI 2024: So schützen Sie sich vor digitalem Identitätsdiebstahl

[4] vgl. BVL 2024

Da die verschiedenen Produkte auf unterschiedliche Art und Weise Daten sammeln und speichern, seien an dieser Stelle exemplarisch einige vorgestellt:

Sprechende Puppen und Kuscheltiere

Sie sind mit **Mikrofonen und Lautsprechern** ausgestattet, um mit den Kindern interagieren zu können. Sie erfassen Stimmen und Gespräche, Informationen über Interaktionen und Lernfortschritte, die zur Speicherung, Verarbeitung und Analyse der Daten an den Server des Herstellers gesendet werden.

Wearables für Kinder

Wearables, also am Körper tragbare Geräte, wie Smartwatches, Fitness-Tracker oder GPS-Tracker, sind mit dem Internet verbunden und lassen sich über eine Smartphone-App steuern. Sie geben beispielsweise Auskunft über den Standort des Kindes und erstellen **Bewegungs- und Aktivitätsprofile**.

Vernetzte Spielzeugautos, Drohnen und Augmented Reality (AR)

Diese Spielzeuge ermöglichen Live-Übertragungen, zeichnen Fahrten oder Flüge auf und senden diese Daten an verbundene Geräte.

Smarte Lernspielzeuge

Diese Spielzeuge sind häufig mit Sensoren und Prozessoren ausgestattet, die eine Interaktion mit dem Kind ermöglichen. Sie bieten oft personalisierte Lerninhalte oder Spielaktivitäten, basierend auf den Fortschritten des Kindes.

Sie zeichnen die Nutzungsdauer und –häufigkeit auf und können persönliche Informationen, wie Alter und Name des Kindes sowie Daten über den Lernfortschritt, Antworten auf Aufgaben und Bewertungen, sammeln. Bei Spielzeugen mit Emotionserkennung können zusätzlich Daten über die emotionale Reaktion des Kindes auf verschiedene Lernaktivitäten erfasst werden.

Babyphones mit erweiterten Funktionen

Moderne Babyphones sind oft mehr als einfache Audioübertragungsgeräte. Sie sind mit Bewegungssensoren, Nachtsichtkameras und Temperatur-Überwachung ausgestattet und übertragen die Daten über Funk oder WLAN.

DAS KÖNNEN ELTERN PRÄVENTIV TUN

Vor dem Kauf informieren

- nur smarte Geräte von vertrauenswürdigen Herstellern im Geltungsbereich der DSGVO kaufen
- Verbrauchertests und Produktinformationen zu Rate ziehen
- Sicherheitsrisiken, wie Datenklau und Speicherung, abklären
- Altersempfehlungen ernst nehmen
- Risiken zur Privatsphäre abklären

Während der Nutzung

- so wenig personenbezogene Daten wie möglich preisgeben
- in den Einstellungen der Geräte und Apps den Zugriff auf unnötige Daten beschränken
- Sicherheitsupdates regelmäßig durchführen
- Heimnetzwerk durch starke Passwörter und sichere **Konfiguration des Routers** schützen
- Offline-Nutzung des Gerätes bevorzugen[1]
- Kameras/Mikrofone bei Nichtverwendung deaktivieren oder abkleben



NOTFALLTIPPS

Im Falle eines Datenhacks

- betroffenes Spielzeug sofort vom Internet trennen, um weiteren Datenverlust oder -missbrauch zu verhindern
- alle Passwörter ändern, die für das Spielzeug und dessen Apps eingerichtet wurden
- **Hersteller des Spielzeugs** informieren, um das Problem zu melden und Rat zu erhalten
- bei Verlust persönlicher Daten die zuständige **Datenschutzaufsichtsbehörde** informieren
- bei schwerwiegenden Verstößen **rechtliche Schritte** gegen den Hersteller oder Anbieter einleiten (Schadensersatz)
- **Verbraucherschutzorganisationen kontaktieren** zur Beratung in Fällen von Missbrauch oder unsachgemäßer Nutzung



[1] vgl. BSI 2024: Smart Toys





LINKTIPPS

Worauf Eltern vorm Kauf achten sollten

↗ www.verbraucherzentrale.de/wissen/umwelt-haushalt/spielzeug/vorsicht-bei-smart-toys-die-risiken-von-vernetztem-spielzeug-29297

Bei Unklarheiten, ob ein bestimmtes Spielzeug verboten ist, hilft die Bundesnetzagentur weiter

↗ www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2022/20221207_SmarteProdukte.html

↗ www.jugendschutz.net/fileadmin/daten/publikationen/praxisinfos_reports/praxisinfo_vernetztes_spielzeug.pdf

#DigitaleVorbilder
SMARTE SPIELZEUGE

STANDORT

MODERATION: ANTJE KIEßLER



WAS SIND smarte SPIELZEUGE?
- WLAN
- INTERNET
- BLUETOOTH

NUTZUNGS DATEN + TON + KAMERA-BILD

TIPP: -PW -KAMERA +MIKRO AUSSTELLEN

TIPP: KINDER SENSIBILISIEREN

VERANTWORTUNG ÜBER KINDERDATEN LIEGT BEI ELTERN!



ACHTUNG! HERSTELLER GEBEN DATEN WEITER

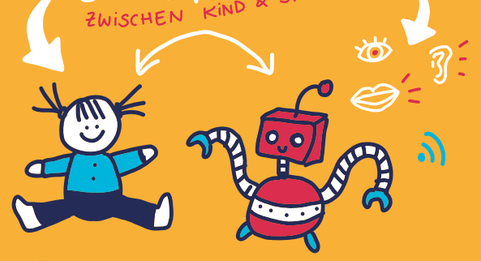


COGNI TOYS

TIPP: ·DSGVO ·AUSKUNFT BEIM HERSTELLER EINFORDERN

DATENSCHUTZ IST MENSCHENSCHUTZ

INTERAKTIONEN
ZWISCHEN KIND & SPIELZEUG





EXPERTIN: JESSICA WAWRZYNIAK

HELLO BARBIE APP ALS WANZE EINGESTUFT



ABGEHÖRT & GESPEICHERT AUF DEM TOYTALK SERVER

MATTEL

PERSÖNLICHKEITS-RECHTE
- RECHT AUF SELBSTDARSTELLUNG

§

hallo*
*ICH HÖRE ZU!

VERTRAUEN STATT KONTROLLE

SMART WATCH



TIPP: KANN DAS W-LAN AUSGESTELLT WERDEN?

BUCHEMPFEHLUNG

BEWUSSTSEIN SCHAFFEN
WO SIND DIE SPIELZEUGE?
WANN HÖREN SIE MIT?

TIPTOI

DIGITAL ZWANG? #VORBILDSEIN

MISSBRAUCH DATENNUTZUNG FÜR MOBBING

TIPP: ·BUNDES-NETZ-AGENTUR ·DSGVO

BNetzA

TIPP: VERBRAUCHER-SCHUTZ

GRAPHIC RECORDING @elibrewing

Über die Moderatorin

Antje Kießler
Moderatorin & Journalistin

Über die Referentin

Jessica Wawrzyniak
Erziehungs- und Medienwissenschaftlerin,
Referentin, Autorin

ANLEITUNG FÜR DIE NUTZUNG VON MESSENGERDIENSTEN

Messengerdienste sind digitale Kommunikationsplattformen zum Versenden von Sofortnachrichten in Form von Text, Bildern, Audios oder Videos zwischen zwei oder mehreren Kommunikationspartner:innen über eine Internetverbindung. Gerade Gruppenchats und Kanäle können zum Abgreifen von Daten oder Verbreiten strafbarer Inhalte genutzt werden.

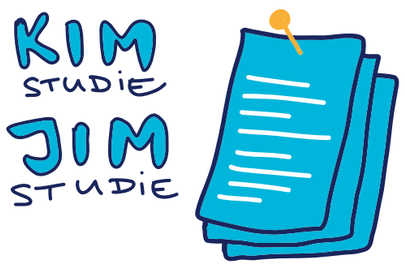
DARUM IST DAS FÜR FAMILIEN RELEVANT

Laut aktueller JIM-Studie besitzen 96 % der Jugendlichen ein eigenes Smartphone und sind täglich durchschnittlich 224 Minuten online. Dabei wird der Messengerdienst WhatsApp bei 74 % der befragten Jugendlichen als die mit Abstand wichtigste App bezeichnet.

Im Vergleich zu aktuell auf dem Markt befindlichen Messengerdiensten wird WhatsApp von Jugendlichen mit 94 % am häufigsten genutzt. Erwachsene mitgerechnet, nutzten die App 2023 laut einer Statista-Umfrage 86 % aller Messenger-Nutzenden.

Messenger-Alternativen zu WhatsApp laufen gemessen an der Nutzungsverbreitung weit außerhalb der Konkurrenz des Marktführers: Telegram nutzen 10 %, Signal 9 % und Threema 3 % der befragten Jugendlichen. Die beiden letztgenannten Messengerdienste können aus datenschutzrechtlicher Sicht als weniger bedenklich eingestuft werden.

Es gibt Messenger-dienste, die haben sich Werten wie Privatsphäre, Sicherheit und Transparenz verschrieben. Das sollte man regelmäßig überprüfen.



DAS HABEN MESSENGERDIENSTE MIT DATENSCHUTZ ZU TUN

Es gibt einige Aspekte, die aus datenschutzrechtlicher Perspektive bei Messengerdiensten zu berücksichtigen sind.

Kritisch zu betrachten sind Gruppenchats und Kanäle. Hier besteht die Gefahr, dass in großen, anonymen Gruppen Fremde die Telefonnummer und das hinterlegte Profilbild mit Namen und Beschreibungstext sehen können. Dies kann in den **Privatsphäre-Einstellungen** des Messengerdienstes unterbunden werden.

Vorsicht bei Statusmeldungen: Jeder abgespeicherte Kontakt kann gemäß den Voreinstellungen die eigenen Statusmeldungen einsehen. Wer dies nicht möchte, sollte regelmäßig die Ausschlusskontakte in den Datenschutzeinstellungen aktualisieren oder ganz auf Statusmeldungen verzichten.

Empfehlenswert sind Messengerdienste mit **Ende-zu-Ende-Verschlüsselung**, auch von Gruppenchats. Ohne diese ist es Dritten sowie dem Anbieter selbst möglich, Inhalte mitzulesen und Daten abzugreifen

DIESE RECHTE GELTEN AUCH IM NETZ

Wer Mitglied in einem (möglicherweise anonymen) Gruppenchat oder Abonnent eines Kanals ist, läuft Gefahr, Adressat von **strafbaren Inhalten** zu werden. Diese Inhalte können für Kinder und Jugendliche **entwicklungsschädigend** und traumatisierend sein.

Verbotene Inhalte umfassen u.a.

- verfassungsfeindliche Symbole
- Aufrufe zu Straftaten
- Volksverhetzung
- Holocaustleugnung
- Billigen, Leugnen und Verharmlosen von Völkermord
- Verbrechen gegen die Menschlichkeit und Kriegsverbrechen
- Verherrlichung von Gewalt und Verletzung der Menschenwürde
- Verbreitung pornografischer Inhalte, darunter fällt auch Kinderpornografie oder beispielsweise auch mit Tieren u.ä.
- Gewaltandrohung

Die **Verbreitung dieser Inhalte** ist in Deutschland verboten und kann zu einem Strafverfahren mit **Geld- oder Freiheitsstrafen** führen. Bis zur Vollendung des 18. Lebensjahres unterfallen diese Vergehen dem Jugendstrafrecht.

Bei **(kinder)pornografischem Bild- und Videomaterial** ist bereits der **Besitz strafbar**.

Messengerdienste benötigen das Adressbuch, um die Kontakte auch in der App anzuzeigen. Bei WhatsApp passiert das **automatisiert** und kann nicht unterbunden werden. Damit werden alle dort abgespeicherten Kontakte sowie die dazugehörigen Daten, wie Profilbild, Beschreibungstext und Name (auch wenn diese Kontakte selbst kein WhatsApp nutzen) ausgelesen und an den Mutterkonzern Meta und ihre Tochter-Unternehmen Facebook und Instagram weitergegeben. Das ermöglicht es, Profile zu vervollständigen und zudem an nicht näher benannte (Werbe-)Partner (auch in nicht EU-Ländern) weiterzugeben. Das passiert ganz schnell, wenn der automatische Download von Inhalten eingeschaltet ist.

[1] vgl. BZgA 2024

Auch für Nutzende vielleicht als harmlos eingestufte Metadaten werden von Messengern **unverschlüsselt erfasst**. Diese Daten sind für Werbetreibende interessant, da sich mit ihrer Hilfe ein Nutzender unter Umständen eindeutig identifizieren sowie sein Kommunikationsverhalten analysieren lässt.

Je nach Messengerdienst und Einstellung werden folgende Daten gesammelt und ggf. weiterverwendet:

- Fotos: Profilbild, Statusmeldungen, ggf. unverschlüsselte Chats
- eigene Telefonnummer und Kontakte aus dem Telefonbuch
- Metadaten: Mit wem wurde wie oft und wie lange kommuniziert? Wie lange online? Nutzungshäufigkeit, IP-Adresse und Geräteinformationen (Modellnummer, Betriebssystemversion, App-Version, Ländervorwahl, Netzwerkcode, Nutzungsinformationen wie das Registrierungsdatum, Art der Nutzung)
- Standort aus GPS, WLAN und mobilen Daten
- Anzeigename
- Geburtsdatum
- noch nicht empfangene Nachrichten (Server)
- Anrufinformationen wie Zeitpunkt, Telefon- und Gerätenummer

Vorsicht bei Handyvertragswechsel vor ungewollter **Account-Übernahme durch Fremde.** Durch die Verknüpfung des WhatsApp-Profils mit der Telefonnummer kann es bei Neuvergabe der alten Telefonnummer passieren, dass derjenige, dem die alte Handynummer bei Anbieterwechsel neu zugeteilt wurde, nun Zugriff auf ein bestehendes WhatsApp-Profil erhält, inklusive Chathistorie und Kontakten. Deswegen bei Rufnummernwechsel immer WhatsApp informieren und sicherheitshalber eine 2-Faktor-Authentifizierung einrichten.[1]

[1] vgl. Verbraucherzentrale 2024

DAS KÖNNEN ELTERN PRÄVENTIV TUN

Auswahl eines datenschutzfreundlichen Messengerdienstes

Aus den **AGB und den Nutzungsbedingungen** lassen sich folgende Informationen entnehmen:

- Welche Daten werden wo und wie lange gespeichert?
- Welche Informationen werden an Dritte (Werbepartner) weitergegeben?
- Welche Bildrechte gebe ich ab, wenn ich sie hochlade?
- Wenn die App kostenlos ist, wie finanziert sie sich?
- Gibt es eine integrierte Ende-zu-Ende-Verschlüsselung für Einzel- und Gruppenchats?
- Lassen sich selbstlöschende Nachrichten einstellen oder auch rückwirkend aus dem Chatverlauf entfernen?
- Lässt sich die Standortfreigabe deaktivieren?
- Kann die Freigabe des Adressbuchs abgelehnt werden?
- Gibt es die Möglichkeit, in Gruppenchats das Anzeigen des Profilbildes und der Handynummer zu unterbinden?
- Ab welchem Alter ist der Dienst geeignet?

Passt die Altersfreigabe zum Alter meines Kindes?

Die Gefahren, welche die Verwendung von Messengerdiensten mit sich bringen, sind vielfältig. Gleichzeitig gibt es unterschiedliche Altersangaben. Die richtigen Angaben stehen in den AGB. Wichtig ist zu wissen, dass die Angaben die in den App-Stores stehen nicht immer richtig sind. Wenn die USK den Dienst bewertet hat, dann wurde dort nur die Funktionsweise bewertet, nicht mögliche Gefahren durch die Nutzung.

Vorabeinstellungen zusammen mit dem Kind/Jugendlichen vornehmen

- Kontoinformationen pseudonymisieren (weder Klarname noch identifizierbares Profilbild)
- App-Sperre einrichten
- Einschränken der:
  - Live-Standortfreigabe
  - Kontaktdaten-Freigabe (Telefonnummer, Info, Profilbild)
  - Aktivitätsstatus auswählen und besprechen (zuletzt online, Lesebestätigung)
  - Reichweite Statusmeldungen
  - Berechtigung, in Gruppen hinzugefügt zu werden
- Deaktivieren automatischer Downloads geteilter Bilder/Videos und der zusätzlichen Sicherung auf dem Gerät
- Cache mit einem zeitlichen Ablauf versehen, damit lokale Daten nach einer gewissen Zeit gelöscht werden
- Standardeinstellung, wie Speicherdauer, selbstlöschende Nachrichten, zum Nachrichtenversand vornehmen
- Melde- und Blockierfunktion erkunden
- ggf. Zeitbegrenzung unter der Funktion Digital Wellbeing in der App vornehmen

Nutzungsregeln für die Kommunikation

- respektvollen Umgangston wählen
- Regeln für das Teilen von Inhalten festlegen: Was sind strafbare Inhalte?
- vor dem Versenden kurz innehalten und überlegen, wer die Fotos, Videos und Nachrichten sehen soll
- keine Kettenbriefe weiterleiten
- in Gruppenchats aktiv Position beziehen, wenn jemand gemobbt wird
- für den Klassenchat Regeln und Konsequenzen bei Regelverstoß festlegen und einen Admin bestimmen (z.B. Nutzungszeiten, Umgang mit Spam, Inhalte allg.)

NOTFALLTIPPS

- fragwürdigen Gruppenchat verlassen
- Konto löschen (nicht nur die App!)
- alternativen Messengerdienst nutzen
- neue Nummer beantragen (Mobilfunkanbieter)

LINKTIPPS

Online-Meldestelle für Kinderpornografie, Extremismus und Cybercrime

- www.netzverweis.de/Meldestelle/
- www.internet-beschwerdestelle.de

Polizeiberatung zu strafbaren Inhalten

- www.polizei-beratung.de
- www.polizeifuerdich.de

Vergleich von Messenger-Alternativen

- www.test.de/Messenger-Apps-im-Vergleich-4884453-0/
- www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsapalternativen-messenger-im-ueberblick-13055

Regeln für Gruppenchats

- www.handysektor.de/artikel/10-goldene-regeln-fuer-den-gruppenchat-in-whatsapp

Literaturverzeichnis

AG Bad Hersfeld Familiengericht (2017): familiengerichtlicher Beschluss (Sorgerecht / Auflagen) bzgl. Aufsichtspflicht, Medien-Nutzung durch Minderjährige, Suchtgefahr, https://www.lareda.hessenrecht.hessen.de/bshe/document/LARE190000030 zuletzt aufgerufen am 26.09.2024.

Ansario, Dariush (2023): Deepfakes und WormGPT - Mit KI gegen KI, https://www.connect-professional.de/security/mit-ki-gegen-ki.328422.html zuletzt aufgerufen am 30.09.2024.

Barmer (2021): Gaming für die Gesundheit? Diese Auswirkungen haben Videospiele, https://www.barmer.de/gesundheit-verstehen/sport/e-sport/gaming-gesundheit-1135180 zuletzt aufgerufen am 02.09.2024.

BfDI (Die Bundesbeauftragte für Datenschutz und Informationsfreiheit) (2024): Die KI-Verordnung der EU, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/KI-Verordnung.html?nn=251928 zuletzt aufgerufen am 06.09.2024.

BMFSFJ (Bundesministerium für Familie, Frauen und Jugend) (2024): Übereinkommen über die Rechte des Kindes VN-Kinderrechtskonvention im Wortlaut mit Materialien, https://www.bmfsfj.de/resource/blob/93140/78b9572c1bffdda3345d8d393acbbfe8/uebereinkommen-ueber-die-rechte-des-kindes-data.pdf zuletzt aufgerufen 21.10.2024.

BKA (Bundeskriminalamt) (2024): Cybergrooming, https://www.bka.de/DE/UnsereAufgaben/Aufgabenbereiche/Zentralstellen/Kinderpornografie/Cybergrooming/Cybergrooming_node.html zuletzt aufgerufen am 02.09.2024.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2024): Cybermobbing und Cyberstalking, https://www.bsi.bund.de/dok/6692496 zuletzt aufgerufen 05.06.2024.

BSI (2024): Gaming – Spielregeln für digitale Sicherheit #accountschutzover9000, https://www.bsi.bund.de/dok/508842 zuletzt aufgerufen am 02.09.2024.

BSI (2024): Sichere Passwörter erstellen, https://www.bsi.bund.de/dok/6596574 zuletzt aufgerufen am 05.09.2024.

BSI (2024): Smart Toys: So nutzen Sie smarte Teddys, Autos & Co. sicher, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/Smart-Home/Smart-Toys/smart-toys.html zuletzt aufgerufen am 06.09.2024.

BSI (2024): So schützen Sie sich vor digitalem Identitätsdiebstahl und gehackten Accounts, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/Schutzmassnahmen/schutzmassnahmen_node.html zuletzt aufgerufen am 30.09.2024.

BVL (Bundesamt für Verbraucherschutz und Lebensmittelsicherheit) (2024): Spielwaren und Scherzartikel, https://www.bvl.bund.de/DE/Arbeitsbereiche/03_Verbraucherprodukte/03_AntragstellerUnternehmen/01_Spielwaren/bgs_spielwaren_node.html zuletzt aufgerufen am 18.09.2024.

BZgA (Bundeszentrale für gesundheitliche Aufklärung, Ins Netz gehen) (2024): Datenschutz für Familien – Wie Sie sich vor Datenklau schützen, https://www.ins-netz-gehen.info/eltern/internet-sicherheit-kinder/datenschutz-innerhalb-der-familie/ zuletzt aufgerufen am 27.08.2024.

BZgA (Bundeszentrale für gesundheitliche Aufklärung, Ins Netz gehen) (2024): Kostenfallen in Videospielen – Überblick für Eltern, https://www.ins-netz-gehen.info/eltern/computerspiele-kinder/kostenfallen/ zuletzt aufgerufen am 06.09.2024.

Die Bundesregierung (2024): AI-Act verabschiedet, https://www.bundesregierung.de/breg-de/themen/digitalisierung/kuenstliche-intelligenz/ai-act-2285944 zuletzt aufgerufen am 30.08.2024.

DKHW (Deutsches Kinderhilfswerk) (2018): Kinderreport Deutschland 2018, https://www.dkhw.de/fileadmin/Redaktion/1_Unsere_Arbeit/1_Schwerpunkte/2_Kinderrechte/2.2_Kinderreport_aktuell_und_aeltere/Kinderreport_2018/DKHW_Kinderreport_2018.pdf zuletzt aufgerufen am 27.08.2024.

DKHW (Deutsches Kinderhilfswerk) (2024): Kinderrechte in der digitalen Welt, https://www.dkhw.de/informieren/unsere-themen/kinder-und-medien/kinderrechte-in-der-digitalen-welt/ zuletzt aufgerufen am 27.08.2024.

DSK (Datenschutzkonferenz) (2024): Orientierungshilfe Künstliche Intelligenz und Datenschutz Version 1.0, https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

EVZ (Europäisches Verbraucherzentrum) (2021): Datenschutz und Videospiele: Welche Folgen hat die DSGVO für digitale Spiele?, https://www.evz.de/einkaufen-internet/gaming/datenschutz-und-videospiele.html zuletzt aufgerufen am 02.09.2024.

Foitzick, Klaus (2021): Wann gilt die DSGVO auch für Privatpersonen? In: activeMind.AG, https://www.activemind.de/magazin/privatpersonen/ zuletzt aufgerufen am 27.08.2024.

FSM (Freiwillige Selbstkontrolle Multimedia-Dienstanbieter) (2019): Haftung von Minderjährigen, https://www.fsm.de/en/wissen/a-bis-z/haftung-von-minderjaehrigen/ zuletzt aufgerufen am 27.08.2024.

game (Verband der deutschen Games-Branche e.V.) (2024): Gesetzlicher Rahmen – Jugendschutzgesetz, https://www.game.de/themen/jugendschutz/gesetzlicher-rahmen-jugendschutzgesetz/ zuletzt aufgerufen am 02.09.2024.

Hauser, Prof. Dr. Bernhard (2021): Digitale Spiele In: socialnet.de, https://www.socialnet.de/lexikon/Digitale-Spiele zuletzt aufgerufen am 02.09.2024.

Havighurst, R.J. (1953): Human Development and Education. David McKay, New York

Heise online (2024): Studie: Smarte Spielzeuge senden Nutzungsdaten an Hersteller, https://www.heise.de/news/Studie-Smarte-Kinderspielzeuge-haben-oft-mangelhaften-Datenschutz-9847746.html zuletzt aufgerufen am 18.09.2024.

JIM (2023): JIM-Studie: Jugend, Informationen, Medien 2023, https://www.mpfs.de/studien/jim-studie/2023/, zuletzt abgerufen 05.06.2024.

Kaspersky (2024): Wie sicher sind Smart Homes?, https://www.kaspersky.de/resource-center/threats/how-safe-is-your-smart-home zuletzt aufgerufen am 12.09.2024.

KIM (2022): KIM-Studie: Kindheit, Internet, Medien 2022, https://www.mpfs.de/studien/kim-studie/2022/ zuletzt aufgerufen am 27.08.2024.

Klicksafe (2023): Cybergrooming. Hilfe bei sexueller Belästigung von Kindern, https://www.klicksafe.de/cybergrooming zuletzt aufgerufen am 29.08.2024.

Klicksafe (2023): Was ist generative KI?, https://www.klicksafe.de/kuenstliche-intelligenz/was-ist-generative-ki zuletzt aufgerufen am 15.08.2024.

Medienkindergarten (2024): Die Rolle der Familie in der Medienerziehung https://medienkindergarten.wien/medienpaedagogik/kind-und-medien/die-rolle-der-familie-in-der-medienerziehung zuletzt abgerufen 28.10.2024.

N., Louisa (2024): Cookies: was Sie über die kleinen Dateien wissen sollten, In: datenschutz.org, https://www.datenschutz.org/cookies/ zuletzt aufgerufen am 05.09.2024.

PROJUVENTUTE (2024): Lust statt Frust mit digitalen Medien, https://www.projuventute.ch/de/eltern/medien-internet/umgang-digitalen-medien zuletzt aufgerufen am 27.08.2024.

Rausch, Felix (2023): Die verheerenden Folgen von Datenmissbrauch In: Dr. Datenschutz intersoft consultin services, https://www.dr-datenschutz.de/die-verheerenden-folgen-von-datenmissbrauch/ zuletzt aufgerufen am 05.09.2024

Schmidt, Caroline (2024): Sharenting: Kinderfotos im Netz, https://www.e-recht24.de/online-marketing/10277-sharenting-kinderfotos-im-netz.html zuletzt aufgerufen am 30.09.2024.

Statista (2024): Anteil der Nutzer von Social-Media-Plattformen nach Altersgruppen in Deutschland im Jahr 2023, https://de.statista.com/statistik/daten/studie/543605/umfrage/verteilung-der-nutzer-von-social-media-plattformen-nach-altersgruppen-in-deutschland/ zuletzt aufgerufen am 27.08.2024.

Statistisches Bundesamt (2022): Ausstattung privater Haushalt mit smarten Geräten und Systemen nach Gebietsständen, https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/Ausstattung-Gebrauchsgueter/Tabellen/a-smarte-geraete-systeme-gebietsstaende-lwr.html zuletzt aufgerufen 28.08.2024.

Telekom (2024): Nachricht von Ella, https://www.telekom.com/de/medien/medieninformationen/detail/nachricht-von-ella-without-consent-1048362 zuletzt abgerufen 21.10.2024.

UBSKM (Unabhängige Beauftragte für Fragen des sexuellen Kindesmissbrauchs) (2022): Zahlen und Fakten. Sexuelle Gewalt gegen Kinder und Jugendliche, 2022, https://beauftragte-missbrauch.de/fileadmin/user_upload/Materialien/Publikationen/Zahlen_und_Fakten/Fact_Sheet_Zahlen_und_Fakten_UBSKM-2022-01.pdf zuletzt aufgerufen 28.08.2024.

Verbraucherzentrale (2018): Soziale Medien und die DSGVO, https://www.verbraucherzentrale.de/marktbeobachtung/soziale-medien-und-die-dsgvo-41413 zuletzt aufgerufen am 27.08.2024.

Verbraucherzentrale (2023): Smartes Spielzeug: Der Spion im Kinderzimmer, https://www.verbraucherzentrale-niedersachsen.de/themen/internet-telefon/smartes-spielzeug-der-spion-im-kinderzimmer zuletzt aufgerufen am 18.09.2024.

Verbraucherzentrale (2024): Neue Handynummer? Auch in WhatsApp ändern!, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/neue-handynummer-auch-in-whatsapp-aendern-20706 zuletzt aufgerufen am 16.09.2024.

Wawrzyniak, Jessica (2020): Datenschutz als Medienkompetenz, In: digitalcourage, https://digitalcourage.de/blog/2020/datenschutz-als-medienkompetenz zuletzt aufgerufen am 27.08.2024.

Welchering, Peter (2024): Abhör-Apps für Werbezwecke:Hört mein Handy mit?, https://www.zdf.de/nachrichten/panorama/handy-sprachdaten-abhoeren-werbeanzeigen-konzerne-100.html zuletzt aufgerufen am 27.09.2024.

Wiener Bildungsserver, Medien Kindergarten (2024): Die Rolle der Familie in der Medienerziehung, https://medienkindergarten.wien/medienpaedagogik/kind-und-medien/die-rolle-der-familie-in-der-medienerziehung zuletzt aufgerufen am 27.08.2024.

Wolfer, Julia (2024): Active Listening - Personalisierte Werbung: Hört dein Handy dich wirklich ab?, https://www.prosieben.de/serien/galileo/news/personalisierte-werbung-hoert-dein-handy-dich-ab-spionage-350760 zuletzt aufgerufen am 05.09.2024.

Index

Abo-Falle

Als Abo-Falle wird eine Art des Internetbetrugs bezeichnet, bei dem häufig im Kontext einer Online-Registrierung unwissentlich ein kostenpflichtiges Abonnement abgeschlossen wird.

Ad-Blocker

Ein Ad-Blocker (engl. für Werbeblocker) ist eine Filter-Software, mit der die Einblendung von Werbung im Internet unterdrückt wird.

Admin

Ein Admin(istrator) ist eine Person, die z.B. in Messengergruppen oder bei Social Media Accounts eine übergeordnete Rolle in einer Gruppe einnimmt und mehr Rechte als normale Teilnehmende hat, wie das Hinzufügen und Löschen von Teilnehmenden oder die Aufstellung und Durchsetzung eines Verhaltenskodex.

Algorithmus

Im Bereich der Computerprogrammierung sind Algorithmen Anweisungen, die dem Computer sagen, wie und in welcher Reihenfolge er eine Aufgabe ausführen soll. Alle digitalen Anwendungen und Geräte funktionieren auf der Grundlage von Algorithmen.

App

App ist die Abkürzung für „Application Software“ und bedeutet so viel wie Anwendungssoftware. Mit diesen Zusatzprogrammen kann die Funktion digitaler Endgeräte beliebig erweitert werden.

Aufsichtsbehörde

Eine Datenschutzaufsichtsbehörde ist eine unabhängige staatliche Behörde, welche für die Überwachung und Durchsetzung der Datenschutzgesetze zuständig ist. In Deutschland gibt es in jedem Bundesland eine eigene Behörde als Ansprechpartner für Beschwerden sowie eine Bundesbeauftragte für Datenschutz.

Augmented Reality

Augmented Reality (engl. für erweiterte Realität) bezeichnet eine computerunterstützte Wahrnehmung bzw. Darstellung, welche die reale Welt mittels Einblendung/Überlagerung um virtuelle Aspekte erweitert.

Bio

Bio ist die Abkürzung für Biografie und beschreibt bei Social Media-Plattformen die Profil-Informationen in Form von Wörtern, Emojis, Hashtags oder Links, mit denen sich User anderen Usern vorstellen.

Bots

Bots (Kurzform von engl. „robots“ = Roboter) sind Computerprogramme, die Aufgaben automatisiert abarbeiten. Schädliche Bots können digitale Geräte ferngesteuert übernehmen und sie damit für einen Angriff auf Computersysteme nutzen.

Browser(verlauf)

Mit einem Webbrowser werden Webseiten im Internet dargestellt. Der Browserverlauf zeigt die Webseiten in chronologischer Reihenfolge an, die zuletzt besucht wurden. Darüber hinaus werden auch zugehörige Metadaten, wie Seitentitel und Besuchszeit, lokal gespeichert.

Bundesnetzagentur

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNA) ist als obere Bundesbehörde für alle öffentlichen Netze in Deutschland verantwortlich. Seit Inkrafttreten des Digital Services Acts verantwortet sie auch die Überwachung der dort festgeschriebenen Regeln. Wenn Internetanbieter Hinweisen über illegale Inhalte und Produkte nicht nachgehen oder bei Hass- und Falschmeldungen untätig bleiben, kann sich bei der BNA beschwert werden.

Bußgeld

Ein Bußgeld wird durch Behörden oder Gerichte verhängt, um eine Ordnungswidrigkeit zivilrechtlich zu ahnden. Davon zu unterscheiden ist die Geldstrafe, durch die im Strafrecht eine Straftat sanktioniert werden soll.

CEO Fraud

Der CEO Fraud (engl. für Chef-Betrug) ist eine Betrugsmasche, bei der Mitarbeitende eines Unternehmens via E-Mail oder Telefonat dazu gebracht werden, eine höhere Geldsumme zu überweisen. Dabei geben sich die Kriminellen authentisch als eine höhere Führungskraft aus.

Challenge

Challenge (engl. für Mutprobe oder Herausforderung) beschreibt ein auf Social Media verbreitetes Phänomen, bei dem meist Jugendliche sich einer Herausforderung stellen und dies filmen, um Likes zu gewinnen. Es gibt lustige, kreative, aber auch (lebens-)gefährliche Challenges.

Clouddienst

Unter Clouddiensten (Cloud engl. für Wolke) versteht man IT-Unternehmen, die über das Internet abrufbare Ressourcen, wie Rechenleistung, Datenspeicher oder Anwendungen, bereitstellen. Um die Verfügbarkeit zu gewährleisten, werden die zu speichernden Daten häufig auf Rechenzentren in der ganzen Welt verteilt.

Community (-Richtlinien)

Unter Community (engl. für Gemeinschaft) wird ein organisiertes, soziales Netzwerk verstanden, in dem sich Mitglieder mit einem gemeinsamen Ziel, geteilter Identität oder gemeinsamen Interessen zusammenfinden und austauschen. Der Austausch untereinander findet unter Einhaltung gemeinsamer Regeln zu den Inhalten und der Art und Weise der Kommunikation statt.

Content

Unter Content (engl. für Inhalt) werden mediale Inhalte jeglicher Art verstanden, die anhand analoger sowie digitaler Medien verbreitet werden.

Datenleck, Datenleak, Datenpanne

Bei einem Datenleck handelt es sich um einen Sicherheitsvorfall durch einen Softwarefehler oder vorsätzliches Herbeiführen, bei dem ungewollt vertrauliche Daten verlorengehen oder offengelegt werden und somit Unberechtigte Zugriff auf eine Datensammlung erhalten.

Deepfake

Der Begriff „Deepfake“ setzt sich aus „Deep Learning“ und „Fake“ (engl. für Fälschung) zusammen. Er bezeichnet realistisch wirkende Medieninhalte (Foto, Audio, Video usw.), die durch Techniken der künstlichen Intelligenz abgeändert, erzeugt bzw. verfälscht worden sind.

Drittanbietersperre

Drittanbieter sind Unternehmen, die Produkte oder Dienstleistungen auf Plattformen anbieten, die ihnen nicht selbst gehören. Eine Drittanbietersperre ist eine Funktion, welche sich beim Mobilfunkanbieter aktivieren lässt, um die Zahlung über die Mobilfunkrechnung an Dritte zu unterbinden, falls durch Werbebanner, Gewinnspiele oder Links versehentlich eine Kostenfalle ausgelöst wurde.

Duett

Unter Duett wird eine Funktion bei TikTok verstanden, in der User:innen Videos zu bestehenden TikTok-Videos aufnehmen und diese gleichzeitig, nebeneinander abspielen lassen können.

Ende-zu-Ende-Verschlüsselung

Unter Ende-zu-Ende-Verschlüsselung (engl. End-to-end encryption, EE2E) versteht man die Verschlüsselung zu übertragender Daten, um Daten vor Diebstahl und Missbrauch zu schützen. Niemand, außer dem Sender und dem Empfänger, hat mit EE2E Zugriff auf die geteilten Inhalte, auch nicht der Netzanbieter oder der Anbieter des Kommunikationsdienstes.

Enkeltrick 2.0

Beim Enkeltrick 2.0 handelt es sich um eine Betrugsmasche, bei der sich die Täter:innen via Messenger und nicht, wie früher, per Telefonanruf (Enkeltrick 1.0) als Kind oder Enkelkind ausgeben. Die Täterperson gibt an, eine neue Telefonnummer zu haben und bittet das Opfer aufgrund einer Notlage um eine Geldüberweisung.

Fake News

Fake News sind in den Medien und im Internet, besonders auf Social Media-Plattformen bzw. Kanäle, in manipulativer Absicht verbreitete Falschmeldungen. Sie sind oft politisch motiviert und dienen der Meinungsmache. Durch die professionelle Aufmachung sind sie auf den ersten Blick oft nicht zu erkennen.

Fake-Shops

Hinter einem Fake-Shop verbirgt sich eine gefälschte Internet-Verkaufs-Plattform, die mit meist sehr günstigen Schnäppchen für angeblich hochwertige Waren wirbt. Nach der Bezahlung per Vorkasse wird diese jedoch gar nicht oder nicht in der bestellten Qualität geliefert.

Feed

Unter einem Feed in sozialen Medien versteht man fortlaufende Inhalte an Texten, Bildern und Videos, die Nutzenden von Social-Media-Plattformen zentral angezeigt werden. Dies können Updates von Freunden oder Followern sowie Inhalte von Seiten oder Konten sein, denen gefolgt wird.

Firewall

Eine Firewall ist ein Sicherheitssystem, das den Datenverkehr überwacht und unerwünschte oder gefährliche Verbindungen blockiert. Es schützt das Netzwerk vor Angriffen und Bedrohungen durch Dritte und ermöglicht die sichere Nutzung des Netzwerks.

GPS – Tracking oder **Standortverfolgung**

GPS steht für „Global Positioning System“ und ist ein Satellitennavigationssystem, das es ermöglicht, den genauen Standort eines mit einem Tracker versehenen Objektes in Echtzeit via Mobilfunk, Wi-Fi oder Funkfrequenzen zu verfolgen.

Index

Identifizierbare Merkmale

Identifizierbare Merkmale einer Person sind z.B. der Name, eine Kennnummer, Standortdaten, die Telefonnummer, die Kreditkarten- oder Personalnummer, die Kontodaten, ein Kfz-Kennzeichen, das Aussehen, der Fingerabdruck, die Kundennummer oder die Anschrift.

In-App-Käufe

In-App-Käufe sind zusätzliche Inhalte, Artikel, Abonnements oder Services, die man innerhalb einer App kaufen kann. Meist sind die Apps an sich kostenlos, durch die In-App-Käufe können sie jedoch schnell zur Kostenfalle werden.

IP-Adresse

Eine IP-Adresse (Internet Protocol-Adresse) besteht aus einer Abfolge von Zahlen, die jedem Gerät zugewiesen wird, das mit einem Computernetzwerk oder dem Internet verbunden ist. Mithilfe von IP-Adressen werden Onlinegeräte, wie Computer oder Mobiltelefone, identifiziert.

Kanal

Kanäle in Telegram oder WhatsApp bieten Administrator:innen die Möglichkeit, ihre Inhalte in Form von Textnachrichten, Links zu Informationen, Bildern oder Videos mit einer großen Öffentlichkeit zu teilen. Der Beitritt zu einem Kanal, der standardmäßig nicht Ende-zu-Ende-verschlüsselt ist, erfolgt freiwillig. Dabei ist weder die Telefonnummer noch das Profilfoto für andere sichtbar.

Kettenbriefe

Kettenbriefe sind Nachrichten, die meist über Messenger verbreitet werden. Neben harmlosen und witzigen Nachrichten enthalten Kettenbriefe oft auch Betrugsversuche, Einschüchterungen, Fake News, Drohungen oder sogar Todesprophezeihungen. Bei sogenannten Horror-Kettenbriefen sollen sich die Empfänger:innen gruseln und fürchten. Sie werden dazu aufgefordert, die Nachricht an möglichst viele andere Kontakte weiterzuleiten, da ansonsten angeblich etwas Schlimmes passiert.

KI

Künstliche Intelligenz (KI) ist ein Bereich der Informatik, der sich mit der Entwicklung von Systemen beschäftigt, die menschenähnliche Intelligenz zeigen, wie z.B. das Lernen, Problemlösen und das Treffen von Entscheidungen. Diese Systeme nutzen Algorithmen und Modelle, um aus Daten zu lernen und Aufgaben autonom auszuführen.

Kinderpornografie

Um Kinderpornografie handelt es sich, wenn auf Fotos oder Videos zu sehen ist, wie sexuelle Handlungen vor oder an Kindern (unter 14 Jahren) vorgenommen werden oder wenn Kinder solche Handlungen selbst ausführen, z.B. weil sie dazu gezwungen werden. Auch Fotos oder Videos, auf denen Kinder teilweise oder ganz nackt abgebildet sind zählen zu kinderpornografischen Inhalten.

Klarname

Ein Klarname ist der Name, der in Ausweisdokumenten steht. Er setzt sich aus mindestens einem Vornamen sowie dem Familiennamen zusammen.

Leak bzw. **leaken**

Bei einem Leak (engl. für Leck bzw. undicht) gelangen nicht autorisierte Inhalte durch gewollte bzw. gezielte Offenlegung an die Öffentlichkeit, die eigentlich vertraulich sind.

Let‘s Plays

Bei einem Let’s Play (engl. für „Lasst uns spielen“) können Zuschauende über eine witzige oder spannend kommentierte Videoaufnahme (Screencast) an dem Spielerlebnis anderer Personen teilhaben. Die Let‘s Player werden dabei via „Facecam” in einer kleinen Ecke eingeblendet.

Likes

Unter einem Like (engl. für gefallen) versteht man eine zustimmende, positive Bewertung eines Beitrags in einem sozialen Netzwerk. Durch Zählung von Likes können User:innen ablesen, wie gut ein geposteter Beitrag ankommt.

Malware

Malware (von „malicious software“, engl. für Schadprogramm) bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meist schädliche Funktionen auf einem IT-System auszuführen. Sie verbreiten sich über E-Mail-Anhänge, manipulierte Webseiten oder Datenträger.

Metadaten

Metadaten sind übergeordnete Informationen, die etwas über andere Daten sagen. Diese werden an eine Datei angehängt, wie z.B. der Dateiname, das Erstellungsdatum, die Datei- oder Bildgröße oder auch Geodaten. Aber auch Informationen, wie die IP-Adresse oder die Information, wer wann mit wem kommuniziert hat, gehören zu den Metadaten.

Nickname

Ein Nickname (engl. für Spitzname) wird benötigt, um sich bei Onlinediensten, Messengern, in (Chat-)Foren oder auf Plattformen anzumelden. Er erleichtert die schnelle und anonyme Kommunikation online, ohne persönliche Daten preiszugeben.

Passwortmanager

Ein Passwortmanager generiert, speichert und verwaltet komplexe Passwörter für verschiedene Onlinekonten sicher und zugänglich. Mit einem sicheren Masterpasswort wird der Zugriff auf die gespeicherten komplexen Passwörter gewährleistet.

Phishing

Mit Phishing (von fishing, engl. für angeln) bezeichnet man einen Cyberangriff, bei dem betrügerische E-Mails, Textnachrichten, Telefonanrufe oder gefälschte Websites eingesetzt werden, um Menschen dazu zu verleiten, Malware herunterzuladen oder sensible Daten weiterzugeben. Diese werden anschließend meist für illegale Zwecke genutzt.

Prank

Ein Prank (engl. für Streich) bezeichnet das absichtliche Hereinlegen einer Person, um diese zu ärgern, zu provozieren oder zu erschrecken. Auf Social Media sind Pranks deswegen bekannt, da die Vorbereitung und die Reaktionen der Opfer gefilmt und hochgeladen werden.

Prompts

Unter einem Prompt versteht man eine in natürlicher Sprache formulierte Aufforderung an eine KI, eine Antwort abzugeben. Dieser wird von der KI analysiert, um basierend auf dem vorherigen Training und dem Muster, das aus den Trainingsdaten gelernt wurde, eine Antwort zu erzeugen.

Prozessor

Ein Prozessor (CPU) ist ein Mikrochip, der für die Ausführung von Berechnungen und die Verarbeitung von Daten zuständig ist. Als zentrale Recheneinheit übernimmt er die Steuerung und Koordination aller Abläufe im System.

Pseudonym(isieren)

Durch Pseudonymisierung können personenbezogene Daten geschützt werden. Pseudonymisierung, im Gegensatz zur Anonymisierung, bedeutet, dass Personen durch zusätzliche Informationen, die als Schlüssel fungieren, weiterhin identifiziert werden können.

Push-Nachrichten

Eine Push-Benachrichtigung ist eine Meldung, die von einer Mobiltelefon-App generiert wird, wenn die App nicht geöffnet ist. Sie wird angezeigt, um auf eine neue Nachricht, ein Update oder ein Werbeangebot aufmerksam zu machen.

Reichweite

Reichweite auf Social Media ist eine Kennzahl dafür, wie viele Einzelpersonen einen Beitrag mindestens einmal gesehen haben. Davon zu unterscheiden ist die „bezahlte Reichweite“, also die Anzahl der Personen, auf deren Bildschirmen bezahlte Beiträge angezeigt wurden.

Router(konfiguration)

Ein Router ist ein Hardwaregerät, das als Verbindungspunkt zwischen einem lokalen Netzwerk (z.B. zu Hause) und dem physischen Internetanschluss an der Wand/Dose dient.
Bei der Routerkonfiguration geht es darum, einen Router einzurichten und anzupassen , um optimale Netzwerkleistung, Sicherheit und Funktionalität zu gewährleisten.

Skins & Outfits

Ein Skin (engl. für Haut) im Online-Games, wie z.B: Fortnite ist eine kosmetische Anpassung für Charaktere oder für im Spiel vorkommende Gegenstände. Outfits werden als Skins bezeichnet, mit denen der eigene Spielcharakter angepasst werden kann.

Scoring

Unter Scoring (engl. für Wertung) wird die Abschätzung der Wahrscheinlichkeit über ein bestimmtes zukünftiges Verhalten einer natürlichen Person verstanden, um zu entscheiden, ob mit dieser Person ein Vertragsverhältnis eingegangen werden kann. Am bekanntesten ist das Kreditscoring zur Abschätzung der Kreditwürdigkeit (Bonität) einer Person.

Screenshot

Ein Screenshot (engl. für Bildschirmfoto) ist eine Aufnahme des Bildschirms, keine Fotografie. Er dient als Beweis, Gedächtnisstütze, Anleitung oder zum Teilen interessanter Inhalte und kann als Bilddatei in niedriger Auflösung abgespeichert werden.

Sexting

Das Wort „Sexting“ setzt sich aus den Wörtern „Sex“ und „texting“ (engl. für „Nachrichten verschicken“) zusammen und beschreibt den Vorgang, wenn Personen sich gegenseitig online erotische Nachrichten, Fotos oder Videos zuschicken.

Index

Sharenting

„Sharenting“ ist ein Begriff, der sich aus den Wörtern „sharing“ (engl. für teilen) und „parenting“ (engl. für Elternschaft) zusammensetzt. Er bezieht sich auf den Trend, dass Eltern Bilder, Videos oder Informationen über die eigenen Kinder in sozialen Medien teilen.

Sicherheitsfeatures

Sicherheitsfeatures sind Funktionen, die riskante Sicherheitslücken in der IT reduzieren oder schließen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Benutzer-, Anwendungs-, Geräte- und Netzwerkinformationen sowie physischen Ressourcen zu gewährleisten.

Social Engineering

Beim Social Engineering (engl. für soziale Manipulation) werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität von Cyberkriminellen ausgenutzt, um Personen so zu manipulieren, dass vertrauliche Informationen preisgegeben, Sicherheitsfunktionen ausgehebelt, Überweisungen getätigt werden oder Schadsoftware installiert wird.

Sprachassistent

Sprachassistenten funktionieren mithilfe von Künstlicher Intelligenz, die es ermöglicht, mit elektronischen Geräten und Anwendungen in Interaktion zu treten. Durch das permanente Abhören der Umgebung, kann ein Sprachassistent nach Aktivierung durch ein Schlüsselwort auf einen entsprechenden Sprachbefehl reagieren.

Standortfreigabe

Die Standortfreigabe ist eine GPS-basierte Funktion des Smartphones, die es Apps ermöglicht zu erkennen, wo sich der Nutzende des Smartphones gerade aufhält, um ihn bspw. zu navigieren oder zu orten. Über einen Messenger kann der aktuelle Standort einer anderen Person oder Gruppe für eine bestimmte Zeit live geteilt werden.

Story

Stories (engl. für Geschichten) bezeichnen im Social Media-Bereich kurze, hintereinander ablaufende Video- oder Bildsequenzen, die als mediale Statusmeldungen benutzt werden und nur für 24 Stunden verfügbar sind. Durch Emojis, Text, Musik, Sticker usw. können Stories kreativ erweitert werden.

Tool

Unter einem Tool (engl. für Werkzeug) versteht man ein Hilfsprogramm von geringem Umfang, welches zusätzliche Aufgaben für ein bestimmtes Betriebssystem oder Anwendungsprogramm übernimmt.

Tracking

Tracking (engl. für folgen) bezeichnet die Verfolgung, Aufzeichnung und anschließende Auswertung des Nutzerverhaltens im Internet. Dabei ist für Webseitenbetreiber interessant, über welche Websites ein Besucher auf die eigene Website gekommen ist, wie lange sich eine Person auf der Website aufhielt, welche Seiten danach aufgerufen wurden und welche IP-Adresse sie hat.

Urheberrecht

Das Urheberrecht schützt kreative Leistungen, insbesondere im Bereich von Kultur und Kunst. Es regelt die wirtschaftliche Verwertung der kreativen Inhalte, insbesondere über Lizenzen oder gesetzliche Nutzungserlaubnisse. Bei Social Media spielt das Vervielfältigungsrecht und das Recht der öffentlichen Wiedergabe eine zentrale Rolle.

USK

Die USK (Unterhaltungssoftware Selbstkontrolle) ist die offizielle Stelle in Deutschland, die prüft, ob Spiele für bestimmte Altersgruppen geeignet sind und ordnet sie in verschiedene Alterskategorien ein. Diese Alterskennzeichen sollen dabei helfen, die Angemessenheit eines Spiels für Kinder und Jugendliche einzuschätzen.

Views

View (engl. für Ansicht) bezeichnet die Anzahl der Aufrufe eines veröffentlichten Inhalts. Zu unterscheiden sind Story-Views, Webseiten-Views und Video-Views. Wobei letztere entweder erst ab einer vorher definierten Ansichtsdauer gezählt werden oder aber sobald das Video gelikt, geteilt, kommentiert, oder dem Account gefolgt wird. Je mehr Views ein Beitrag hat, desto größer ist in der Regel die Reichweite und der Verdienst.

Voice Monitoring

Voice Monitoring (engl. für Stimm-Überwachung) bezeichnet die Abhörfunktion eines smarten Gerätes, wie z.B. einer Smartwatch. Das Mikrofon kann in diesem Fall entweder per App oder per SMS-Befehl aus der Ferne aktiviert werden, so dass alle Stimmen und Geräusche im Umfeld unerkannt mitgehört werden können.

Zwei-Faktor-Authentisierung
(oder **2-Faktor-Authentifizierung)**

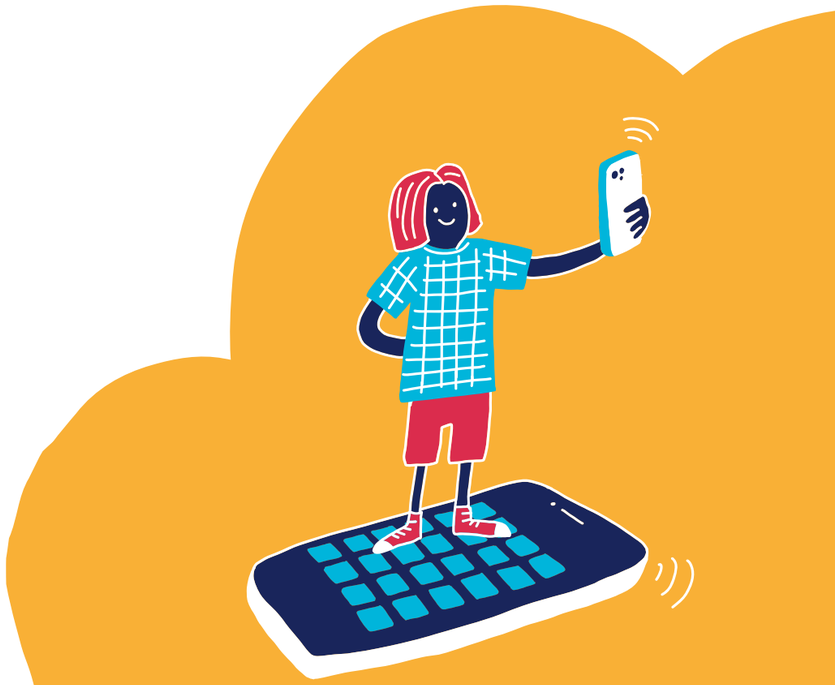
Bei der Zwei-Faktor-Authentisierung (2FA) gibt es für den Identitätsnachweis des Nutzenden zusätzlich zum Passwort noch einen zweiten, davon unabhängigen Faktor, über den die Anmeldung zu einem Konto erfolgen muss. Auf diesem unabhängigen Weg, z.B. über SMS, eine App u.ä. wird verhindert, dass unbefugte Dritte Zugang zu Nutzerdaten oder Funktionen erhalten, nur weil sie in den Besitz des Passworts gelangt sind.

Danksagung

Wir bedanken uns herzlich bei allen Beteiligten, die das Projekt **#DigitaleVorbilder – Familien gehen online.** möglich gemacht haben. Ein besonderer Dank gilt den teilnehmenden Familien, die ihre Erfahrungen und Einblicke geteilt haben, sowie den Expert:innen, die mit ihrem Wissen und ihrer Unterstützung wesentlich zum Erfolg des Projekts beigetragen haben.

Unser Dank gilt auch unseren Partner:innen, Beiratsmitgliedern und Kolleg:innen, die uns mit ihrer tatkräftigen Hilfe und ihrem Vertrauen begleitet haben. Ein besonderer Dank geht an die Europäische Union, die das Projekt finanziell gefördert und damit maßgeblich unterstützt hat. Gemeinsam konnten wir wertvolle Impulse für den digitalen Familienalltag setzen.

Vielen Dank an alle, die dieses Projekt unterstützt haben!



Impressum

Titel:
Orientierungshilfe Datenschutz: Ein Familien-Guide für den digitalen Dschungel (1. Auflage, Oktober 2024)

Herausgegeben von:
Die Orientierungshilfe Datenschutz wurde vom EU-Projekt #DigitaleVorbilder – Familien gehen online. (www.digitale-vorbilder.eu) erstellt.

Ein Gemeinschaftsprojekt von:
Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
Werderstraße 74A, 19055 Schwerin
Tel. +49 385 59494-0
E-Mail: info@datenschutz-mv.de
Web: www.datenschutz-mv.de

und

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Straße 22, 20459 Hamburg
Tel. +49 40 428 54 40 40
E-Mail: mailbox@datenschutz.hamburg.de
Web: www.datenschutz-hamburg.de

Redaktion: Lydia Roth, Christina Münster, Isabel Schlosshauer, Antje Kaiser
Titelcover und Grafiken: Eli Breuing
Fotorechte: Sebastian Schmidt: EckiRaff | Thomas Fuchs: Bildwerkstatt-Nienstedten
Layout: Caro Günther (Caros Colors)
Druck: WIRmachenDRUCK

Download und Bestellung:
Die Orientierungshilfe kann unter dem folgenden Link heruntergeladen werden: https://datenschutz-hamburg.de/digitalevorbilder/mediathek.
Neben der deutschen Version steht sie auch in den Sprachen **Englisch**, **Französisch** und **Spanisch** zum Download zur Verfügung.
Für eine Bestellung wenden Sie sich bitte an die jeweilige Aufsichtsbehörde in Mecklenburg-Vorpommern oder Hamburg (siehe oben Kontaktdaten)

Es wird darauf hingewiesen, dass alle Angaben trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der Herausgebenden ausgeschlossen ist.

Die Broschüre ist ein Produkt des Projektes #DigitaleVorbilder – Familien gehen online. Finanziert aus dem Programm „Citizens, Equality, Rights and Values“ (CERV) der Europäischen Union.

Die Veröffentlichung steht unter der Creative-Commons-Lizenz „Namensnennung – keine kommerzielle Nutzung – keine Bearbeitung 3.0 Deutschland“ (byncnd), das heißt sie kann bei Angabe der Herausgebenden #DigitaleVorbilder in unveränderter Fassung zu nicht kommerziellen Zwecken beliebig vervielfältigt, verbreitet und öffentlich wiedergegeben werden. Der Lizenztext kann abgerufen werden unter: https://creativecommons.org/licenses/by-nc-nd/3.0/de.

https://digitale-vorbilder.eu/

#DigitaleVorbilder ist ein Gemeinschaftsprojekt von:

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Landesbeauftragte für DATENSCHUTZ und INFORMATIONSFREIHEIT Mecklenburg-Vorpommern

Finanziert von der Europäischen Union

in Kooperation mit TIDE



Finanziert von der
Europäischen Union