

#DigitaleVorbilder
Familien gehen online.

Guide d'orientation Protection des données :

Un guide destiné aux familles pour se repérer dans la jungle numérique

Scannez le code QR et consultez, en plus de la brochure, nos supports éducatifs tels que des vidéos, des enregistrements graphiques, des clips vidéos et bien plus encore.

L'« Aide à l'orientation sur la protection des données » élaborée ici traite des thèmes généraux de l'éducation aux médias et de la sensibilisation à la protection des données pour les familles résidant dans le champ d'application du RGPD de l'UE. La classification juridique dans la section thématique « Ces droits sont également valables en ligne » est effectuée du point de vue de l'Allemagne, pays d'exécution du projet. Outre les droits de l'enfant de l'ONU reconnus au niveau international et les droits généraux de la personnalité, les lois exclusivement en vigueur en Allemagne, telles que la Loi fondamentale allemande (GG), le Code pénal allemand (StGB) et les lois allemandes sur la protection des mineurs, jouent un rôle important. En outre, les liens conseillés se rapportent exclusivement à des sites web en langue allemande, que l'équipe de projet recommande à la fin de chaque chapitre pour une recherche plus approfondie.

Avant-propos

Quel est le rapport entre la protection des données et la formation et l'éducation aux médias ? Dans notre monde numérisé, il est de plus en plus difficile de savoir où subsistent des traces de données. C'est compliqué pour les adultes, mais ça l'est davantage pour les enfants et les adolescents. C'est pourquoi nous, les Délégués à la protection des données du Mecklembourg-Poméranie occidentale (LfDI MV) et de Hambourg (HmbBfDI), avons lancé le projet financé par l'UE **#DigitaleVorbilder – Familien gehen online.**. Ce projet a pour but d'aider les familles à éduquer activement leurs enfants aux médias.

« Les autorités de protection des données ont, en plus de leur rôle de surveillance, la mission légale de sensibiliser le public aux risques, réglementations, garanties et droits liés au traitement des données et de l'informer à ce sujet. Une attention particulière est accordée aux mesures spécifiques pour les enfants ; » (article 57, paragraphe 1, point b) du RGPD). C'est pourquoi nous proposons depuis longtemps déjà à Hambourg et dans le Mecklembourg-Poméranie occidentale des offres d'éducation aux médias et de sensibilisation à la protection des données pour les enfants et les adolescents ainsi que pour le personnel pédagogique. Dans le cadre de notre **projet européen**, nous nous adressons maintenant à un nouveau groupe cible : **les familles**.

Nous pensons que la sensibilisation à la protection des données et les compétences numériques sont des connaissances nécessaires. Nous sommes conscients que les médias numériques et les applications sont devenus incontournables dans le quotidien des familles.

Nous sommes convaincus que les enfants et les adolescents doivent connaître les avantages et les inconvénients de l'utilisation des médias numériques afin s'exprimer librement **en toute sécurité et de manière autonome** et d'évoluer dans notre société numérique.

Avec notre projet européen **#DigitaleVorbilder**, nous avons fait intervenir de nombreux spécialistes pour leur demander des conseils et des astuces. Vous trouverez toutes ces connaissances spécialisées sur notre site web www.digitale-vorbilder.eu et dans cette brochure.
Nous vous souhaitons beaucoup de plaisir à lire, à parcourir et à partager cette documentation, car nous sommes tous des **des #DigitaleVorbilder** pour nos enfants et nos jeunes !

Bien cordialement,
Thomas Fuchs et Sebastian Schmidt



Thomas Fuchs
Le Délégué hambourgeois à la protection des données et à la liberté d'information



Sebastian Schmidt
Le Délégué à la protection des données et à la liberté d'information du Land Mecklembourg-Poméranie occidentale

Table des matières

1 Avant-propos 1

2 Table des matières 2

3 Que signifie #DigitaleVorbilder ? 3-4
Présentation du projet & Ce que dit l'équipe du projet

4 Thèmes 5-71

4.1 Introduction à la protection des données 5-7
4.2 Les plus grands mythes sur la protection des données 8-13
4.3 Droits, devoirs et responsabilité au sein de l'espace numérique 14-19
4.4 Photos d'enfants sur Internet 20-25
4.5 TikTok, Insta, Snapchat & Co 26-31
4.6 Utilisation des médias dans la famille 32-37
4.7 Gaming : jouer en toute sécurité 38-43
4.8 Cyberharcèlement 44-49
4.9 Lieu du crime, Internet - cybergrooming 50-55
4.10 Smart Family 56-61
4.11 Jouets intelligents 62-67
4.12 Aparté : Services de messagerie 68-71

5 Bibliographie 72-73
Sources pour lecture complémentaire

6 Index 74-78
Tous les termes importants expliqués en bref

7 Remerciements 79

8 Mentions légales 80

Présentation du projet

Qui sommes-nous ?

#DigitaleVorbilder – Familien gehen online. est un projet commun du délégué à la protection des données et à la liberté d'information du Land de Mecklembourg-Poméranie occidentale (LfDI MV) et du délégué hambourgeois à la protection des données et à la liberté d'information (HmbBfDI), en partenariat avec la chaîne citoyenne TIDE de Hambourg. Il est financé par le programme « Citoyens, Égalité, Droits et Valeurs » (CERV) de l'Union européenne pour la période 11/2022-10/2024.

Une équipe de cinq personnes motivées et engagées plus que jamais, issues des domaines de la pédagogie sociale, de la sociologie, des sciences sociales, de la communication et des médias, a donné vie au projet **#DigitaleVorbilder** au-delà des frontières régionales.

Ce que nous voulons

Nous souhaitons rendre le thème de la protection des données plus tangible et compréhensible pour les familles. Notre objectif est de sensibiliser les familles à l'environnement numérique de leurs enfants et aux nouvelles technologies, leur montrer comment protéger leur vie privée et utiliser les médias en toute sécurité avec leurs enfants et les inciter à réfléchir à leur propre usage des médias.

Tous les thèmes que nous avons jugés importants pour le quotidien des familles en matière de médias numériques sont abordés : des jouets intelligents aux droits et obligations au sein de l'espace numérique, en passant par les jeux ou les réseaux sociaux.

De quoi traite cette brochure

Avec ce guide, nous souhaitons fournir des informations condensées d'un seul coup d'œil, complétées par des graphic recordings attrayants. Les graphiques sont basés sur les enregistrements des webinaires correspondant aux chapitres.

Après une introduction générale sur la protection des données et l'éclaircissement de quelques mythes assez répandus sur ce sujet, nous avons répondu aux questions suivantes dans chaque chapitre :

- En quoi le thème choisi est-il pertinent pour les familles ?
- Quel est le rapport concret entre ce thème et la protection des données ?
- Quels sont les droits concernés par ce sujet, qui doivent également être respectés sur Internet ?
- Quels conseils préventifs et quels conseils d'urgence pouvons-nous donner aux parents ?

Nous souhaitons que cette brochure permette d'être un **#DigitaleVorbilder** dans l'utilisation des médias, aussi bien dans la vie privée que professionnelle. La brochure a également été traduite dans d'autres langues et peut être téléchargée sur notre site **www.digitale-vorbilder.eu**.

L'équipe du projet vous souhaite une bonne lecture et des découvertes éclairantes

Antje, Alina, Christina, Isabel et Lydia

C’est ce que dit l’équipe de projet :

Alina
Les enfants grandissent aujourd’hui dans un monde numérisé et devraient donc apprendre très tôt à utiliser les médias numériques de manière compétente et responsable. Le projet **#DigitaleVorbilder** a démontré avec brio que le thème de la protection des données reste très pertinent et préoccupe de nombreuses familles. Je suis très heureuse de l’accueil qui nous a été réservé au cours des deux dernières années. Une chose est sûre : **#DigitaleVorbilder** n’en est qu’à ses débuts et il reste encore beaucoup à faire !

Antje
Avec le projet **#DigitaleVorbilder**, nous voulons nous adresser spécialement aux familles et les sensibiliser à l’éducation aux médias et au thème de la protection des données pour elles-mêmes et leurs enfants. Ce sont nous, les adultes, qui avons créé ce monde des médias, et non les enfants. Ainsi, il est également de notre responsabilité de transmettre aux enfants et aux jeunes les compétences nécessaires et une compréhension des valeurs médiatiques. De nombreux parents craignent cette confrontation. Notre projet a toutefois montré que l’intérêt est là lorsque le contenu est bien présenté, comme dans notre projet.



Christina :
Ce ne sont pas seulement les parents, mais toute la société qui doit montrer l’exemple. En effet, même dans l’espace numérique, les droits de la personnalité de chacun doivent être préservés par une cohabitation respectueuse. Cela commence par le respect de sa propre sphère privée en faisant attention à ses propres données !

Isabel
À l’ère du numérique, la protection des données personnelles revêt une grande importance, en particulier pour les enfants. Il est important que nous nous assurions, en tant que société, que la protection des données ne soit pas seulement un slogan, mais une réalité vécue. Dans ce contexte, nous nous devons d’agir en tant que modèle numérique et assumer la responsabilité d’une utilisation sûre des données.

Lydia
L’utilisation sûre des médias numériques peut être un élément fédérateur. C’est ce que j’ai constaté dans le cadre de **#DigitaleVorbilder**. La majorité des parents craignent que leurs enfants divulguent trop d’informations sur Internet ou soient approchés par des personnes inconnues. J’ai vu beaucoup de parents avides de connaissances et reconnaissants pour les conseils qu’ils reçoivent. Quelle joie de voir que nos vidéos, nos enregistrements graphiques et cette brochure pourront être utilisés encore longtemps et que davantage de familles pourront se pencher sur ce sujet important.

PROTECTION DES DONNÉES POUR LES FAMILLES

Ce chapitre introductif vise à créer une compréhension de base du thème de la protection des données. Pour que les chapitres suivants soient compréhensibles et clairs, il est important d’acquérir des connaissances de base. Les deux pages suivantes expliquent les principes et les termes courants de la législation sur la protection des données.

QU’ENTEND-ON PAR PROTECTION DES DONNÉES ?

Lorsque nous parlons de protection des données, nous entendons la **Protection de la vie privée**. Toute personne physique peut décider elle-même de la divulgation et de l’utilisation de ses données à caractère personnel. Cela permettra également de protéger le **Droit à l’autodétermination en matière d’information** appelé droit à la vie privée.



Que sont les données à caractère personnel ?
Il s’agit de toutes les informations permettant d’identifier **une personne vivante est identifiée**, par exemple :

- coordonnées (nom,adresse, numéro de téléphone, e-mail)
- données de localisation
- informations sur les préférences et les intérêts
- qui communique avec qui et pendant combien de temps
- le comportement d’achat
- le type de terminal

Il existe aussi des **données particulièrement sensibles** qui bénéficient d’une **protection particulière**. Il s’agit d’informations sur :

- l’origine ethnique et culturelle
- les opinions politiques, religieuses et philosophiques
- **la santé**
- **la sexualité**
- **l’appartenance à un syndicat**

LE GUIDE EUROPÉEN DE LA PROTECTION DES DONNÉES :

Le guide pour la circulation des données en Europe est le **Règlement général sur la protection des données**, ou **RGPD**.

Les entreprises et les institutions publiques, comme les écoles ou les administrations (appelés **responsables** selon le RGPD), doivent se conformer au RGPD dès que des données de personnes (appelées **personnes concernées** selon le RGPD) sont collectées.

Le RGPD ne s'applique toutefois pas lorsque les données à caractère personnel **sont utilisées exclusivement pour des activités familiales et personnelles**. Celles-ci relèvent du « **privilège domestique** », comme par exemple la correspondance privée, le carnet d'adresses, les listes de contacts personnels, les photos de vacances et les enregistrements privés d'amis et de famille.

En Allemagne, le RGPD est complété par la loi fédérale sur la protection des données (BDSG), les lois des Länder sur la protection des données ainsi que d'autres lois spéciales, comme par exemple la loi sur les écoles, la loi sur la promotion de la garde d'enfants.

LES PRINCIPES DU RGPD :

Sept **principes** déterminent la manière dont les données à caractère personnel peuvent être utilisées.

Ceux-ci visent à garantir que les données personnelles sont traitées avec soin et de manière responsable. Ils constituent la base des **droits des personnes concernées**, auxquels les consommateurs peuvent se référer.

1. Légalité

La **légalité** stipule que le traitement des données à caractère personnel est en principe interdit. Il existe une exception lorsqu'il s'agit de **bases légales** applicables, comme des contrats d'achat ou de traitement, des lois scolaires, ou des consentements pour recevoir une newsletter.

2. Transparence

Le RGPD exige des entreprises, des autorités et d'autres organismes de **la transparence**. S'ils souhaitent traiter des données, ils doivent donc respecter leur **obligation d'information**, d'où l'existence des **déclarations de confidentialité**, des **bannières de cookies** et des **avis de surveillance par caméra** dans les espaces publics.

Les personnes dont les données sont traitées disposent, grâce au principe de transparence, d'un **droit d'accès**. Cela signifie qu'elles peuvent demander aux entreprises et aux autorités quelles données sont traitées par elles et dans quel but, à qui ces données sont éventuellement transmises et pendant combien de temps elles sont conservées. Elles peuvent également être informées de la source de ces données et de la question de savoir si elles sont traitées automatiquement, par exemple avec une IA. Les autorités responsables sont tenues de répondre à ces questions dans un délai d'un mois.

Les principaux droits des personnes concernées sont :

- **Droit à l'information**
- **Droit de rectification** si des données erronées circulent
- **Droit à la limitation** du traitement (comme une 'pause' dans le traitement des données)
- **Droit à l'effacement** si les données ne sont plus nécessaires à l'exécution d'un contrat ou à des obligations de conservation prescrites par la loi, comme par exemple en droit fiscal
- **Droit de retirer un consentement** avec effet pour l'avenir
- **Droit de déposer une plainte** auprès de l'autorité de surveillance compétente

3. Limitation de la finalité

Le principe de **limitation de la finalité** signifie que les responsables ne peuvent utiliser les données que pour un objectif spécifique, préalablement communiqué. Par exemple, les données de contact demandées à la suite d'une commande ou pour l'inscription à un cours ne peuvent pas être utilisées pour contacter des personnes à des fins publicitaires ou pour leur envoyer un bulletin d'information. Sauf si l'on a donné son accord dès l'inscription. L'accord donné par le spécialiste pour la transmission de résultats au médecin de famille ne signifie donc pas automatiquement que ces données peuvent également être transmises à un institut de recherche médicale.

Si les personnes concernées estiment que leurs données ont été transmises illégalement, elles peuvent s'adresser à l'**Autorité de contrôle de la protection des données**.

4. Minimisation des données

En plus de la limitation de la finalité, la réduction des données, ou **minimisation des données**, est un autre principe important du RGPD. Cela signifie que seules les données réellement nécessaires à une opération prédéfinie peuvent être consultées et traitées. Par exemple, il n'est pas important de connaître la religion d'une personne pour s'inscrire dans une auto-école. Ce genre d'information ne doit pas être demandé uniquement parce que l'auto-école souhaite, par exemple, réaliser des statistiques internes à ce sujet.

5. Exactitude

Le principe d'exactitude stipule que les données stockées doivent être **exactes et à jour**. Si ce n'est pas le cas, les personnes concernées peuvent exiger qu'elles soient rectifiées ou, le cas échéant, effacées.

6. Limitation de la conservation des données

Les données à caractère personnel enregistrées ne peuvent être conservées que pendant la durée nécessaire à la finalité préalablement définie et aux obligations légales qui en découlent. C'est pourquoi les responsables du traitement des données doivent mettre en place une un **concept de suppression**. Si, pour certaines raisons, les données ne peuvent pas encore être entièrement supprimées, il faut en être informé.

7. Sécurité des données

Les personnes concernées doivent pouvoir compter sur le fait que les données collectées pour un objectif nécessaire seront traitées de manière **confidentielle** par les responsables et **protégées contre tout accès non autorisé**. Pour garantir cela, les institutions doivent mettre en œuvre des mesures techniques et organisationnelles, comme un système de verrouillage, des formations sur la protection des données et des mots de passe sécurisés pour les dispositifs techniques.

SUGGESTIONS DE LIENS

Portail d'information multimédia pour les consommateurs sur le RGPD

↗ https://deinedatendeinerechte.de/

Informations du BlnBDI sur le RGPD adaptées aux enfants

↗ https://data-kids.de/

LES PLUS GRANDS MYTHES SUR LA PROTECTION DES DONNÉES

– Des arguments pour la vie quotidienne



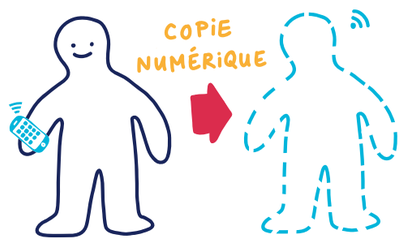
Nous vivons dans un monde où l'information est disponible en permanence et peut-être consultée de n'importe où grâce à Internet. Pour que nous puissions utiliser ces informations, applications et services, il est souvent nécessaire de s'inscrire ou de s'enregistrer. Nos données sont ainsi rapidement propagées dans le monde entier. Il nous est souvent difficile de savoir qui peut accéder à ces informations et données en ligne, et de garder une vue d'ensemble de nos traces de données. Les fuites de données peuvent engendrer des dommages imprévisibles.

MYTHE 1 : JE N'AI RIEN À CACHER ET JE N'AI PAS À ME SOUCIER DE LA PROTECTION DES DONNÉES.

Faux ! L'utilisation abusive de données qui se retrouvent sur Internet, volontairement ou par accident, peut entraîner des dommages personnels considérables.
Il est difficile d'avoir une vue d'ensemble des conséquences que peut avoir un manque de protection des données, car le danger semble abstrait. C'est pourquoi il est important de comprendre les risques **et de savoir les évaluer.**

Conséquences possibles d'une utilisation abusive des données

1. **Atteinte à la vie privée**, comme par le suivi de la localisation, la révélation de données personnelles, des fonctionnalités d'espionnage ou des chats non sécurisés.



2. **Création de profils** à partir des données saisies et du croisement de données provenant de différentes sources, afin d'afficher des contenus et publicités ciblés
3. **Atteinte au droit fondamental au libre développement de la personnalité** à cause de la sensation de surveillance ou d'évaluation
4. **Transmission opaque de données**, par exemple à des agences publicitaires ou des services de renseignement
5. **Manipulation des décisions d'achat, voire des décisions électorales** par le Suivi et la publicité personnalisée
6. **Vol ou fraude d'identité,** permettant à des criminels d'effectuer des achats ou de conclure des contrats sous le nom d'autrui. Les infractions courantes liées à la fraude identitaire incluent le truc des grands-parents version 2.0, la fraude au CEO et l'extorsion sexuelle (sextortion).
7. **Discrimination en raison, par exemple, de l'origine, des convictions personnelles ou des préférences**
8. **Atteinte à la réputation, désavantages économiques ou sociaux** jusqu'à la mise en danger de l'existence
9. **Évaluation par score :** Évaluation des performances professionnelles, de la situation économique, de la santé, des préférences et des intérêts personnels
10. **Perte de la confidentialité des secrets professionnels**

MYTHE 2 : LES BANNIÈRES DE COOKIE, C'EST VRAIMENT TROP COMPLIQUÉ ! IL SUFFIT DE TOUT ACCEPTER ET C'EST TOUT !

Faux ! Pour comprendre pourquoi ces bannières de cookies existent et comment elles nous aident, il convient tout d'abord d'expliquer ce que sont les cookies et quelle est leur fonction.

Qu'est-ce qu'un cookie ?

Les cookies sont des informations stockées dans le navigateur Internet d'un utilisateur lors de la visite d'un site web, afin de pouvoir l'identifier ultérieurement. Ils sont placés directement par l'exploitant du site web ou par des tiers intégrés à l'offre du site.

Cookies nécessaires

Certains cookies sont nécessaires pour permettre des fonctions importantes d'un site web. Ces cookies enregistrent par exemple des données de connexion, le contenu d'un panier d'achat ou aident à garantir la sécurité. Cela présente également un avantage pour l'utilisateur du site, car des informations comme la langue, les données saisies dans les champs (informations personnelles, compte utilisateur, adresse e-mail) ou les suggestions de produits personnalisées peuvent être sauvegardées.

Cookies non nécessaires

D'autres cookies ne sont en revanche pas nécessaires au fonctionnement du site. Il s'agit notamment des cookies des annonceurs, des services de suivi et d'analyse, appelés cookies tiers. Ceux-ci sont utilisés pour suivre le comportement des utilisateurs et établir des profils détaillés de ces derniers.

La question de savoir s'il faut autoriser ou non l'installation de cookies non nécessaires dépend de ce qui est important pour chaque individu.
En tant que parents modèles, il convient toutefois de veiller à ce que son propre usage d'Internet respecte la protection des données, même si ce n'est pas toujours la manière la plus simple et la plus pratique.

Conseil 1 : L'extension de navigateur **Lightbeam** pour Mozilla Firefox et Chrome montre visuellement comment le comportement des utilisateurs est suivi à l'aide de cookies tiers.

Conseil 2 : Les cookies peuvent persister pendant de nombreuses années. La suppression régulière de l'historique du navigateur et des cookies enregistrés dans les paramètres, ainsi que l'utilisation du mode privé ou de paramètres de suivi stricts, rendent plus difficile la création d'un profil utilisateur.

Obligation de consentement pour les cookies non nécessaires

Ces cookies ne peuvent être utilisés **qu'avec le consentement de l'utilisateur**. Les exploitants de sites web sont tenus d'indiquer quels cookies sont utilisés à l'aide de la bannière des cookies. Ils demandent également si, en plus de ceux qui sont techniquement nécessaires, d'autres, cookies **non** nécessaires peuvent être placés.

Pourquoi « accepter tous » n'est pas le meilleur choix ?

Pour protéger sa vie privée et limiter ses traces numériques en ligne, il est conseillé de cliquer sur le **bouton « Refuser »** dans les bannières de cookies ou d'examiner les cookies spécifiques et de les sélectionner individuellement. Les **cookies de suivi** permettent d'enregistrer le **comportement des utilisateurs sur les sites web** : Qu'est-ce qui est regardé sur le site et pendant combien de temps ? Combien de fois la page a-t-elle été visitée et quels éléments ont été cliqués ? Quels sites l'utilisateur a-t-il visités avant ou après celui-ci ?

Le regroupement des informations collectées sur plusieurs sites, associé à l'adresse IP et aux détails des appareils utilisés, rend possible une **identification précise de l'utilisateur**.
Le risque principal réside dans la possibilité de **capturer des données** par l'utilisation de cookies. Des cookies défectueux ou insuffisamment sécurisés peuvent permettre ce type de vol de données.[1]





MYTHE 3 : CE N'EST PAS UN PROBLÈME D'UTILISER LES MÊMES MOTS DE PASSE PARTOUT !

Si, c'est même un gros problème !
Si un compte est piraté et que le même mot de passe est utilisé pour plusieurs services en lien avec une adresse e-mail, d'autres comptes peuvent facilement être compromis. Cela augmente le risque d'usurpation d'identité, de perte de données et d'accès non autorisé à des informations personnelles et sensibles.

Qu'est-ce qui fait qu'un mot de passe est sûr ?

Un bon mot de passe comporte au moins **12 caractères** et est un bon **mélange de caractères spéciaux, de chiffres, de lettres majuscules et de lettres minuscules**. Les suites de chiffres comme 1234 ou le nom de l'animal de compagnie ou les trémas comme ä, ö, ü ne sont pas recommandés.



Comment se souvenir des mots de passe ?

Conseil 1 : Faites une phrase et utilisez la première lettre de chaque mot en respectant les majuscules et les minuscules. Remplace certaines lettres par des chiffres ou des caractères spéciaux, par exemple E = 3, i = !

Conseil 2 : Un gestionnaire de mots de passe permet de gérer plus facilement les différents mots de passe.[2]

Conseil 3 : Invente une phrase, caractères spéciaux compris, et complète-la à chaque nouveau compte avec l'abréviation du fournisseur : par ex. Vraimentbien!0815Insta

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

MYTHE 4 : MON SMARTPHONE M'ÉCOUTE.



Probablement pas ! Il existe une rumeur selon laquelle les smartphones écoutent les conversations pour afficher des publicités ciblées.

Les raisons suivantes contredisent cette croyance

1. Les applications pour smartphone nécessitent une **autorisation explicite** pour pouvoir utiliser le microphone.
2. Les systèmes d'exploitation à partir d'Android 12 et d'iOS 14 n'autorisent plus l'accès invisible au microphone et à la caméra par des applications fonctionnant en arrière-plan. Ils informent, à l'aide d'un **indicateur de confidentialité**, lorsqu'une application utilise le microphone ou la caméra.
3. Si le smartphone écoutait effectivement en permanence et transmettait les conversations, cela se verrait à la consommation d'énergie et au **volume de données consommé**.

Pourquoi nous voyons quand même des publicités personnalisées

1. Les annonces publicitaires se basent sur le **comportement en ligne de l'utilisateur**. Les requêtes de recherche, l'historique de navigation et d'autres données aident les entreprises publicitaires à créer des annonces adaptées. Les algorithmes utilisent les données qui sont de toute façon partagées.
2. De même, les rencontres personnelles peuvent, en **combinant notre statut d'ami** sur les réseaux sociaux et **nos données de localisation**, nous permettre de voir ce produit, dont nous avons peut-être parlé en personne, dans notre Feed.[3]
3. En fait, il existe une technologie basée sur l'IA appelée « **écoute active** ». Elle permet aux entreprises publicitaires d'évaluer les conversations en temps réel afin de diffuser des publicités ciblées en combinaison avec d'autres données comportementales de la personne. Toutefois, il n'est pas prouvé à l'heure actuelle que cette technologie interdite en Allemagne ait été utilisée dans le passé.[4]



Celui qui n'a rien à cacher n'a rien à craindre, n'est-ce pas ?





SUGGESTION DE LIENS

Le HPI Identity Leak Checker permet de vérifier si sa propre adresse e-mail a déjà été trouvée dans une fuite de données

↗ https://sec.hpi.de/ilc/

#DigitaleVorbilder

DIE 10 GRÖßTEN DATENSCHUTZMYTHEN

juuuport.de

MODERATION: VERENA GONSCH



EXPERTE: ULRICH KÜHN



EXPERTE: DR. JENS AMBROCK













TIPP: DIREKTE ANSPRACHE

WELCHE DATEN SIND WIRKLICH ERFORDERLICH FÜR MEINE APPS?

01000001 10100 0110

TIPP: -INFORMATIONEN LIEBER STREUEN -VERSCHIEDENE BROWSER VERWENDEN

DATEN WENIGER IST MEHR

§ RECHT AUF Auskunft

§ RECHT AUF Löschung

DAS INTERNET VERGISST NICHT !!!

TIPP: EIGENVERANTWORTLICHKEIT DER KINDER FÖRDERN

FAIRER AUSGLEICH: WERBEFREIE BEZAHLMODELLE IM JOURNALISMUS

TIPP: SICH ALS ELTERN FÜR DIE LEBENSWELT DER KINDER INTERESSIEREN

- KINDER BEGLEITEN!
- WAS MACHE ICH? STATT EINFACH GLEICH CLICKEN!

WICHTIG:
- KI VERSTEHEN
- TECHNOLOGIE WIRD SICH WEITER ENTWICKELN

WAS IST TRACKING?
VERKETTUNG VON INFORMATIONEN
SUCHHISTORIE
OPTION: ALLES ABLEHNEN

TIPP: AUSTAUSCH MIT DEN KINDERN SUCHEN

SUCHMASCHINEN ALTERNATIVE DUCKDUCKGO NICHT SO INVASIV!

ALTERSGRENZEN KÖNNEN NICHT GUT KONTROLLIERT WERDEN

IMAGEPROBLEM DSGVO

GRAPHIC RECORDING @elibrewing

À propos de l'animatrice

Verena Gonsch
Journaliste, auteure et coach

À propos des intervenants

Dr. Jens Ambrock
Chef d'unité Économie et pouvoirs publics auprès du délégué hambourgeois à la protection des données et à la liberté d'information (HmbBfDI)
↗ datenschutz-hamburg.de

Ulrich Kühn
Suppléant. Direction du délégué hambourgeois à la protection des données et à la liberté d'information (HmbBfDI) et chef d'unité e-Privacy, médias, Europe, réseaux sociaux
↗ datenschutz-hamburg.de

DROITS, DEVOIRS ET RESPONSABILITÉ AU SEIN DE L'ESPACE NUMÉRIQUE

Les parents sont responsables de leurs enfants, en particulier au sein de l'espace numérique peu clair. Le devoir de surveillance implique d'informer les enfants des dangers, de leur apprendre à adopter un comportement approprié, de créer des structures sûres en prenant des mesures de protection individuelles et d'accompagner l'utilisation des médias.

POURQUOI C'EST IMPORTANT POUR LES FAMILLES

Disputes et discussions à propos des médias numériques ? C'est le quotidien de la plupart des familles. Qu'il s'agisse du temps d'écran de l'enfant, de la question des jeux auxquels il peut jouer ou de l'endroit où les comptes peuvent être créés.

L'impuissance s'installe chez de nombreux parents qui se demandent :

- Comment instaurer une utilisation des médias détendue et sécurisée dans notre vie de famille ?
- Quelle est ma responsabilité en tant que parent lorsque mon enfant agit de manière de plus en plus autonome dans l'espace numérique ?
- Comment réussir à transmettre des compétences médiatiques aux enfants dans un quotidien familial et professionnel stressant ?

Par **compétence médiatique**, on entend la capacité à utiliser les médias de manière autonome, critique et active.

LE RAPPORT ENTRE L'ÉDUCATION AUX MÉDIAS ET LA PROTECTION DES DONNÉES

Savoir comment protéger ses données privées est considéré comme partie intégrante de la **compétence médiatique**. Les enfants devraient être en mesure de déterminer eux-mêmes qui reçoit ou peut consulter leurs données. Mais il est tout aussi important de respecter et de préserver les droits correspondants des autres.

Les connaissances à acquérir en matière de protection des données comprennent, par exemple :

- la connaissance des **mots de passe sûrs** et des **paramètres de confidentialité**
- **l'utilisation consciente de ses propres images et de celles des autres**
- la connaissance des modèles commerciaux des grandes entreprises (**commerce de données**)
- **les conséquences des processus de numérisation** sur la société (« l'homme de verre ») et la politique (manipulation des élections)[1]

CES DROITS S'APPLIQUENT AUSSI EN LIGNE

Droits de l'enfant selon la Convention des Nations unies relative aux droits de l'enfant[2]

Presque tous les **droits de l'enfant** sont également touchés dans **l'espace numérique** :

- Accès aux médias
- Protection des données et de la vie privée
- Protection contre la violence et l'exploitation
- Liberté d'expression et d'information
- Association et rassemblement pacifique
- Participation et jeu
- Éducation et compétences médiatiques

Limites d'âge pour la responsabilité pénale et civile

Selon l'article 19 du code pénal (StGB), **les enfants de moins de 14 ans sont considérés comme pénalement irresponsables**. Cela ne doit pas être confondu avec la **capacité délictuelle**, c'est-à-dire la responsabilité civile pour les dommages causés, [3] qui s'accompagne d'une obligation d'indemnisation. Sous réserve de l'existence d'une **intention** ou d'une **négligence**, les enfants peuvent acquérir la **capacité délictuelle dès l'âge de 7 ans**. En 2015, une élève de sixième a été condamnée par le tribunal de grande instance de Memmingen à payer 1500 € pour avoir harcelé un camarade.[4]
En cas de demandes de réparation civile, un titre exécutoire peut ainsi être délivré dès le plus jeune âge et rester valable jusqu'à 30 ans.

Obligation de surveillance en ligne

Les obligations parentales comprennent non seulement la **surveillance**, mais aussi l'**information sur certains dangers** et l'**instruction** avant de laisser les enfants utiliser des appareils numériques ou connectés à Internet.[5] Si les parents ont rempli cette obligation de surveillance, ils ne sont pas automatiquement responsables des actes de leurs enfants.[6]

Les parents ont un **devoir d'éducation et de formation**, et devraient donc être informés des principes fondamentaux en matière de protection des données.[7]

« Jeu, intimité, éducation : Les enfants ont des droits, même dans l'espace numérique ! Les adultes doivent accompagner et encourager les enfants dans leur parcours vers le monde numérique. Décider dans le meilleur intérêt de l'enfant implique de respecter sa volonté tout en garantissant sa sécurité, son inclusion et son épanouissement. »

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

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

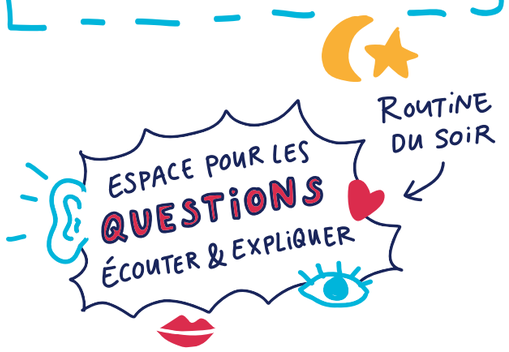
Surveillance ou supervision ?

Malgré la surveillance : Au regard du **droit général à la personnalité** et de la dignité humaine de l'enfant, le **contrôle sans motif** des messages privés sur les services de messagerie ainsi que la surveillance sans raison via le suivi GPS sont généralement interdits.

Cela signifie qu'il doit y avoir un juste équilibre entre le contrôle, la surveillance et l'autonomie croissante des enfants et des adolescents. En cas d'indices concrets de situations critiques, les parents devraient vérifier les appareils de leurs enfants dans un échange direct avec eux, afin de remplir leur devoir parental.

Conseils pour un temps d'utilisation des médias équilibré

- Définition d'un contingent journalier ou hebdomadaire
- Limitation des heures d'utilisation par des réglages sur le routeur, via des applications de contrôle parental ou sur l'appareil lui-même
- Définition conjointe de moments et d'espaces sans médias.
- Donner l'exemple d'une utilisation raisonnable et
- équilibrée des médias.



CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

Créer un environnement en ligne protégé

- Utilisation de messageries, d'applications et de jeux en respectant **l'âge minimum requis**
- Orientation sur les recommandations de l'USK
- effectuer des réglages techniques de sécurité, tels que le blocage des fournisseurs tiers, l'interdiction des achats in-app, le blocage des publicités, la protection par mot de passe pour le téléchargement d'applications, le blocage des sites dangereux pour les mineurs dans le navigateur

Informer les enfants des dangers qu'ils encourent et des conséquences de leurs propres actes délictueux

- Violation des droits d'auteur de tiers
- Diffusion de contenus offensants ou menaçants (cyberharcèlement)
- Diffusion de fake news (par ex. chaînes de messages)
- Sexting avec des mineurs
- Envoi de contenus pornographiques ou de stickers/symboles anticonstitutionnels.
- Atteinte au droit à l'image d'autrui

Informer les enfants des dangers que représentent les autres

- contenus dangereux pour les mineurs
- Pièges financiers liés aux achats intégrés dans les applications, abonnements piégés, faux sites marchands, publicités trompeuses et escroqueries
- Explication des modèles commerciaux des fournisseurs d'applications, des médias sociaux, des assistants vocaux
- Cybergrooming : Cyberintimidation, Deep Fake, Vol d'identité

QUE PEUVENT ENCORE FAIRE LES PARENTS ?

- Informer sur les nouvelles applications, les jeux et les développements techniques
- mener des discussions régulières sur les expériences dans l'espace numérique
- être attentif aux signes avant-coureurs
- aborder à nouveau le sujet lorsque l'enfant, malgré les accords ou les paramètres de sécurité, est exposé à des contenus inappropriés ou engage des frais
- ne pas utiliser la consommation de médias comme récompense ou comme punition
- mettre en place des règles accompagnées de sanctions logiques.

Un **contrat d'utilisation des médias** peut donner des idées pour aborder ensemble, en famille, le thème complexe de l'éducation aux médias.

Nuancé selon les groupes d'âge, il donne des propositions de **règles** aussi bien **pour les parents** que pour **les enfants** et peut être adapté individuellement. Le contrat d'utilisation des médias permet de clarifier ses propres idées et valeurs concernant l'utilisation souhaitée des médias au sein de la famille et de trouver des règles communes. Si chacun comprend clairement ce qui est autorisé ou non, cela peut prévenir des débats et des disputes superflues.





Un contrat d'utilisation des médias rédigé à l'avance permet de clarifier ce qui est permis ou non pour toutes les parties.

extrait du dépliant sur le contrat d'utilisation des médias, **éd. klicksafe & internet-abc**

SUGGESTION DE LIENS

Références pour l'éducation aux médias au sein de la famille

↗ www.mediennutzungsvertrag.de

↗ www.klicksafe.de/eltern

↗ www.internet-abc.de/eltern

Portails d'information sur les bases juridiques au sein de l'espace numérique

↗ https://irights.info/

↗ www.safe-im-recht.de

↗ https://kinderrechte-digital-leben.de/

Conseils en ligne sur la pédagogie des médias pour les jeux vidéo et les médias modernes

↗ https://spieleratgeber-nrw.de/

Instructions détaillées pour le contrôle technique des médias destiné aux jeunes

↗ www.medien-kindersicher.de

#DigitaleVorbilder

RECHTE, PFLICHTEN & VERANTWORTUNG IM DIGITALEN RAUM

TIPP: ELTERN-RATGEBER-SEITEN NUTZEN

GILT AUCH DIGITAL

UN-KINDERRECHTS-KONVENTION

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

RECHT AM EIGENEN BILD!

KLASSENCHATS

DATENSCHUTZ & PERSÖNLICHKEITSRECHTE ACHTEN!

ZIVILRECHTLICH STRAFBAR AB 7 JAHREN

medien-nutzungs-vertrag!

ÜBERTRAG

REGELN & KONSEQUENZEN FÜR ELTERN & KINDER

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

TIPP: FRAGZEBRA.DE FRAGFINN.DE

KINDER-SUCHMASCHINE

EXPERTIN: ANTJE KAISER

GRAPHIC RECORDING @elibreuing

À propos de l'animatrice

Katharina Krüger
Journaliste & chef de projet pour les offres pour enfants de l'ARD

À propos des intervenantes

Antje Kaiser
Chef de projet **#DigitaleVorbilder** & Direction du département Presse, Communication et Éducation aux Médias auprès du LFDI MV
↗ datenschutz-mv.de

Clara von der Heydt,
Pédagogue des médias ou M.A. Médias pour les enfants et les jeunes, responsable du projet #Kinderrechte digital leben!, Der Kinderschutzbund Landesverband Thüringen e.V.
↗ kinderrechte-digital-leben.de/das-projekt

IMAGES D'ENFANTS SUR LE WEB

VIE PRIVÉE DES PETITS UTILISATEURS



Les photos d'enfants sur Internet sont des photographies ou des vidéos qui sont mises en ligne ou partagées via des applications de messagerie. Il est de la responsabilité des tuteurs légaux de protéger la vie privée des enfants et de préserver leur droit à l'image et à la représentation de soi.

POURQUOI C'EST IMPORTANT POUR LES FAMILLES

Les images d'enfants sur les réseaux sociaux sont omniprésentes. Non seulement les enfants et les adolescents, mais aussi les parents, les grands-parents et les amis diffusent des photos numériques et montrent ainsi des aperçus de la vie privée de tous les membres de la famille. Dans de nombreuses familles, les réseaux sociaux et les appareils mobiles font naturellement partie de la communication et de l'échange de photos, comme le montre une étude du Deutsches Kinderhilfswerk.[1] Grâce aux appareils photo de haute qualité des smartphones, il est possible de réaliser de très belles photos, parfois professionnelles. Ces images numériques peuvent être facilement envoyées à des membres de la famille éloignés et servent à se remémorer des étapes importantes de la vie des enfants.

Il existe ce que l'on appelle le **phénomène** du sharenting, selon lequel les parents partagent régulièrement des images et des informations personnelles de leurs enfants sur les réseaux sociaux et les plateformes numériques (mot-clé : Momfluencer).

EN QUOI LES IMAGES D'ENFANTS EN LIGNE SONT-ELLES CONCERNÉES PAR LA PROTECTION DES DONNÉES ?

Les images d'enfants en ligne peuvent révéler des **informations personnelles et sensibles** qui relèvent de la **vie privée** des enfants. Les clichés d'enfants révèlent non seulement leur apparence (données biométriques), mais également, de manière indirecte, des renseignements sur leur **identité, leur adresse, leur école, leurs activités et leur milieu social**. Ces informations sont des **données personnelles sensibles**. Si ces photos sont utilisées par des organismes publics, tels que des crèches, des écoles ou des associations, ces derniers doivent respecter les principes du RGPD, par exemple en obtenant un consentement pour les photos. Les parents, en revanche, ne sont pas soumis à cette obligation.

Le RGPD ne s'applique pas au partage de photos d'enfants dans le cercle privé et familial. Néanmoins, le **droit à l'image** doit être pris en compte. C'est pourquoi il est également important de se demander quelles images sont partagées avec qui.

§ DROITS DE L'ENFANT

La prudence est de mise lors du partage d'images privées via un compte public de médias sociaux. En effet, les photos d'enfants et de famille se retrouvent ainsi mises à la disposition d'un grand nombre de destinataires. La manière dont les photos d'enfants peuvent être modifiées avec les technologies actuelles, comme l'IA, est illustrée de manière très claire dans la vidéo « Message d'Ella »[2].

Les services de messagerie **cryptés de bout en bout offrent plus de** confidentialité **et de** contrôle que les médias sociaux. Les services cloud conformes à la protection des données sont encore plus sûrs, car ils permettent de partager des albums spécifiques avec un cercle restreint. De manière générale, il est important de s'assurer que les plateformes et applications utilisées ont leur siège social dans le périmètre du RGPD, car elles sont ainsi tenues de respecter la législation en vigueur sur la protection des données chez nous.



En tant que parent, membre de la famille, ami(e) ou personne ayant autorité, il est important d'**accepter le refus de l'enfant** et de ne pas essayer de le convaincre. Cela renforce la **confiance en soi et l'efficacité personnelle de l'enfant** en lui apprenant que ses souhaits et ses limites sont pris au sérieux.

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

CES DROITS S'APPLIQUENT AUSSI EN LIGNE

Art. 16 de la Convention des Nations Unies relative aux droits de l'enfant : **Droit à la vie privée**. Les enfants ont le droit à ce que leur honneur ne soit pas bafoué et à ce que des images d'eux ne se retrouvent pas sur Internet sans autorisation.[3]

Tout comme les adultes, les enfants ont le **droit à leur propre image**. Avec l'âge, les enfants développent une conscience personnelle quant à l'autorisation de prendre des photos d'eux. Lors de la diffusion d'images d'enfants, les parents doivent fondamentalement se demander s'ils souhaitent que certaines images se retrouvent sur la toile. Ce droit fait partie du **droit général à la personnalité** et est réglementé par la **loi sur le droit d'auteur des œuvres artistiques** (KunstUrhg). En cas de garde partagée, les deux parents devraient consentir ensemble à la publication de photos de l'enfant, comme celles de la crèche, de l'école ou des vacances, et trouver un arrangement qui soit dans l'intérêt supérieur de l'enfant.

En cas de publication d'images, ce sont en principe les titulaires de l'autorité parentale qui ont le pouvoir de décision et qui doivent donner leur accord à la publication de photos ou de vidéos. Toutefois, à partir de 14 ans environ, la KunstUrhG considère que l'adolescent est **capable de discernement**. Cela signifie que les jeunes peuvent évaluer eux-mêmes les risques liés à la publication et peuvent donc décider si une photo peut être publiée. Un adolescent peut donc autoriser la publication d'une photo par ses amis, même si ses parents s'y opposent. L'inverse est également vrai : Si les parents ont donné l'autorisation de publication mais que l'enfant s'y oppose, c'est la volonté de l'enfant qui prime.

§ DROIT À LA suppression §

Dans l'ensemble, les parents devraient réfléchir très attentivement à l'endroit où ils partagent les images. Même avec un statut sur une application de messagerie, des collègues de travail peuvent voir les photos d'enfants si les paramètres n'ont pas été modifiés au préalable. Les parents devraient se poser la question de savoir si tous leurs contacts téléphoniques doivent vraiment avoir accès à ce statut.

CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

Avant de prendre la photo

- Demander aux enfants / aux tuteurs s'ils peuvent être pris en photo
- Désactiver la fonction de localisation de l'application Appareil photo (souvent aussi des indications de localisation dans les métadonnées des photos)
- Les photos de nudité et en sous-vêtements sont à proscrire
- Vérifier la sécurité des services cloud
- Ne photographier les lieux et situations intimes qu'à des fins privées

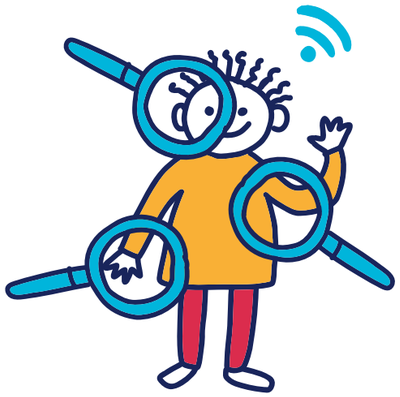
Avant que la photo ne soit téléchargée sur le réseau

- **Demander l'accord de l'enfant concerné** (ou de son tuteur légal) pour publier la photo
- Informer les enfants, en fonction de leur âge, **des risques liés à la publication d'images sur Internet**
- éviter les **données personnelles** telles que le nom, la date de naissance, l'école ou le lieu de résidence
- **Vérifier les droits d'accès** et les **paramètres de confidentialité** des plateformes (également pour les messages de statut)
- Ne pas publier le visage de l'enfant, les détails personnels et les caractéristiques identifiables
- Partager les images uniquement dans des **groupes de confiance** avec un cryptage de bout en bout
- utiliser, le cas échéant, les fonctions d'effacement automatique des images après leur visualisation

CONSEILS D'URGENCE

Si des images d'enfants apparaissent sur Internet sans autorisation, les parents peuvent faire ce qui suit :

- Contacter la personne ou le site web et demander la **suppression des images**
- Utiliser la **fonction de signalement** des plateformes et marquer les images comme inappropriées
- engager des poursuites judiciaires (au civil) en cas de sites non coopératifs ou d'infractions (graves)
- si cela se produit dans le champ d'application du RGPD (par ex. associations), s'adresser à **l'autorité de surveillance de la protection des données**



« La vie privée n'est pas qu'une image. Je sais beaucoup plus de choses sur les enfants des influenceurs familiaux que sur ceux des enfants de mes meilleurs amis : à quelle heure ils se lèvent, quand ils sont agacés, ce qu'ils reçoivent pour leur anniversaire, quelles sont leurs préoccupations, etc. »

Sara Flieder, militante pour les droits de l'enfant

LE SAVIEZ-VOUS ?

Mettre un émoji sur le visage d'un enfant ne suffit pas ? Les lieux et/ou les caractéristiques comme les vêtements restent généralement reconnaissables. La photo se trouve en outre sur le serveur des exploitants de la plate-forme et peut être divulguée, par exemple en cas de cyberattaque. De plus, il existe des logiciels d'image qui permettent de supprimer les émojis.

Vous devriez aussi informer les **grands-parents** des risques liés à la protection des données ? Beaucoup utilisent des smartphones ou des tablettes sans avoir grandi avec Internet et ne sont donc pas conscients des dangers.





SUGGESTION DE LIENS

Plus de conseils pour les parents sur le thème des images d'enfants sur internet

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

Étude du Deutsches Kinderhilfswerk
« Des enfants. Des images. Des droits. Les droits de la personnalité des enfants dans le contexte de l'utilisation des médias numériques au sein de la famille »

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

DAS INTERNET VERGISST NICHT!

MODERATION: NICOLE AHLES

EXPERTIN: SOPHIE POHLE

TIPP: STICKER NICHT ERST IN DER APP HINZUFÜGEN!

ERSTE LIEBE & PORNOGRAFIE ÜBER WHATSAPP

DIGITALER STECKBRIEF

- FOTOS / GESICHTER
- PRIVATE INFOS
- HOBBIES & VORLIEBEN

SICHER SURFEN

KINDERWEBSITES + SUCHMASCHINEN

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

EINVERSTÄNDNISERKLÄRUNG

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

Medienerziehung

ELTERN Medien LOTS:INNEN (FÜR MEDIENPÄDAGOGISCHE ELTERNABENDE)

SAMMLUNGEN VON KINDERBILDERN AUF DEM PC FREMDER? NEIN DANKE!

ELTERNRATGEBER

[!]SCHAU HIN

EXPERTIN: SARA FLIEDER

SHARENTING

Meine ELTERN = MEIN ARBEITGEBER

INFLUENCER KIDS

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

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

SCHAM

Mama, Papa, das ist mir peinlich!

GRAPHIC RECORDING @elibrewing

À propos de l'animatrice

Nicole Ahles
Présentatrice & journaliste

À propos des intervenants

Wiro Nestler
LKA Hambourg
polizei.hamburg.de

Sara Flieder
Militante pour les droits de l'enfant

Sophie Pohle
Chargée de mission auprès du service de coordination des droits de l'enfant de l'association allemande Kinderhilfswerk
dkhw.de

TikTok, Instagram, Snapchat & Co



Les réseaux sociaux sont des services Internet qui permettent d'entrer en contact avec des amis, des connaissances ou des inconnus, d'échanger des informations, mais aussi de se mettre en scène et de partager des informations. Selon le réseau, les utilisateurs rencontrent différents groupes d'âge. Alors que Facebook est depuis de nombreuses années le service le plus populaire chez les plus de 30 ans, les plus jeunes ont tendance à se tourner vers Instagram, Snapchat et TikTok.[1]

POURQUOI C'EST IMPORTANT POUR LES FAMILLES

Sur les 224 minutes de temps moyen passé en ligne chaque jour, les adolescents consacrent une grande partie à des activités sur les réseaux sociaux. Instagram est utilisé régulièrement par 62 % des jeunes âgés de 12 à 19 ans, 59 % utilisent TikTok et 49 % sont actifs sur Snapchat.[2]

Pourquoi ces réseaux sociaux sont-ils si populaires auprès des jeunes ?
Les différentes plateformes de réseaux sociaux proposent aux jeunes des offres variées et répondent ainsi à des besoins spécifiques et à des phases de développement.

Selon Havighurst[3], cela englobe les aspects suivants du développement :

- de l'autonomie et du détachement des parents
- de sa propre identité (sexuelle)
- d'un système de morale et de valeurs
- d'une perspective d'avenir

Les réseaux sociaux offrent un fort potentiel de divertissement, car les algorithmes affichent dans le Feed personnel des utilisateurs des informations captivantes, adaptées à leurs intérêts et préférences Dans le même temps, les médias sociaux permettent **l'échange d'expériences** entre personnes partageant les mêmes idées dans le monde entier (**entraide**) et contribuent également à la **formation d'opinion** et au **développement des intérêts**.

Un profil personnel sur les médias sociaux offre aux jeunes la possibilité de se **présenter de manière positive**. Qu'il s'agisse de situations de la vie quotidienne, de danse, de karaoké, de let's Plays, de pranks ou de duos : Grâce à des outils professionnels intuitifs pour le montage, le son et les effets visuels, il n'a jamais été aussi facile de devenir soi-même créatif. Le contenu créé est partagé tout aussi rapidement. Cela favorise d'une part **l'efficacité personnelle** et peut également contribuer à l'augmentation de l'estime de soi, encouragée par les likes et les **commentaires positifs**. Enfin, les réseaux sociaux incitent à se lancer des défis et à repousser ses limites.

RISQUES GÉNÉRAUX DES PLATEFORMES SOCIALES

Les aspects positifs des médias sociaux s'accompagnent également de risques dont les parents et les jeunes doivent être conscients :

- **Risque** de dépendance aux médias
- **Réduction de la durée d'attention en raison de l'accoutumance à des clips de courte durée**
- **Isolement** dans le monde « réel »
- **problèmes psychologiques** et troubles du sommeil dus à des contenus non adaptés aux enfants et à l'absence de contrôle de l'âge (violence, opinions politiques extrêmes, pornographie)
- défis et blagues potentiellement mortelles
- **pression sociale** due à la quête de likes, de flammes, de réactions sur les publications
- **FOMO** (angl. Fear of missing out) : la peur de manquer quelque chose, renforcée par les messages push
- Préférence pour des représentations sexualisées et dénudées, ainsi que la mise en scène de rôles stéréotypés, encouragée par la communauté (plus de likes et de visibilité).
- Des aperçus d'espaces très privés, comme les chambres d'enfants
- portée ingérable pour les profils publics
- diffusion facile de fake news
- **Faux profils**



- **Risque de coûts cachés** à travers les cadeaux virtuels pendant les livestreams (comme sur TikTok)
- **Cession des droits** sur les images et les vidéos téléchargées aux opérateurs de la plateforme
- Risque d'agir de manière **contraire à la loi** en portant atteinte aux **droits d'auteur, aux droits à l'image** ou à d'autres droits relatifs à la personnalité.

Même les jeunes qui connaissent bien les smartphones, les réseaux sociaux et les applications ne sont pas forcément en mesure d'évaluer correctement les risques qui y sont liés et ont besoin d'aide pour classer et traiter ce qu'ils voient.

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

PLATEFORMES SOCIALES ET PROTECTION DE LA VIE PRIVÉE

Les réseaux sociaux visent à se connecter avec le plus grand nombre de personnes possible ou à obtenir une attention particulière de la part d'autres utilisateurs. Cela est difficilement conciliable avec le principe fondamental de la protection des données, qui consiste à ne pas perdre le contrôle sur ses propres données.

Les utilisateurs de réseaux sociaux doivent être conscients que l'obligation de proposer des réglages respectueux de la vie privée (Privacy by default) est insuffisamment appliquée par la plupart des plateformes sociales. Souvent, on cède les droits sur les contenus téléchargés (y compris sur les profils privés) aux exploitants des plateformes. Les tuteurs légaux ont l'obligation de veiller aux droits de la personnalité de leurs enfants mineurs.

Les profils publics, en particulier, comportent le risque que les contenus postés se répandent de manière incontrôlée sur le réseau. Ces profils peuvent être trouvés par les moteurs de recherche, même par des personnes qui ne possèdent pas de compte sur les médias sociaux. **Tout ce qui est publié sur Internet y reste définitivement !** Même si les Stories ou les messages disparaissent automatiquement après un certain laps de temps, les captures d'écran permettent de sauvegarder ces contributions et de les diffuser plus largement.

Les fournisseurs de réseaux sociaux gagnent de l'argent avec les données fournies. **L'accès gratuit se fait au prix de vos propres données**. C'est souvent résumé par la phrase : « Si tu ne paies pas pour un produit, c'est toi le produit. »

Ces données sont utilisées pour créer un **profil d'utilisateur individuel** et pour pouvoir diffuser de la publicité et des contenus le plus efficacement possible. Les contenus personnalisés permettent aux utilisateurs de rester plus longtemps sur les pages.

Mais les données des contacts personnels sont aussi souvent récupérées sans être demandées.

Pour pouvoir suggérer des amis et de la famille aux utilisateurs, les contacts du répertoire téléphonique sont automatiquement lus. Il est possible d'empêcher cela en permettant aux utilisateurs de refuser de manière proactive dans les paramètres.

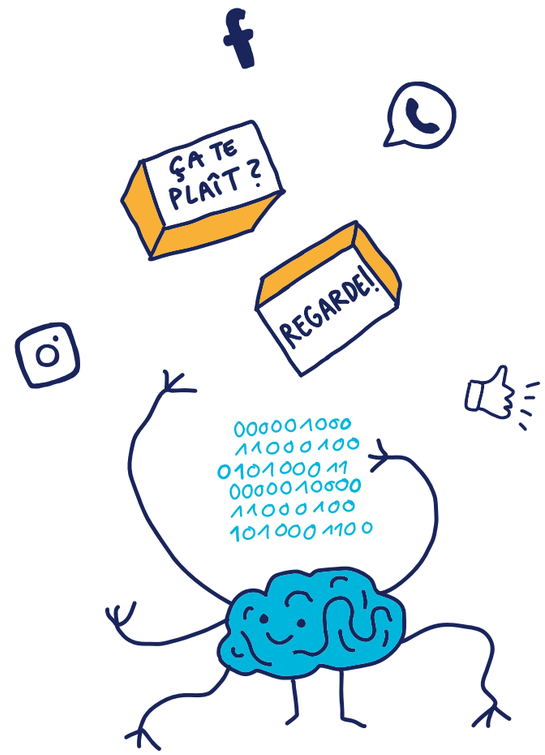
« L'algorithme de TikTok fonctionne particulièrement bien en nous montrant de manière ciblée des choses que nous trouvons intéressantes. Nous avons l'impression qu'il nous connaît mieux que nous ne nous connaissons nous-mêmes. Cela peut nous amener à y passer plus de temps que nous ne l'avions prévu. »

Martin Bregenzer

CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

Pour sécuriser au maximum l'utilisation des médias sociaux, il existe différentes possibilités de paramétrage :

- Mettre le compte en mode privé (la photo de profil, le nom et éventuellement les informations de profil optionnelles, la bio, peuvent néanmoins être visibles par tous les utilisateurs)
- savoir où signaler et bloquer les messages, les commentaires, les messages directs (DM) et les utilisateurs (tout ce qui va à l'encontre des directives de la communauté)
- lire les directives de la communauté avec l'enfant
- Restreindre le cercle des personnes autorisées à envoyer des messages privés
- Désactiver, filtrer, masquer la fonction de commentaire
- Limiter les likes, les vues
- Vérifier qui peut mentionner le profil
- Gérer les paramètres des Stories : voir, répondre, partager uniquement avec les amis proches
- Temps d'écran : Définir des limites de temps, rappeler les pauses, désactiver les notifications push ou par e-mail sur les activités
- mettre en place un mode restreint pour les jeunes enfants, afin de masquer les contenus douteux
- utiliser le mode parental / supervision / family center si nécessaire
- Désactiver le partage de site



SUGGESTION DE LIENS

Dépliant de Klicksafe sur différentes plateformes de réseaux sociaux

↗ www.klicksafe.de/materialien/

Informations sur divers réseaux sociaux de SchauHin !

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

Instructions pour une utilisation respectueuse de la vie privée de différentes plateformes de réseaux sociaux

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

#Digitale Vorbilder

TikTok, Instagram, Snapchat & Co







WECKER STELLEN?

WÖCHENTLICHES KONTINGENT?

Medien-zeiten FESTLEGEN?

TIPP: WIE GEHT ES MEINEM KIND? SELBSTWERT

SNAPCHAT STREAK

SEIT 2011

Mindestens 1x TÄGLICH SNAPPEN

USK 12

SEIT 2018

SEIT 2010

EIGENE WERTE WEITERGEBEN BEWUSSTSEIN

TIPP: WAS PASST FÜR UNSERE FAMILIE?

KOSTENLOS EINFACH SCHNELL

Medien-nutzungs-vertrag

ERSTE MEDIEN-SCHRITTE GEMEINSAM

ACHTUNG: CHATANFRAGEN VON UNBEKANNTEN

DOOOM SCROLLING ACHTUNG SUCHTGEFAHR!

ALGORITHMUS+ MANIPULATIVES DESIGN

SCHAM SELBSTWERT WACHSEN LASSEN & DAS KIND NICHT BESCHÄMEN!

GENUG SCHLAF

ICH BRAUCHE BEWEGUNG!!!

BILDSCHIRMZEIT

TIPP: BEGLEIT-MODUS AUF DEN APPS NUTZEN

TikTok

DIGITAL WELLBEING EINSTELLUNG

JUGENDLICHE HELFEN JUGENDLICHEN

20,9 Mio. MONATLICH AUF TikTok !!!

· ANONYM
· KOSTENFREI
· GLEICHALTRIGE

FAIRNESS IM UMGANG mit Regeln

OFFLINE ABENTEUER

TIPP: KINDER BEGLEITEN + INTERESSE ZEIGEN

klicksafe.de
juuuport.de

MEDIEN-KINDERSICHER.DE

REINER KONSUM ODER SELBST PRODUZIEREND?

SELBSTDARSTELLUNG ODER AKTIV SELBST kreativ werden!

SICHER KONSUMIEREN

KINDGERECHTE INHALTE AUCH OHNE WERBUNG

WICHTIG! GUTE GESETZE VERANTWORTUNG DER UNTERNEHMEN

TIPP: SELBST-REGULA-TION: WIE MACHEN MA&PA DAS?

GRAPHIC RECORDING @elibreuing

À propos de l'animatrice

Katharina Krüger
Journaliste & chef de projet pour les offres pour enfants de l'ARD

À propos des intervenants

Martin Bregenzer
Chargé de mission pour la compétence médiatique auprès de l'initiative européenne klicksafe, Medienanstalt Rheinland-Pfalz

↗ www.klicksafe.de

Dr. Phil. Detlef Scholz,
Pédagogue en sciences de l'éducation, thérapeute systémique (SG), éducateur aux médias, conseiller psychologique ; directeur du centre de compétences et service de conseil pour l'utilisation excessive des médias et la dépendance aux médias.

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

UTILISATION DES MÉDIAS
DANS LA FAMILLE



L'utilisation des médias au sein de la famille fait référence à la manière dont les membres de la famille consomment et utilisent les médias numériques. Cela inclut une variété d'activités où les technologies et les médias sont intégrés dans la vie quotidienne de la famille. Cela comprend aussi bien l'utilisation individuelle par les différents membres de la famille que les activités communes liées aux médias.

Dans ce contexte, il est très important que tous les membres de la famille aient une approche critique et réfléchie des données et des informations en ligne.

POURQUOI C'EST IMPORTANT POUR LES FAMILLES

Dans la plupart des familles, on trouve une grande variété d'équipements techniques et d'habitudes d'utilisation des médias.

Dans de nombreux foyers, l'équipement avec les derniers **appareils techniques** et applications, souvent dotés de dispositifs intelligents comme des assistants vocaux, est déjà la norme. De l'interrupteur de lumière à la machine à café, de l'ouverture de porte au robot aspirateur, de nombreuses fonctions sont **automatisées et (télé)commandées**.

Les avantages d'Internet sont également indiscutables pour l'**organisation de la vie familiale**, entre autres par le biais de calendriers partagés, de listes de courses ou **d'échanges** avec les proches au-delà des frontières. Cela est renforcé, par exemple, par les **jeux numériques**, les facilités offertes par l'intelligence artificielle et les **applications éducatives pour l'apprentissage** à l'école et à l'université, ou encore par l'inspiration des influenceurs sur les réseaux sociaux.

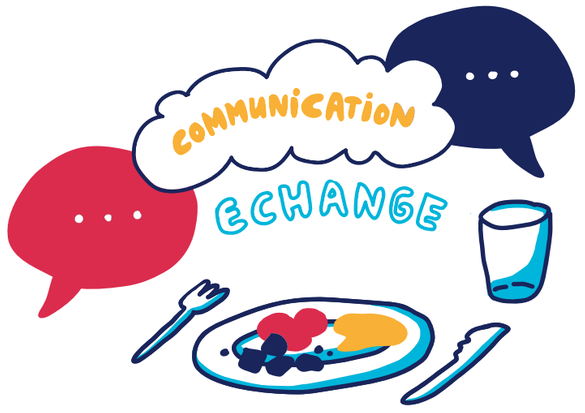
L'étude KIM 2022 révèle que de plus en plus d'enfants utilisent les médias numériques de manière autonome et sans supervision adulte. 48 % des parents interrogés d'enfants âgés de 6 à 12 ans l'ont confirmé. Alors qu'avec l'âge, de plus en plus d'enfants sont en ligne, les possibilités et services techniques de protection contre les contenus inappropriés en ligne ne sont utilisés que par un tiers des parents. Ce résultat est surprenant dans la mesure où 80 % des parents sont conscients des dangers que courent les enfants sur Internet.[1]

UTILISATION DES MÉDIAS ET PROTECTION DES DONNÉES

La protection de la vie privée dans la famille est un aspect crucial de l'utilisation des médias qui nécessite une action proactive de la part des parents afin de garantir la **vie privée et la sécurité** de tous les membres de la famille dans **l'espace numérique**. Tous les membres adultes de la famille sont invités à montrer l'exemple en montrant comment la **protection des données** est bien appliquée et pourquoi elle est si importante. Ils assument la responsabilité de **l'empreinte numérique** que les enfants laissent sur le web dès leur plus jeune âge.

Les parents devraient veiller à ce que les appareils utilisés par la famille soient sécurisés, par exemple par des mises à jour régulières, des pare-feu et des mots de passe sûrs.

Si le contrôle parental est important, les parents doivent également respecter le **droit à la vie privée de leurs enfants** et être sensibles à leurs données.



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



« Il peut arriver que les enfants développent une sorte de comportement jaloux ou voient les appareils numériques comme des concurrents si les parents y passent trop de temps. Il est important que les parents mettent délibérément de côté les appareils numériques pour passer du temps avec leur enfant, sinon le lien en pâtira.[2] »

CES DROITS S'APPLIQUENT AUSSI EN LIGNE

Ce chapitre se concentre particulièrement sur le **droit de l'enfant à une famille, à des soins parentaux et à un foyer sécurisé**. On peut en déduire que les parents ont le devoir d'accompagner leurs enfants dans le monde des médias et de les protéger contre des contenus ou des contacts inappropriés, notamment en utilisant des paramètres de sécurité adaptés. Mais cela implique également une utilisation réfléchie et sûre des technologies intelligentes à la maison.

« **L'éducation aux médias** consiste à accompagner les enfants dans le **développement** de **leurs compétences médiatiques** et dans le traitement de leurs expériences médiatiques. »[1]

« Les parents ont le devoir d'orienter leurs enfants dans le **choix des médias** et de les accompagner dans leur utilisation. Après tout, ce sont eux qui autorisent (ou peuvent interdire) l'accès des enfants à certaines offres médiatiques). Les souhaits et les besoins des enfants doivent également être pris en compte. »[2]

Conseil : Il est judicieux de se rechercher régulièrement sur les moteurs de recherche et les réseaux sociaux pour vérifier l'état de sa réputation en ligne. De fausses informations circulent-elles sur votre vous ? Des informations personnelles ont-elles été publiées sans le consentement éclairé de la personne concernée ? Si tel est le cas, il convient de prendre des mesures proactives pour y remédier et d'exiger des responsables la suppression des informations incorrectes ou éventuellement publiées illégalement.

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

CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

Développer une attitude personnelle face aux médias numériques

- **La base de l'action et de la décision en matière d'éducation aux médias** devrait être une interaction entre les valeurs, les objectifs, les convictions, les expériences et les connaissances
- Défi de la génération actuelle de parents, apprendre à connaître les technologies et à utiliser les médias numériques en toute sécurité
- un contact détendu et une **attitude ouverte**, ainsi que la **confiance** dans l'apprentissage des enfants par leurs propres expériences (positives et négatives)
- **voir les opportunités plutôt que les risques** en premier lieu
- **une discussion constructive**, comme base d'une éducation aux médias accompagnée et respectueuse[3]

Donner l'exemple

- dans la gestion des photos (d'enfants), lors de leur prise et de leur partage
- en ayant son propre équilibre numérique dans la vie privée, en particulier pendant la période parents-enfants
- en home-office/en tant qu'indépendant devant l'enfant fixer des priorités dans sa propre attention
- dans la gestion de sa propre vie privée : Combien d'informations personnelles est-ce que je partage sur les réseaux sociaux/en ligne ?
- Quand dois-je choisir « Autoriser tous les cookies » au lieu de « Autoriser uniquement les cookies techniquement nécessaires » dans la requête relative aux cookies ?
- Dans quelle mesure est-ce que je donne mes informations de contact sans réfléchir pour participer à des jeux-concours ou permets à des fournisseurs de programmes de programmes de fidélité, comme la collecte de points ou les applications de supermarchés et de pharmacies, à recueillir mes données pour créer des profils d'utilisation, de santé, d'achat ou de déplacement ?
- Est-ce que je prends le temps de lire les conditions générales pour m'informer sur les autorisations des applications ?
- Est-ce que j'attache de l'importance aux paramètres de protection des données sur mes terminaux ?

Informer et établir des règles

- **Permis de conduire médiatique** pour l'enfant comme condition préalable à l'obtention de son propre smartphone
- Les enfants ont aussi besoin de règles et de limites sur Internet
- accord commun sur un **contrat d'utilisation des médias**
- **Aborder, dans le dialogue, des dangers adaptés à l'âge ainsi que des stratégies de solution, et indiquer des points de contact.**
- utiliser des mesures techniques de protection pour appliquer de manière cohérente les règles d'utilisation des médias convenues

S'établir comme personne de confiance

- **montrer de l'intérêt pour les préoccupations** et les besoins de l'enfant
- se faire expliquer la **fascination des jeux en ligne et** y jouer soi-même
- ne pas punir par la privation de médias



Présenter des alternatives à l'utilisation des médias numériques

- **Montrer des aventures en dehors du monde numérique** : par exemple dans la forêt, lors d'une randonnée ou d'une baignade, jeu de rôle avec déguisement, géocaching, etc.
- **donner envie d'utiliser des médias analogiques**, comme les livres ou les jeux de société
- Explorer la **« bibliothèque des objets »**

« Si nous jouions davantage avec nos enfants, les jeux numériques ne seraient peut-être pas si importants ! »

Thomas Feibel, fondateur du prix logiciel TOMMI

SUGGESTION DE LIENS

24 idées pour que votre enfant délaisse un peu les écrans

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

Permis médias pour les enfants

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

Liste de contrôle familiale sur la protection des données

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

Accompagner les enfants en toute sécurité sur le web – Guide pour les parents

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

#Digitale Vorbilder
MEDIENNUTZUNG
IN DER FAMILIE

















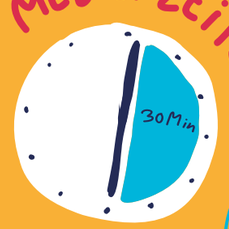








































GRAPHIC RECORDING @elibrewing

À propos de l'animatrice

Katharina Krüger
Journaliste & chef de projet pour les offres pour enfants de l'ARD

À propos des intervenants

Thomas Feibel
Journaliste, directeur du bureau des médias pour enfants, organisateur & fondateur du Prix allemand des logiciels pour enfants TOMMI, auteur de guides sur l'éducation aux médias et de livres pour enfants et adolescents sur le fait de grandir dans un monde numérique. Intervenant
↗ https://feibel.de/

Katherine Zimmermann
Pédagogue des médias et auteure spécialisée dans les médias pour enfants et adolescents
↗ https://medienmentorin.de/

JOUER

EN TOUTE SÉCURITÉ !



Le gaming désigne le fait de jouer à des jeux numériques sur des appareils électroniques, tels que les consoles de jeux, les ordinateurs, les ordinateurs portables, les tablettes ou les smartphones, seul ou avec d'autres. Les jeux numériques peuvent être divisés en différents genres, qui se distinguent principalement par leurs mécanismes de jeu. Cela peut concerner des processus abstraits et des tâches, des imitations de jeux et sports conventionnels, ou encore des applications de réalité virtuelle. Cela exige des joueurs qu'ils fassent preuve d'endurance, d'habileté, de rapidité, de tactique ou de finesse.

POURQUOI C'EST IMPORTANT POUR LES FAMILLES

Les jeux numériques sont devenus incontournables dans de nombreux foyers. Au total, 72 % des jeunes jouent régulièrement. Peu importe qu'ils jouent sur un **ordinateur, une console, une tablette ou un téléphone portable**. Les habitudes d'utilisation diffèrent selon le sexe. Les garçons sont deux fois plus actifs (119 min/jour) que les filles (61 min/jour seulement). Parmi les favoris des garçons, on trouve « Minecraft », « FIFA », « Fortnite » et « GTA - Grand Theft Auto ». Les filles, en revanche, préfèrent Les Sims, Hay Day, Mario Kart, Candy Crush, Roblox, Subway Surfer, Super Mario et Poudlard Legacy.[1]

Il existe de nombreux **aspects positifs** qui rendent les jeux numériques recommandables pour les enfants et les adolescents :



- Développer des compétences telles que la **vitesse de réaction, la coordination œil-main, l'attention visuelle** et **la pensée logique et spatiale**
- Stimulation de la **créativité**
- Les défis complexes suscitent la **motivation** nécessaire pour maîtriser des moments difficiles
- Augmentation de la **persévérance** Promotion de l'éducation **historique et politique**
- Naissance et entretien **d'amitiés** par le biais de chats ou de jeux communs
- Approfondissement des connaissances en langues étrangères

Mais il y a aussi des **aspects négatifs** qui peuvent causer des dommages à l'enfant :

- jouer **de manière excessive** peut engendrer des problèmes tels que des **troubles du sommeil, des problèmes de concentration et la mise de côté d'autres activités**
- Augmentation possible des **comportements agressifs**
- **problèmes de santé dus au** manque d'exercice et à la position assise
- Infiltration des chats de jeux par des **extrémistes** qui les utilisent pour leur propagande
- Infiltration par des adultes pour initier des contacts sexuels avec des enfants et des adolescents (cybergrooming)

Il appartient aux parents d'évaluer les avantages et les inconvénients, de surveiller les jeux numériques que l'enfant utilise actuellement, et d'intervenir si des risques ou des signes de surcharge apparaissent.

« Utilise un pseudo qui ne permet pas d'identifier l'âge, le sexe ou le lieu de résidence. »

Thomas Freitag, Office régional de la police criminelle M-V

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



JEUX EN LIGNE SONT ET PROTECTION DES DONNÉES PERSONNELLES

Pour acheter du matériel et des logiciels, télécharger des jeux, installer des mises à jour et jouer en ligne contre d'autres, un compte est nécessaire. Dans ce compte sont enregistrés les **données de contact, l'adresse e-mail, les mots de passe, les questions de sécurité, la date de naissance, les informations de carte bancaire, les coordonnées bancaires et les jeux achetés**.[2]

De plus, les éditeurs de jeux et les plateformes enregistrent des données biométriques, des détails sur les habitudes de jeu individuelles et les interactions avec d'autres joueurs. Ces données sont utilisées pour **personnaliser l'expérience de jeu**, **créer un profil utilisateur** et **afficher des publicités ciblées**.

Depuis l'avènement des technologies de réalité augmentée, les **données de géolocalisation** des joueurs sont également enregistrées. Ces données permettent non seulement de déterminer la localisation des joueurs, mais aussi de connaître le temps passé à jouer et même le nombre de calories brûlées pendant une session. « Dans l'ensemble, ces données de géolocalisation peuvent dresser un tableau précis des routines quotidiennes d'un joueur, comme son adresse personnelle, son lieu de travail ou ses lieux de loisirs favoris. »[3]

Les jeux et plates-formes commercialisés en Europe doivent à cet égard respecter les directives et principes du **RGPD**. D'après ce règlement, les joueurs ont un droit d'accès concernant l'utilisation de leurs **données à caractère personnel**. Ils doivent avoir consenti au traitement et à la transmission de leurs données soit en concluant un **contrat d'achat** et/ou en donnant leur **consentement explicite**.

En particulier pour les éditeurs de jeux et les plateformes situés en dehors du champ d'application du **RGPD**, il est impossible de garantir avec certitude quelles données sont effectivement collectées, stockées et traitées.[4]

CES DROITS S'APPLIQUENT AUSSI EN LIGNE

Selon la loi sur la **protection de la jeunesse** (JuSchG), les jeux informatiques et vidéo sur supports physiques ne peuvent être vendus aux enfants et aux adolescents qu'après examen et approbation par l'Autorité de régulation du logiciel de divertissement (USK). Les tranches d'âge respectives sont 0, 6, 12, 16 et 18 ans. Les jeux qui n'ont pas été soumis à l'évaluation de l'USK ou qui n'ont pas obtenu de classification d'âge par l'USK ne peuvent être vendus qu'à des adultes. Toutefois, les tranches d'âge ne constituent pas une recommandation d'aptitude pédagogique.

Le **traité d'État sur la protection des jeunes dans les médias** (JMStV) conclu entre tous les états fédéraux allemand régit la protection des jeunes dans les médias, notamment dans le domaine de la radio et télévision et des services de télécommunication (offres en ligne accessibles sur Internet). Contrairement à la JuSchG, le JMStV ne prévoit pas de classification par âge progressive. Cependant, il doit être assuré, par une restriction des horaires de diffusion ou des mesures techniques, que les offres pouvant affecter le développement ne soient pas accessibles aux enfants de la tranche d'âge concernée. [1]C'est pour cela que les plateformes de streaming et de vidéos proposent des réglages d'âge.



[1] cf. game 2024

[2] cf. BzGA 2024: Kostenfallen

CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

Veiller à la sécurité

- **Activer les contrôles parentaux et les fonctions de sécurité** sur les appareils afin de limiter l'accès aux contenus payants et dangereux pour les mineurs
- **Vérifier les paramètres de confidentialité** dans les jeux et sur les plateformes
- Désactiver la possibilité de **contacter des inconnus** dans le **chat**
- ne pas utiliser de nom clair mais un pseudonyme qui ne permette pas de déduire l'âge, le sexe ou le lieu de résidence
- **Respecter les limites d'âge et les restrictions de contenu** (informer l'enfant de la nécessité de ces paramètres de protection, qui peuvent facilement être contournés par l'absence de vérification de l'âge par le fournisseur)
- **Utiliser des programmes de contrôle parental et des logiciels de protection**



Avoir des discussion parents-enfants sur l'utilisation des jeux en ligne

- **Créer un compte commun**
- évaluer quelles données personnelles et quelles autorisations d'application sont nécessaires
- **s'informer sur les jeux (comprendre le contenu, les caractéristiques de sécurité)**
- établir des règles claires **pour le temps de jeu** (contrôle technique par les réglages dans l'application)
- **Informer sur les** dangers potentiels**, tels que la publicité personnalisée**, les contenus inappropriés, l'utilisation abusive des données personnelles, le cybergrooming
- **Aborder les pièges des coûts**

Connaître les pièges des coûts

- multiplication des dépenses pour les **loot boxes**, les skins et les costumes additionnels
- Danger des abonnements pièges
- contenus **additionnels onéreux pour jeux, disponibles sur des plateformes en ligne**[2]
- Le **Play to earn** (jouer pour gagner) promet aux enfants de gagner de l'argent en jouant, mais cela implique souvent un investissement initial élevé.

Éviter les pièges financiers et conseils pratiques en cas d'urgence

- **Limiter** et désactiver **les moyens de paiement** et **les achats in-app** sur les appareils de l'enfant (protégés par un mot de passe)
- **Éviter de donner des informations sur les cartes de crédit ou les comptes bancaires**
- **Paiement par carte de recharge**, comme paysafe, google play/apple cards (accord sur des montants fixes)
- **Contrôle de l'historique des achats** sur les appareils de l'enfant (identification des achats involontaires ou non autorisés)
- **Contacter le service clientèle** de la plateforme concernée ou du développeur du jeu pour obtenir le remboursement d'achats non autorisés

***Conseil aux parents :**
Attention aux loot boxes !

Dans certains jeux, et notamment dans les applications de jeux gratuits, on trouve des loot boxes. Les loot boxes, dérivées de l'anglais « to loot » (ramasser), promettent du contenu utile, comme des armes, de l'équipement ou des unités d'argent pour progresser dans le jeu. Les contenus arrivent de manière aléatoire et ont tendance à inciter à l'achat d'autres loot boxes. Comme les loot boxes sont payées avec de l'argent réel, elles sont particulièrement lucratives pour les fournisseurs de jeux.

Recommandation pour les parents et les éducateurs : « Jouez donc vous-même, faites des expériences pratiques avec ce média, créez vos propres comptes et discutez avec (vos) enfants de ce qu'ils y vivent! »

Mick Prinz, Fondation Amadeu-Antonio

SUGGESTION DE LIENS

Classification des loot boxes : « Analyse des très controversées loot boxes du point de vue de la protection des mineurs »

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

Aperçu de l'adéquation des jeux selon des critères pédagogiques

↗ https://spieleratgeber-nrw.de/

Conseils aux parents pour accompagner les enfants dans leurs jeux et conseils de sécurité

↗ www.klicksafe.de/digitale-spiele

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

Aperçu des centres d'accueil en cas de dépendance aux médias (et aux jeux)

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



À propos de l'animatrice

Antje Kießler
Présentatrice & journaliste

À propos de l'intervenant

Benjamin Heinemann
Pédagogue indépendant chez
Creative Gaming e.V.

↗ creative-gaming.eu

>>>> LUTTER ACTIVEMENT CONTRE LE <<<<

CYBERHARCÈLEMENT

#@?!%

?%!!!

Le cyberharcèlement désigne le fait d'offenser, de menacer, de ridiculiser, d'exclure ou de harceler délibérément autrui via Internet, généralement par une ou plusieurs personnes, sur une période prolongée. Les propos offensants se diffusent à grande vitesse en ligne, et dans le cas de cyberharcèlement, l'audience peut devenir ingérable.

POURQUOI C'EST IMPORTANT POUR LES FAMILLES

Des études récentes montrent que **plus d'un jeune sur deux a été victime de cyberintimidation** dans **son environnement personnel direct**. Selon la dernière étude JIM de 2023, 14 % des jeunes de 12 à 19 ans interrogés ont été victimes **d'insultes personnelles** ou **d'hostilité** à leur égard au cours du mois écoulé, et 39 % ont été confrontés à des **messages de haine** sur Internet.[1]

Le cyberharcèlement survient là où les jeunes sont les plus actifs en ligne : 52 % sur la messagerie **WhatsApp**, suivie de près par les plateformes de médias sociaux **TikTok** avec 34 % et **Instagram** avec 33 %.[2]

CYBERHARCÈLEMENT ET PROTECTION DES DONNÉES PERSONNELLES

Le cyberharcèlement est un phénomène de diffusion numérique abusive de **données à caractère personnel**, telles que des **photos ou des informations personnelles**. Par ces actions, les auteurs enfreignent le droit fondamental à l'autodétermination informationnelle.

Dans certains cas, le cyberharcèlement s'accompagne de ce que l'on appelle une **usurpation d'identité**. La victime se fait ainsi subtiliser ses données d'accès à son compte sur un réseau social. Les auteurs peuvent alors publier des contenus ou écrire des messages au nom de la victime afin de la discréditer.[3]

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

CES DROITS S'APPLIQUENT AUSSI EN LIGNE

En Allemagne, le droit à la liberté d'expression est décrit dans l'article 5 de la Loi fondamentale. Certains pensent que cela permet de tout se permettre. Mais ce n'est pas le cas !

Le droit à la liberté d'expression n'est pas absolu. Il atteint ses limites là où la dignité humaine et le droit de la personnalité d'autrui sont violés. De même, les contenus punissables ne sont pas couverts par la liberté d'expression. Bien que le cyberharcèlement en tant que tel ne constitue pas une infraction pénale distincte en Allemagne, les faits suivants prévus par le Code pénal allemand (StGB) peuvent être concernés :

§ 187 du code pénal allemand Diffamation
§ 185 du code pénal allemand Insulte
§186 StGB diffamation
§ 253 du code pénal allemand Extorsion

Dans le cadre du cyberharcèlement, ces actes s'accompagnent souvent de la diffusion abusive d'images ou de vidéos de la victime, ce qui viole en outre le droit à l'image, pouvant entraîner des conséquences juridiques civiles. Il est donc important de comprendre que la liberté d'expression ne justifie pas un comportement irrespectueux ou préjudiciable sur Internet.



La sensibilisation à la protection des données implique non seulement la prudence dans l'utilisation de ses propres données, mais aussi le respect des données des autres.



Indicateurs chez les victimes :

- Une baisse frappante de la consommation de médias sur les plateformes habituelles : le « lieu de crime » est boudé
- Résultats scolaires en baisse
- Problèmes de concentration
- Désintérêt pour l'école et refus d'aller à l'école
- Isolement ou exclusion pendant les pauses, les travaux de groupe
- Dépression et problèmes psychiques en général
- Fatigue due aux troubles du sommeil

CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

- Sensibiliser à la protection des données : Faire preuve de prudence dans l'utilisation de ses propres données et de respect pour les données d'autrui
- Définir des règles pour l'utilisation de ses propres données et le partage d'images en ligne (voir chapitre « Images d'enfants en ligne »)

Mettre en place des environnements en ligne protégés

- **des paramètres de confidentialité appropriés**
- une utilisation du **mode parental** d'accompagnement proposé par de nombreuses plates-formes
- le respect des indications d'âge des platesformes
- **l'indication véridique de l'âge** lors de la création du profil

Renforcer la relation de confiance entre parents et enfants

- **Renforcer** l'estime de soi et la résilience
- entretenir une relation de confiance, se montrer intéressé et **ouvert au monde de l'enfant/de l'adolescent** et être disponible en tant qu'interlocuteur
- Sensibiliser à l'importance de **réfléchir avant de poster**, en se demandant si l'on dirait la même chose dans un échange en tête-à-tête, et de formuler ses propos de manière aussi claire que possible (les emojis peuvent y contribuer).
- **Permettre un changement de perspective** : se proposer comme partenaire de réflexion et transmettre de l'empathie pour la manière dont les messages ou les images partagés (par ex. dans le chat de la classe) pourraient être perçus par la personne concernée
- donner l'exemple et communiquer un ton **respectueux et valorisant**

« Si tu vois quelqu'un se faire harceler en ligne, ne reste pas sans rien faire : soutiens cette personne, par exemple en lui envoyant un message d'amour. »

Melina Everhartz de la plate-forme de conseil en ligne JUUUPORT

Pourquoi les gens harcèlent-ils les autres ?

Les auteurs du harcèlement agissent soit par ennui, soit parce qu'ils sont en colère contre quelqu'un, soit tout simplement parce qu'ils ont une faible estime d'eux-mêmes. Certains harceleurs ont eux-mêmes été victimes de harcèlement moral par le passé. En intimidant ceux qu'ils considèrent comme plus faibles et en suscitant des réactions positives de la part d'un « public », ils se sentent forts, drôles, populaires et supérieurs.

Il est facile de poster quelque chose de méchant sur les autres, car on n'a pas à les regarder directement dans les yeux ni à faire face à leur détresse. Certaines pratiquent le harcèlement en restant anonymes, en se cachant derrière un pseudonyme ou un profil fictif. Cela abaisse encore davantage la barrière qui incite à adopter un comportement respectueux.

CONSEILS D'URGENCE

Pour les personnes concernées

- agir et demander de l'aide à des **adultes de confiance**/à un **centre de conseil anonyme**
- **Documenter** les faits avec des captures d'écran **et/ou un** journal de harcèlement
- Signaler le **message au gestionnaire du site et demander sa suppression**.
- Demander aux auteurs de retirer la photo/vidéo/le commentaire
- **Bloquer** les cyberharceleurs
- Déposer une **plainte** auprès de la police avec vos parents et envisager des démarches civiles

Pour les parents de personnes concernées

- **Chercher le dialogue** avec l'enfant/ discuter des prochaines étapes
- impliquer **l'école** et les **parents de l'auteur des faits**, le cas échéant
- Préparer les personnes concernées au fait que des images/vidéos peuvent réapparaître à plusieurs reprises

Pour les parents d'harceleurs

- chercher le dialogue avec toutes les personnes concernées et **remettre en question les motivations**
- Présenter les **conséquences** qui les attendent
- Chercher le dialogue avec la personne concernée/ses parents/l'école et obtenir des excuses/**une compensation/ une réparation**
- Demander la **suppression** immédiate de toutes les images/vidéos/commentaires

Captures d'écran conformes à la législation

Une capture d'écran réalisée rapidement et juridiquement valable est essentielle pour fournir une preuve d'une infraction et permettre une poursuite efficace par les autorités. Pour être valable, une capture d'écran doit contenir les éléments suivants :

- le commentaire en question
- la date et l'heure du commentaire
- le nom (d'utilisateur) de l'auteur présumé de l'infraction
- le contexte dans lequel le commentaire a été posté
- le nom (d'utilisateur) de la victime

SUGGESTION DE LIENS

Points de contact pour les consultations anonymes en ligne

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

Film éducatif interactif pour les élèves de l'école primaire

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

Conseils pour des captures d'écran juridiquement sûres sur différentes plates-formes

- 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

SCHULE

VEREIN

TIPP: HILFE SUCHEN IST WICHTIG!

Hi

Hi!

TELEFON BERATUNG

ONLINE BERATUNG
- SCHNELL
- ANONYM

CYBERMOBBING-HILFE.DE

FOTOS

VIDEOS

VERBREITUNG ÜBER WHATSAPP

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, ABER 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

À propos de l'animatrice

Katharina Krüger
Journaliste & chef de projet pour les offres pour enfants de l'ARD

À propos des intervenants

Ann-Kristin Gaumann
Pédagogue des médias & spécialiste en communication, gestion de projet en pédagogie des médias chez Juuuport e.V.

↗ www.juuuport.de

Lukas Pohland
Victime de cyberintimidation & fondateur de la plate-forme de conseil en ligne Cybermobbing Hilfe e.V.

↗ www.cybermobbing-hilfe.de

INTERNET, LIEU DU CRIME

– Comment protéger nos enfants
Protéger contre le cybergrooming

Le cybergrooming est une forme de violence sexuelle dans le cadre de laquelle des mineurs sont contactés de manière ciblée via les réseaux sociaux et les jeux en ligne afin d'initier des contacts sexuels. Souvent, les auteurs se font passer pour des jeunes de leur âge sur des forums de discussion ou avec l'aide d'IA et profitent de la candeur, de la confiance et du manque de conscience des risques chez les enfants pour établir une relation de confiance ou de dépendance avec leurs victimes.

LES AUTEURS PROCÈDENT SOUVENT DE LA MANIÈRE SUIVANTE

1. Établissement de contacts

L'établissement de contacts avec des mineurs s'effectue fréquemment de façon anonyme via des réseaux sociaux tels qu'Instagram et TikTok, des jeux en ligne comme Fortnite, ou des plateformes comme YouTube ou Twitch.

2. Gagner la confiance

Les harceleurs tentent d'abord d'instaurer un climat de confiance. Ils se montrent intéressés, compréhensifs et serviables, déclarent les mêmes intérêts et font des compliments ou des cadeaux (virtuels). Souvent, les auteurs de ces actes insistent déjà sur le passage à des services de messagerie non modérés avec option caméra, comme WhatsApp ou Skype.



3. Agressions sexuelles

Une fois qu'ils ont gagné la confiance des enfants ou des jeunes, les agresseurs orientent la conversation sur les expériences et les intérêts sexuels des mineurs. Ils envoient éventuellement eux-mêmes du matériel pornographique et demandent des photos ou des vidéos intimes de l'enfant ou du jeune. Il arrive même qu'ils proposent des rencontres personnelles pour établir un contact sexuel hors ligne.[1]

Qui et pourquoi ?

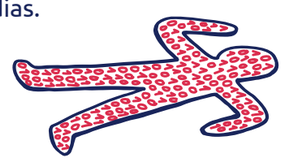
Les abus sexuels sont commis dans environ 80 à 90 % des cas par des hommes et des adolescents de sexe masculin, et dans environ 10 à 20 % des cas par des femmes et des adolescentes. Des études variées et des témoignages de personnes concernées montrent qu'il n'existe pas de personnalité unique de l'auteur. Seul le désir d'exercer le pouvoir et d'éprouver un sentiment de supériorité par l'acte les unit.

POURQUOI C'EST IMPORTANT POUR LES FAMILLES

Le harcèlement sexuel des mineurs en ligne n'est pas rare. Dans le cadre de l'étude JIM, 30 % des jeunes interrogés âgés de 12 à 19 ans ont déclaré avoir déjà été victimes de harcèlement sexuel en ligne. Les filles, avec 36 %, étaient nettement plus touchées que les garçons, avec 24 %, et 6 % subissaient même cela régulièrement chaque semaine. Ce phénomène se manifeste surtout sur Instagram (35 %) et TikTok (20 %). L'étude représentative « Kinder und Jugendliche als Opfer von Cybergrooming » (enfants et adolescents victimes de cyberharcèlement) de 2021, commandée par l'autorité de régulation des médias du Land de Rhénanie-du-Nord-Westphalie, donne des indications plus précises : « Près d'un quart des enfants et des adolescents (24 %) ont déjà été invités à un rendez-vous par des adultes sur le réseau. Un enfant sur six s'est vu promettre des contreparties par des personnes plus âgées s'il envoyait des photos ou des vidéos de lui. Un enfant sur sept a déjà été invité à se déshabiller devant une webcam ou à allumer la caméra de son téléphone portable et environ 15 % de tous les enfants ont reçu des photos de nus sans le vouloir. »[3]

CYBERGROOMING ET PROTECTION DES DONNÉES PERSONNELLES

Le risque de contacts involontaires à des fins criminelles via les canaux de médias sociaux ou les forums de discussion des jeux en ligne peut être évité par un comportement respectueux de la protection des données, combiné à des paramètres de confidentialité et de sécurité appropriés. L'information sur les dangers potentiels, tels que la diffusion d'images dénudées de et par des mineurs sur des profils publics, devrait être un élément important de l'éducation aux médias.



CES DROITS S'APPLIQUENT AUSSI EN LIGNE

Le cybergrooming, en tant que forme d'abus sexuel sur des enfants sans contact physique, est interdit en Allemagne conformément au § 176 du code pénal.

« Quiconque harcèle des enfants et des adolescents sur Internet avec des intentions sexuelles doit s'attendre à des peines d'emprisonnement allant jusqu'à cinq ans », selon l'Office fédéral de la police criminelle.[4]

Les actes suivants sont concernés :

- **Prise de contact avec des mineurs** avec l'intention de commettre des **actes sexuels***
- Présentation de **matériel pornographique**
- **Motiver les enfants à commettre des actes sexuels**
- Création de contenus représentant des **abus** (§ 184b)

Depuis 2020, il est également punissable pour les auteurs de croire qu'ils communiquent avec un enfant de moins de 13 ans, alors qu'en réalité ils échangent avec un adulte, comme un parent ou un policier en civil.

***Bon à savoir :**

Il n'est pas nécessaire que des actes sexuels « réels » aient lieu, ni que l'enfant ait répondu aux messages. La simple prise de connaissance d'un tel message par l'enfant suffit à constituer une infraction.

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

CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

expliquer les risques aux enfants en fonction de leur âge

- parler avec les enfants des intentions et des méthodes des cybergroomers
- informer sur les dangers du sexting
- Afficher les fonctions de notification et de blocage
- s'informer sur les centres d'accueil anonymes (voir les suggestions de liens)

Définir des règles pour l'utilisation et le partage d'images et de données en ligne

Sont à proscrire :

- les photos d'espaces privés et intimes, comme la chambre d'enfant
- les photos révélatrices et de nudité
- les images portant des indications (éventuellement cachées) sur le lieu de résidence
- les photos de profil avec des personnes identifiables
- les pseudonymes en rapport avec le sexe, le lieu de résidence ou l'âge
- Allumer la caméra (live cam) sans demander l'autorisation aux parents

Mettre en place des environnements en ligne protégés

- fournir des informations exactes sur l'âge pour le filtre de contrôle parental intégré
- Empêcher les étrangers de prendre contact avec vous (désactiver le chat)
- désactiver l'accès à la caméra lorsqu'elle n'est pas utilisée

Si une rencontre avec une personne inconnue du chat est prévue

- Afficher l'historique du chat
- Organiser la rencontre dans un lieu public
- Accompagner les rencontres

« Écoutez ton instinct ! Si quelque chose te semble bizarre, coupe le chat et bloque le contact. »

Klicksafe, campagne contre le cybergrooming

Ces SIGNAUX doivent vous mettre la puce à l'oreille lorsque vous discutez avec des inconnus :

- un nombre remarquable de compliments
- beaucoup d'approbation et de compréhension
- profil peu crédible : pas d'amis, nouvellement créé
- beaucoup d'intérêts similaires
- Invitation à passer le plus rapidement possible à un chat privé avec fonction vidéo
- La question « Es-tu seul(e) ? »
- L'auteur dissimule sa propre identité (refus d'allumer la vidéo)
- les allusions sexuelles
- mettre la pression
- Demande de partage de photos intimes, de vidéos et de données personnelles
- Le chat doit rester secret, il ne faut surtout pas en parler aux parents

CONSEILS D'URGEN

Pour les personnes concernées

- interrompre immédiatement le contact en cas de sentiment de malaise
- se confier à un adulte
- sauvegarder l'historique de chat
- supprimer son propre profil et en créer un nouveau, plus sûr
- Repousser verbalement les potentiels agresseurs, par exemple ainsi :

« Laisse-moi tranquille ! »

« Je ne veux pas de ça ! »

« Ce que tu fais est interdit. Je vais le signaler à la police et porte plainte ! »

« Je vais raconter ce que tu fais pour que tu ne puisses pas embêter d'autres enfants. »

« J'ai enregistré tout ce que tu as fait. J'ai des preuves ! »

Pour les parents de personnes concernées

- Préserver les preuves grâce à des captures d'écran juridiquement valables
- Signaler le profil au propriétaire du site et le bloquer
- Déposer rapidement une plainte pénale auprès de la police / du poste de garde en ligne
- Envoyer une remarque au service des réclamations Internet
- Faire appel à des experts en protection des victimes, le cas échéant





SUGGESTION DE LIENS

Services de signalement en ligne pour le cybergrooming

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

Le cybergrooming expliqué aux enfants

- 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

Instructions pour la réalisation de captures d'écran juridiquement valables pour différentes plates-formes et différents systèmes d'exploitation

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

ANONYME POINTS DE CONTACT

Ligne d'écoute en cas de détresse
pour les enfants : 116111
pour les parents : 0800 – 111 0 550

Ligne d'aide pour les abus sexuels
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

BEWUSSTSEIN FÜR EIGENE DATEN

VIRTUELLES GELD

MINECRAFT

ROBLOX

FORTNITE

GEFAHREN:
PHYSISCHER & PSYCHISCHER SCHADEN!

PERSONEN MELDEN

DIREKT ZUR POLIZEI

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

À propos de l'animatrice

Katharina Krüger
Journaliste & chef de projet pour les offres pour enfants de l'ARD

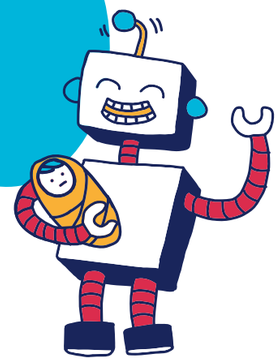
À propos des intervenants

Mario Tschirn
Inspection de police d'Anklam, prévention policière a.D.

Thomas Freitag
Office régional de la police criminelle de Mecklembourg-Poméranie occidentale, prévention policière

SMART FAMILY

L'IA, UN NOUVEAU MEMBRE DE LA FAMILLE



L'intelligence artificielle (IA) est un domaine de l'informatique qui s'occupe du développement de systèmes faisant preuve d'une intelligence proche de celle de l'homme, comme l'apprentissage, la résolution de problèmes et la prise de décisions. Ces systèmes utilisent des algorithmes et des modèles pour apprendre à partir de données et exécuter des tâches de manière autonome. L'IA trouve des applications dans de nombreux domaines : de la reconnaissance vocale au traitement d'images, en passant par les véhicules autonomes et les recommandations personnalisées.

POURQUOI C'EST IMPORTANT POUR LES FAMILLES

L'intelligence artificielle est partout et détermine de plus en plus souvent le quotidien des familles. Parfois, on ne se doute pas que les applications et les appareils sont des IA. Il vaut donc la peine de se pencher sur les outils intelligents qui peuvent être utiles dans la vie quotidienne de la famille, de vérifier s'ils fonctionnent à base d'intelligence artificielle et d'identifier les points nécessitant de la prudence, surtout lorsqu'il s'agit de données personnelles sensibles.
Les appareils intelligents suivants peuvent être envisagés dans un foyer familial :

Appareils intelligents



- Aspirateurs intelligents
- SmartTV
- Enceinte intelligente
- Jouets intelligents
- Caméras de surveillance intelligentes
- Traceur de fitness

IA générative

- Outils de traduction (DeepL, Google Translate)
- Générateurs d'images (Luminar AI, Adobe Sensei, Canva)
- Chatbots ou modèles linguistiques (ChatGPT, Mistral AI)

L'IA comme source d'idées et de possibilités

Les chatbots d'intelligence artificielle, en particulier, peuvent très bien être utilisés comme **source d'idées** dans le quotidien scolaire. L'objectif n'est pas de se contenter de solutions prêtes à l'emploi, mais de recevoir une première impulsion pour continuer à travailler à partir de là.

En tant que **tuteur**, une IA est un bon soutien pour de nombreux parents. Dans les moments où ils n'ont pas de réponses ou de solutions eux-mêmes, ils peuvent utiliser une IA pour faire des recherches.

En général, il est recommandé de tester l'IA en famille et de comprendre quelles sont les possibilités et les limites.

Les aspirateurs intelligents ou les assistants vocaux peuvent ici être de bons assistants ménagers au quotidien.

IA ET PROTECTION DES DONNÉES

Lors de l'utilisation d'appareils et d'applications intelligents, il convient de vérifier si elle utilise des données à caractère personnel et comment celles-ci doivent être protégées. Les systèmes d'IA basés sur **l'apprentissage automatique** ont généralement besoin d'une grande quantité de données (éventuellement personnelles) pour fonctionner. Cela concerne en particulier la phase d'apprentissage et la phase opérationnelle. Si ces données ne sont pas correctement protégées, des personnes ou des organisations non autorisées peuvent y avoir accès, ce qui peut aller de la divulgation non autorisée à l'usurpation d'identité en passant par la falsification (involontaire) des données.

La prudence est de mise, en particulier pour les systèmes d'IA qui utilisent des **technologies telles que la reconnaissance faciale ou les empreintes digitales**. Ces données très sensibles doivent être particulièrement protégées et ne doivent pas tomber entre de mauvaises mains.

Les outils d'intelligence artificielle générative collectent et enregistrent souvent les demandes et les réponses des utilisateurs. Les entreprises analysent ensuite ces données d'interaction et les utilisent pour former de futurs modèles.[1]

Les pirates informatiques utilisent des systèmes d'apprentissage automatique pour des attaques d'ingénierie sociale ou des fraudes par hameçonnage. Ils génèrent des e-mails, des documents, etc. crédibles, qui introduisent des logiciels malveillants ou volent des informations d'identification.[2]

CES DROITS S'APPLIQUENT À L'IA SUR INTERNET

Le règlement sur l'IA (Engl. Artificial Intelligence Act, abrégé **AI Act**) est un règlement de l'Union européenne visant à réglementer le développement et l'utilisation de l'intelligence artificielle. Le règlement vise à garantir que les systèmes d'IA soient sûrs, transparents et compatibles avec les valeurs de l'Union européenne.

Ainsi, les contenus créés artificiellement, comme les vidéos ou les images, doivent être identifiés comme tels.



***Bon à savoir :**

Les appareils intelligents et l'IA sont deux choses différentes. Les appareils intelligents offrent souvent des fonctions automatisées et sont connectés, mais ils ne doivent pas nécessairement disposer d'une IA.

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

CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

S'informer sur les produits basés sur l'IA et sur le fabricant avant l'achat

- Dans quelle mesure les données sont-elles collectées, enregistrées et transmises à des tiers ?
- Est-il possible d'activer le mode veille sur l'appareil/le programme ?
- Quels sont les réglages de sécurité que l'on peut effectuer sur l'appareil/le programme ?
- Est-il possible de désactiver l'entraînement de l'IA ?
- L'appareil existe-t-il sans IA ?
- L'IA présente-t-elle une réelle utilité dans l'appareil ?

S'informer et éduquer sur les dangers

- Vérifier le potentiel d'addiction lorsque les applications d'IA déterminent le quotidien
- utilisation abusive par l'imitation de la voix à l'aide de l'IA
- Les images peuvent être facilement générées et utilisées de manière abusive : Deepfake
- L'IA peut renforcer la cyberintimidation par l'utilisation de bots automatisés

Conseils pour l'utilisation de l'IA

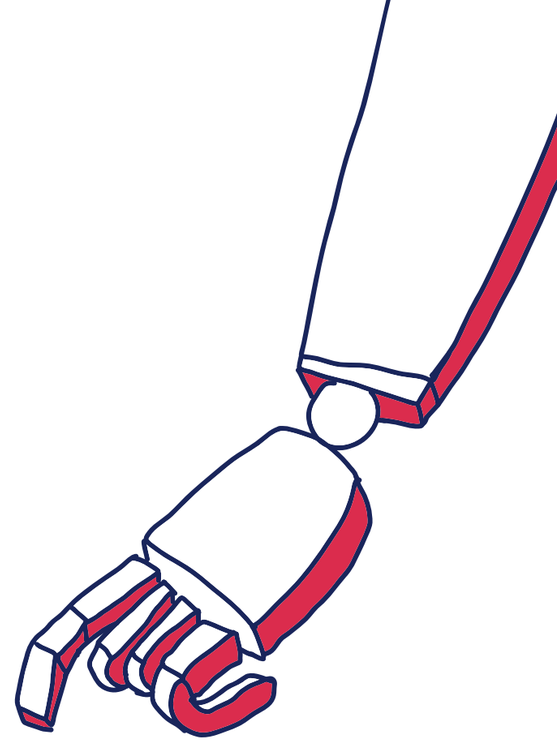
- ne pas divulguer d'informations sensibles lors de la saisie des ordres de travail (prompts) (mots de passe, noms, anniversaires, numéros de téléphone, données relatives à la santé, etc.)
- Vérifier l'exactitude des informations, des sources et des déclarations d'une IA
- Aiguiser la capacité de réflexion de l'utilisateur : Les images et les textes sont-ils générés par l'IA ? S'agit-il de deepfakes ?
- Aborder le thème de la durabilité : IA et consommation d'énergie
- d'abord apprendre par soi-même, ensuite utiliser l'IA
- Indiquer les prompts pour les textes (s'ils n'ont pas été modifiés individuellement) et les images comme source
- informer de la présence d'un assistant vocal actif lors d'une visite à domicile et le désactiver sur demande
- Désactiver l'accès à la caméra lorsqu'elle n'est pas utilisée

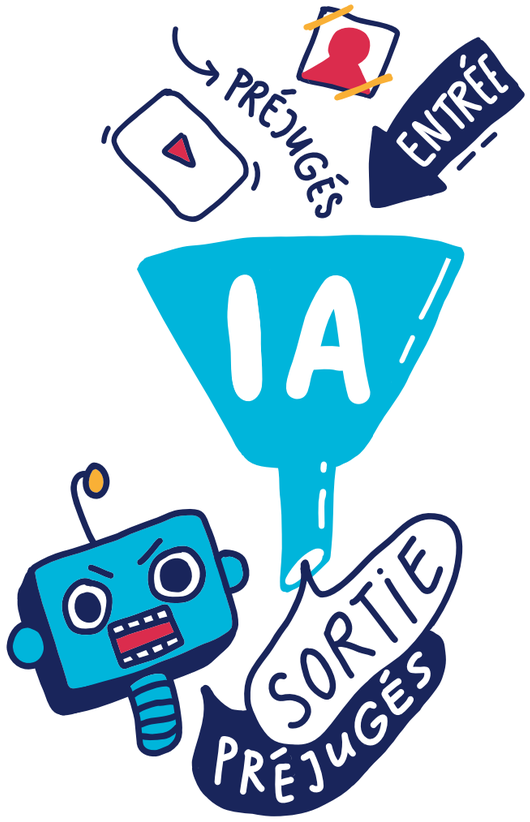
« Nous sommes tous confrontés à l'intelligence artificielle au quotidien. C'est pourquoi nous devrions apprendre à mieux comprendre son fonctionnement et son influence sur nos décisions. »

Extrait du webinaire « Smart Family » du 06.03.2024 par **Prof. Dr. Sandra Schulz**, professeure junior d'informatique et de didactique à l'Université de Hambourg

PERSPECTIVE ÉTHIQUE

Dans de nombreux cas, une IA peut apprendre en permanence grâce aux nouvelles données saisies par les utilisateurs. Cela signifie que le type d'entrées et de contenus utilisés pour former une IA peut influencer ses sorties en conséquence. Lorsqu'une IA a été nourrie de textes et de déclarations discriminatoires, elle les rejoue en conséquence, ce qui peut consolider et renforcer certaines attitudes dans la société. Une IA peut amplifier le phénomène des bulles de filtre, de sorte que les opinions existantes sont ainsi encore plus renforcées. C'est pourquoi les réponses de l'IA doivent toujours être considérées de manière critique et ne devraient pas être adoptées sans réflexion.





SUGGESTION DE LIENS

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

LIVRE CONSEILLÉ

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

#Digitale Vorbilder

SMART FAMILY

KI ALS NEUES FAMILIENMITGLIED

MODERATION: NICOLE AHLES



CAN I HELP U?

TIPP: EIGENLEISTUNG UNTERSTÜTZEN

AMAZON BEWERBUNGS-KI BENACHTEILIGTE FRAUEN

HAMBURGER DATENSCHUTZ

TIPP: CHECKLISTE FÜR UNTERNEHMEN

UMGANG MIT DATEN... ETHISCHE LEITLINIEN

GUCK MAL!

00000 1000
1100 0100
0100 0110 0 1

ALGORITHMUS
=EMPFEHLUNGEN
WAHRSCHEINLICHKEITEN

WER WEIß WAS ÜBER MICH?

TIPP: ERST SELBER LERNEN & DANN TOOLS ALS SUPPORT

INSPIRATION

ÜBERSETZUNGSTOOLS:
DEEPL
CHAT GPT

KI ALS IDEENGEBER

GEFÄLLT DIR DAS?

EXPERTE: TORSTEN OTTO



IST STREAMING NACHHALTIG? SEHR HOHER STROMVERBRAUCH

TIPP: RUHEMODUS AKTIVIEREN



ALEXA...

WO? STEHT ALEXA WANN? HÖRT SIE MIT?

MISSTRAUISCH SEIN!

GERÄTE HÖREN MIT
- PASSWÖRTER
- GESUNDHEITSDATEN
- PRIVATE GESPRÄCHE
...

SPRACHERKENNUNG
↳ BESUCHER·INNEN INFORMIEREN

GRAPHIC RECORDING @elibreuing

MEINE FREUNDIN ROXY

BUCH-EMPFEHLUNG

EXPERTIN: PROF. DR. SANDRA SCHULZ



Hi



medienzeiten FESTLEGEN!

HEJ SIRI!

P

HANDY PARKPLATZ

PROMPTS MÜSSEN ALS QUELLE ANGEGEBEN WERDEN!

TIPP: GEMEINSAM AUSPROBIEREN VONEINANDER LERNEN

À propos de l'animatrice

Nicole Ahles
Présentatrice et journaliste

À propos des intervenants

Sandra Schulz, professeur
Professeure junior de didactique et d'informatique à l'université de Hambourg

Torsten Otto
Professeur d'informatique au Lycée Kurt Körber de Hambourg

JOUETS INTELLIGENTS



Les jouets intelligents sont connectés par Bluetooth ou Internet et peuvent interagir avec leur environnement. Les Poupées, robots, peluches, drones ou voitures sont équipés de capteurs, de microphones ou de caméras pour offrir une expérience ludique qui s'adapte aux besoins et aux préférences de l'enfant.

POURQUOI C'EST IMPORTANT POUR LES FAMILLES

La famille ou le domicile est un lieu particulièrement digne de protection. C'est là que se déroulent les conversations privées et très intimes qui, dans le meilleur des cas, ne sont pas divulguées à l'extérieur. Les jouets intelligents, de plus en plus populaires, offrent des expériences interactives et éducatives aux enfants.

Toutefois, avant d'acheter un jouet intelligent, les parents devraient se renseigner sur les éventuels problèmes de sécurité et sur l'étendue de son utilisation.

Il est important de trouver un équilibre entre les possibilités d'apprentissage innovantes et la **protection de la vie privée**.

[1] cf. Verbraucherzentrale 2023

[2] cf. heise online 2024

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

[4] cf. BVL 2024

JOUETS INTELLIGENTS ET PROTECTION DES DONNÉES

Les jouets intelligents se connectent à Internet et s'adaptent individuellement aux besoins et aux préférences des enfants. Selon le jouet, des enregistrements audio, des photos, des vidéos, des données de localisation, des données d'utilisation et des informations sur l'appareil sont enregistrés et combinés pour former un **profil de comportement**. Ce système permet aux entreprises d'offrir à leurs clients des expériences personnalisées, d'améliorer les interactions, de mieux adapter le contenu aux intérêts des enfants et de diffuser des **publicités personnalisées**.[1]

Comme le montre une étude récente de l'Université de Bâle, outre l'établissement de profils de comportement des enfants, le **manque de transparence** dû à des informations insuffisantes et difficilement accessibles sur la **collecte et le traitement des données** est largement répandu parmi les fabricants de jouets intelligents, qui sont tenus de le faire en vertu du principe de transparence du **RGPD**.[2]

Les familles qui décident d'acheter un jouet intelligent doivent être conscientes des **risques** au préalable.

Les voies de **transmission insuffisamment sécurisées** via Bluetooth ou WLAN, d'une part, et les lieux de stockage **non conformes au RGPD**, d'autre part, constituent des portes d'entrée potentielles pour les criminels intéressés par les quantités de données collectées.

Ainsi, des données telles que le nom, les coordonnées, l'âge et les préférences de l'enfant, les coordonnées bancaires peuvent être récupérées sans autorisation par des pirates informatiques sur des serveurs de fabricants mondiaux insuffisamment sécurisés et utilisées à des fins **d'usurpation d'identité**.

Si le réseau domestique est contrôlé par le compte principal, un tel **piratage de données** met en danger non seulement les données et les informations privées des appareils intelligents, mais aussi éventuellement les données d'accès aux e-mails, aux comptes de médias sociaux et même aux comptes bancaires.[3]

Si les équipements de jeu intelligents utilisent par exemple des **connexions Bluetooth sans protection individuelle par mot de passe**, tout propriétaire de smartphone à portée de cet appareil pourrait espionner des moments intimes de la vie de la famille et, en théorie, entrer en contact avec l'enfant via le microphone. La prise de conscience que son domicile est surveillé par des appareils intelligents peut entraîner des **changements de comportement** chez les parents et les enfants et provoquer un **stress psychologique**, une peur et une insécurité considérables.

Sans paramètres de confidentialité appropriés, le profil de mouvement établi par un **traceur GPS** dans un appareil intelligent (par exemple une montre intelligente) peut tomber involontairement entre les mains de tiers. En combinaison avec d'autres données de profil de l'enfant, cela représente un risque pour la sécurité.

CES DROITS S'APPLIQUENT AUX JOUETS INTELLIGENTS EN LIGNE

Afin de protéger la sécurité des enfants en particulier, l'Agence fédérale des réseaux a interdit en 2017 les jouets intelligents dotés de fonctions d'écoute via le monitoring vocal. Il s'agit d'appareils et de jouets qui enregistrent secrètement des conversations ou filment leurs propriétaires et transmettent ces enregistrements sans fil à d'autres appareils.

Dans la plupart des écoles en Allemagne, l'utilisation de montres intelligentes avec une fonction d'écoute cachée est interdite, afin de protéger les droits généraux de la personne.

Malgré le **droit fondamental à la liberté et à la vie privée** en vigueur, le suivi de ses enfants par GPS est souvent une évidence pour les parents. Cependant, cela équivaut en même temps à une **surveillance permanente** des enfants. Dans ce cas, il convient de clarifier au préalable, en concertation avec les parents et les enfants, les **règles** en vigueur **dans la famille** à ce sujet.

Les drones équipés d'une caméra sont interdits aux enfants de moins de 16 ans dans toute l'UE, sauf s'ils sont couverts par la directive 2009/48/CE relative aux jouets.[4]



Comme les différents produits collectent et enregistrent des données de différentes manières, nous en présentons ici quelques-uns à titre d'exemple :

Poupées et peluches parlantes

Ces jouets sont équipés de **microphones et de haut-parleurs** afin de pouvoir interagir avec les enfants. Ils enregistrent les voix et les conversations, les informations sur les interactions et la progression de l'apprentissage, qui sont envoyées au serveur du fabricant pour le stockage, le traitement et l'analyse des données.

Wearables pour enfants

Les wearables, c'est-à-dire les appareils que l'on porte sur soi, comme les smartwatches, les fitness trackers ou les GPS trackers, sont connectés à Internet et peuvent être contrôlés via une application smartphone. Ils fournissent par exemple des informations sur la localisation de l'enfant et établissent des **profils de mouvement et d'activité**.

Voitures-jouets connectées, drones et réalité augmentée (RA)

Ces jouets permettent des transmissions en direct, enregistrent des trajets ou des vols et envoient ces données à des appareils connectés.

Jouets éducatifs intelligents

Ces jouets sont souvent équipés de capteurs et de processeurs qui permettent une interaction avec l'enfant. Ils proposent souvent un contenu éducatif ou des activités ludiques personnalisés, basés sur les progrès de l'enfant.

Ils enregistrent la durée et la fréquence d'utilisation et peuvent collecter des informations personnelles, telles que l'âge et le nom de l'enfant, ainsi que des données sur les progrès de l'apprentissage, les réponses aux tâches et les évaluations. Les jouets dotés d'un système de reconnaissance des émotions permettent en outre de collecter des données sur la réaction émotionnelle de l'enfant à différentes activités d'apprentissage.

Babyphones avec fonctions avancées

Les babyphones modernes sont souvent plus que de simples appareils de transmission audio. Ils sont équipés de capteurs de mouvement, de caméras à vision nocturne et d'un système de surveillance de la température et transmettent les données par radio ou WLAN.

CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

S'informer avant d'acheter

- N'acheter que des appareils intelligents de fabricants de confiance dans le champ d'application du RGPD
- Consulter les tests de consommateurs et les informations sur les produits
- Clarifier les risques de sécurité, tels que le vol et le stockage des données
- Prendre au sérieux les recommandations d'âge
- Clarifier les risques pour la vie privée

Pendant l'utilisation

- Divulguer le moins de données personnelles possible
- Limiter l'accès aux données inutiles dans les paramètres des appareils et des applications





- Effectuer régulièrement les mises à jour de sécurité
- Protéger le réseau domestique par des mots de passe forts et une **configuration sécurisée du routeur**
- Préférer l'utilisation hors ligne de l'appareil[1]
- Désactiver ou masquer les caméras/microphones lorsqu'ils ne sont pas utilisées



CONSEILS D'URGENCE

En cas de piratage de données

- déconnecter immédiatement le jouet concerné d'Internet afin d'éviter toute nouvelle perte ou utilisation abusive de données
- changer tous les mots de passe définis pour le jouet et ses applications
- **Informer le fabricant du jouet** pour signaler le problème et obtenir des conseils
- Informer **l'autorité de contrôle compétente en matière de protection des données** en cas de perte de données personnelles
- en cas d'infraction grave, engager **une action en justice** contre le fabricant ou le fournisseur (dommages et intérêts)
- **Contacter les organisations de protection des consommateurs** pour obtenir des conseils en cas d'abus ou d'utilisation inappropriée

[1] cf. BSI 2024: Smart Toys



SUGGESTION DE LIENS

Ce à quoi les parents doivent faire attention avant l'achat

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

En cas de doute sur l'interdiction d'un jouet particulier, l'Agence fédérale des réseaux (Bundesnetzagentur) peut vous aider

↗ 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

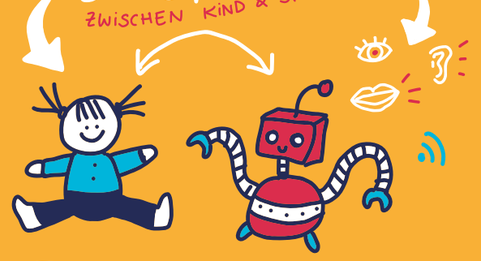


COGNI TOYS

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

MISSBRAUCH DATENNUTZUNG FÜR MOBBING

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

TIPP: ·BUNDES-NETZ-AGENTUR ·DSGVO

BNetzA

TIPP: VERBRAUCHER-SCHUTZ

GRAPHIC RECORDING @elibrewing

À propos de l'animatrice

Antje Kießler
Présentatrice & journaliste

À propos de l'intervenante

Jessica Wawrzyniak
Spécialiste de l'éducation et des médias, conférencière, auteur

INSTRUCTIONS RELATIVES À L'UTILISATION DES SERVICES DE MESSAGERIE

Les services de messagerie sont des plateformes de communication numériques permettant d'envoyer des messages instantanés sous forme de texte, d'images, d'audio ou de vidéo entre deux ou plusieurs partenaires de communication via une connexion Internet.

Les discussions de groupe et les canaux peuvent justement être utilisés pour récupérer des données ou diffuser des contenus punissables.

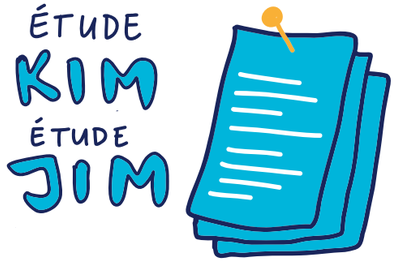
POURQUOI C'EST IMPORTANT POUR LES FAMILLES

Selon la dernière étude JIM, 96 % des jeunes possèdent leur propre smartphone et passent en moyenne 224 minutes par jour en ligne. Dans ce contexte, le service de messagerie WhatsApp est considéré comme l'application de loin la plus importante par 74 % des jeunes interrogés.

Par rapport aux services de messagerie actuellement sur le marché, WhatsApp est le plus utilisé par les jeunes (94 %). En comptant les adultes, 86 % de tous les utilisateurs de Messenger utilisaient l'application en 2023, d'après un sondage de Statista.

Les alternatives à WhatsApp en matière de messagerie sont loin de concurrencer le leader du marché en termes d'utilisation : Telegram est utilisé par 10 % des jeunes interrogés, Signal par 9 % et Threema par 3 %. Ces deux derniers services de messagerie peuvent être considérés comme moins préoccupants du point de vue de la protection des données.

Il existe des services de messagerie qui se sont engagés à respecter des valeurs telles que la vie privée, la sécurité et la transparence. C'est à vérifier régulièrement !



SERVICES DE MESSAGERIE ET PROTECTION DES DONNÉES

Du point de vue de la protection des données, il y a certains aspects à prendre en compte pour les services de messagerie.

Les discussions de groupe et les canaux sont à considérer d'un œil critique. Il existe ici un risque selon lequel dans de grands groupes anonymes, des inconnus puissent voir le numéro de téléphone et la photo de profil déposée avec le nom et le texte de description. Les **paramètres de confidentialité** du service de messagerie peuvent aider à prévenir ce phénomène.

Attention aux messages de statut : Chaque contact enregistré peut consulter ses propres messages d'état conformément aux paramètres prédéfinis. Pour ceux qui ne le souhaitent pas, il est conseillé de mettre régulièrement à jour les contacts exclus via les réglages de confidentialité, ou de ne pas utiliser les statuts du tout.

Les services de messagerie avec **cryptage de bout en bout**, y compris les discussions de groupe, sont recommandés. Sans cela, il est possible à des tiers ainsi qu'au fournisseur lui-même de lire les contenus et d'intercepter les données

CES DROITS S'APPLIQUENT AUSSI EN LIGNE

Toute personne qui est membre d'un groupe de discussion (éventuellement anonyme) ou abonnée à une chaîne court le risque d'être destinataire de **contenus réprimandables**. Ces contenus peuvent être **préjudiciables au développement** et traumatisants pour les enfants et les adolescents.

Les contenus interdits comprennent, entre autres :

- Symboles anticonstitutionnels
- Incitations au crime
- Incitation à la haine
- Négation de l'Holocauste
- Approuver, nier et minimiser le génocide
- Crimes contre l'humanité et crimes de guerre
- Glorification de la violence et atteinte à la dignité humaine
- Diffusion de contenus pornographiques, y compris la pornographie enfantine ou impliquant des animaux, etc.
- Menaces de violence

La **diffusion de ces contenus** est interdite en Allemagne et peut donner lieu à une procédure pénale avec **amendes ou peines d'emprisonnement**. Jusqu'à l'âge de 18 ans, ces délits relèvent du droit pénal des mineurs.

La possession d'images et de vidéos pornographiques (impliquant des enfants) est déjà **punissable**.

Les services de messagerie ont besoin du carnet d'adresses pour afficher les contacts dans l'application. Avec WhatsApp, cela se fait de manière **automatisée** et ne peut pas être empêché. Ainsi, tous les contacts qui y sont enregistrés ainsi que les données correspondantes, telles que la photo de profil, le texte de description et le nom (même si ces contacts n'utilisent pas eux-mêmes WhatsApp) sont lus et transmis à la société mère Meta et à ses filiales Facebook et Instagram. Cela permet de compléter les profils et en outre de les transmettre à des partenaires (publicitaires) non spécifiés (également dans des pays non membres de l'UE). Cela arrive très rapidement lorsque le téléchargement automatique de contenus est activé.

[1] cf. BZgA 2024

Même les métadonnées qui peuvent être considérées comme inoffensives pour les utilisateurs sont collectées par les messagers **sans être cryptées**. Ces données sont intéressantes pour les annonceurs, car elles peuvent permettre d'analyser son comportement de communication.

Selon le service de messagerie et les paramètres, les données suivantes sont collectées et éventuellement réutilisées :

- Photos : Photo de profil, messages de statut, le cas échéant chats non cryptés
- votre propre numéro de téléphone et les contacts de l'annuaire téléphonique
- Métadonnées : Avec qui a-t-on communiqué, à quelle fréquence et pendant combien de temps ? Combien de temps en ligne ? fréquence d'utilisation, adresse IP et informations sur l'appareil (numéro de modèle, version du système d'exploitation, version de l'application, code pays, code réseau, informations d'utilisation telles que la date d'enregistrement, type d'utilisation)
- Localisation à partir du GPS, du WLAN et des données mobiles
- Nom d'affichage
- Date de naissance
- Messages encore non reçus (serveur)
- Informations sur les appels, telles que l'heure, le numéro de téléphone et le numéro de l'appareil

Attention à la **reprise involontaire de comptes par des inconnus lors d'un changement de contrat de téléphonie mobile.** En raison du lien entre le profil WhatsApp et le numéro de téléphone, il peut arriver, en cas de réattribution de l'ancien numéro de téléphone, que la personne ait désormais accès à un profil WhatsApp existant, y compris l'historique des discussions et les contacts. C'est pourquoi il faut toujours informer WhatsApp en cas de changement de numéro d'appel et, par mesure de sécurité, mettre en place une authentification à deux facteurs.[1]

[1] cf. Verbraucherzentrale 2024

CE QUE LES PARENTS PEUVENT FAIRE À TITRE PRÉVENTIF

Choisir un service de messagerie respectueux de la vie privée

Les informations suivantes peuvent être tirées des **conditions générales et des conditions d'utilisation** :

- Quelles données sont stockées, où et pendant combien de temps ?
- Quelles informations sont transmises à des tiers (partenaires publicitaires) ?
- Quels sont les droits d'image que je cède lorsque je les télécharge ?
- Si l'application est gratuite, comment est-elle financée ?
- Existe-t-il un cryptage intégré de bout en bout pour les conversations individuelles et de groupe ?
- Est-il possible de configurer des messages auto-effaçables ou de les supprimer rétroactivement de l'historique de chat ?
- Est-il possible de désactiver le partage de l'emplacement ?
- Peut-on refuser de partager son carnet d'adresses ?
- Est-il possible d'empêcher l'affichage de la photo de profil et du numéro de téléphone portable dans les discussions de groupe ?
- À partir de quel âge le service est-il adapté ?

La classification par âge correspond-elle à l'âge de mon enfant ?

Les dangers liés à l'utilisation des services de messagerie sont nombreux et les tranches d'âge indiquées sont différentes. Les informations correctes se trouvent dans les conditions générales. Il est important de savoir que les indications figurant dans les app stores ne sont pas toujours correctes. Si l'USK a évalué le service, elle n'a évalué que le fonctionnement.

Faire des réglages préalables avec l'enfant/le jeune

- Pseudonymiser les informations du compte (ni nom en clair ni photo de profil identifiable)
- Configurer le verrouillage des applications
- Limiter :
  - le partage de l'emplacement
  - le partage des données de contact (numéro de téléphone, informations, photo de profil)
  - la sélection et la discussion du statut d'activité (dernière connexion, confirmation de lecture)
  - la portée des messages de statut
  - l'autorisation d'être ajouté à des groupes
- Désactiver les téléchargements automatiques des images/vidéos partagées et la sauvegarde supplémentaire sur l'appareil
- Donner au cache un délai d'expiration pour que les données locales soient effacées après un certain temps
- Effectuer des réglages standard, comme la durée de stockage, les messages auto-effaçables, pour l'envoi de messages
- Explorer les fonctions de signalement et de blocage
- le cas échéant, fixer une limite de temps sous la fonction Digital Well-being dans l'application

Règles d'utilisation pour la communication

- choisir un ton respectueux
- Définir des règles pour le partage de contenu : Qu'est-ce qu'un contenu punissable ?
- s'arrêter un instant avant d'envoyer et réfléchir à qui doit voir les photos, les vidéos et les messages
- ne pas transmettre de chaînes de lettres
- prendre activement position dans les discussions de groupe lorsqu'une personne est harcelée
- définir des règles et des conséquences pour le chat de la classe en cas de violation des règles et désigner un administrateur

CONSEILS D'URGENCE

- quitter un chat de groupe douteux
- Supprimer le compte (pas seulement l'application !)
- utiliser un service de messagerie alternatif
- demander un nouveau numéro (opérateur de téléphonie mobile)

SUGGESTION DE LIENS

Centre de signalement en ligne pour la pornographie enfantine, l'extrémisme et la cybercriminalité

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

Conseils de la police sur les contenus punissables

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

Comparaison des services de messagerie alternatifs

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

Règles pour les discussions de groupe

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

Bibliographie

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

Achats in-app

Les achats in-app sont des contenus, articles, abonnements ou services supplémentaires que l'on peut acheter au sein d'une application. La plupart du temps, les applications sont gratuites en soi, mais elles peuvent rapidement devenir un piège financier en raison des achats in-app.

Admin

Un admin(istrateur) est une personne qui, par exemple dans les groupes de messagerie ou les comptes de médias sociaux, joue un rôle prépondérant dans un groupe et a plus de droits que les participants normaux, comme l'ajout et la suppression de participants ou l'établissement et l'application d'un code de conduite.

Adresse IP

Une adresse IP (Internet Protocol Address) est une suite de chiffres attribuée à chaque appareil connecté à un réseau informatique ou à Internet. Les adresses IP permettent d'identifier les appareils en ligne, tels que les ordinateurs ou les téléphones portables.

Agence fédérale des réseaux

L'Agence fédérale des réseaux pour l'électricité, le gaz, les télécommunications, la poste et les chemins de fer (BNA) est l'autorité fédérale supérieure responsable de tous les réseaux publics en Allemagne. Depuis l'entrée en vigueur du Digital Services Act, elle est également responsable de la surveillance des règles qui y sont fixées. Si les fournisseurs d'accès à Internet ne donnent pas suite aux informations sur les contenus et produits illégaux ou restent inactifs face aux messages de haine et aux fausses informations, il est possible de déposer une plainte auprès de la BNA.

Algorithme

Dans le domaine de la programmation informatique, les algorithmes sont des instructions qui indiquent à l'ordinateur comment et dans quel ordre il doit exécuter une tâche. Toutes les applications et tous les appareils numériques fonctionnent sur la base d'algorithmes.

Amende

Une amende est infligée par les autorités ou les tribunaux pour sanctionner une infraction au droit civil. Il faut la distinguer de l'amende qui, en droit pénal, vise à sanctionner une infraction.

App

App est l'abréviation de « Application Software » et signifie en quelque sorte « logiciel d'application ». Ces programmes supplémentaires permettent d'étendre à volonté les fonctions des terminaux numériques.

Assistant vocal

Les assistants vocaux fonctionnent à l'aide de l'intelligence artificielle, qui permet d'interagir avec les appareils et applications électroniques. Grâce à l'écoute permanente de l'environnement, un assistant vocal peut, après avoir été activé par un mot-clé, réagir à une commande vocale correspondante.

Authentification à deux facteurs

Dans le cas de l'authentification à deux facteurs (2FA), il existe, en plus du mot de passe, un deuxième facteur, indépendant du premier, pour prouver l'identité de l'utilisateur et par lequel la connexion à un compte doit être effectuée. Ce moyen indépendant, par exemple via un SMS, une application ou autre, permet d'éviter que des tiers non autorisés aient accès aux données ou aux fonctions de l'utilisateur simplement parce qu'ils sont entrés en possession du mot de passe.

Autorité de surveillance

Une autorité de contrôle de la protection des données est une autorité publique indépendante chargée de surveiller et d'appliquer les lois sur la protection des données. En Allemagne, chaque Land dispose de sa propre autorité de contact pour les plaintes, ainsi que d'un commissaire fédéral à la protection des données.

Bio

Bio est l'abréviation de biographie et décrit, sur les plateformes de médias sociaux, les informations de profil sous forme de mots, d'emojis, de hashtags ou de liens avec lesquels les utilisateurs se présentent aux autres utilisateurs.

Blocage des fournisseurs tiers

Les fournisseurs tiers sont des entreprises qui proposent des produits ou des services sur des plateformes dont ils ne sont pas propriétaires. Un blocage des tiers est une fonction qui peut être activée auprès de l'opérateur de téléphonie mobile afin d'empêcher le paiement à des tiers via la facture de téléphonie mobile, au cas où des bannières publicitaires, des jeux-concours ou des liens auraient déclenché par inadvertance un piège à coûts.

Bloqueur de publicité (ou Ad-Blocker)

Un ad-blocker (en anglais, bloqueur de publicité) est un logiciel de filtrage qui permet de supprimer l'affichage de la publicité sur Internet.

Bots

Les bots (abréviation de l'anglais « robots » = robots) sont des programmes informatiques qui exécutent des tâches de manière automatisée. Des bots malveillants peuvent prendre le contrôle d'appareils numériques à distance et les utiliser ainsi pour attaquer des systèmes informatiques.

Canal

Les canaux Telegram ou WhatsApp permettent aux administrateurs de partager leur contenu avec un large public sous la forme de messages textuels, de liens vers des informations, d'images ou de vidéos. L'adhésion à un canal qui n'est pas crypté de bout en bout par défaut est volontaire. Ni le numéro de téléphone ni la photo de profil ne sont visibles pour les autres.

Capture d'écran

Une capture d'écran (screenshot en anglais) est une image de l'écran et non une photographie. Il sert de preuve, d'aide-mémoire, d'instruction ou de partage de contenus intéressants et peut être sauvegardé sous forme de fichier image en basse résolution.

Caractéristiques de sécurité

Les fonctions de sécurité sont des fonctions qui réduisent ou comblent les failles de sécurité risquées dans l'informatique afin de garantir la confidentialité, l'intégrité et la disponibilité des informations relatives aux utilisateurs, aux applications, aux appareils et au réseau, ainsi que des ressources physiques.

Caractéristiques identifiables

Les caractéristiques identifiables d'une personne sont, par exemple, son nom, un numéro d'identification, des données de localisation, un numéro de téléphone, un numéro de carte de crédit ou un numéro personnel, des données de compte, un numéro d'immatriculation de véhicule, son apparence, son empreinte digitale, son numéro de client ou son adresse.

Chaîne de lettres

Les chaînes de lettres sont des messages qui sont généralement diffusés via Messenger. Outre des messages inoffensifs et amusants, les chaînes de lettres contiennent souvent des tentatives d'escroquerie, des intimidations, des fausses nouvelles, des menaces ou même des prophéties de mort. Les lettres-chaînes de type « Horror » sont destinées à effrayer et à faire peur aux destinataires. On vous demande de transmettre le message au plus grand nombre de contacts possible, sinon quelque chose de grave est censé se produire.

Challenge

Challenge (angl. pour épreuve de courage ou défi) décrit un phénomène répandu sur les médias sociaux, dans lequel la plupart des jeunes relèvent un défi et le filment pour gagner des likes. Il y a des défis amusants, créatifs, mais aussi dangereux voire mortels.

Communauté (politiques)

Par communauté, on entend un réseau social organisé dans lequel des membres se retrouvent et échangent autour d'un objectif commun, d'une identité partagée ou d'intérêts communs. Les échanges entre eux se font dans le respect de règles communes sur les contenus et la manière de communiquer.

Contenu

Par contenu, on entend tout type de contenu médiatique diffusé par le biais de médias analogiques et numériques.

Cryptage de bout en bout

Le cryptage de bout en bout (angl. End-to-end encryption, EE2E) désigne le cryptage des données à transmettre afin de les protéger contre le vol et les abus. Personne, à l'exception de l'expéditeur et du destinataire, n'a accès aux contenus partagés avec EE2E, pas même le fournisseur de réseau ou le fournisseur du service de communication.

Deepfake

Le terme « deepfake » est la contraction de « deep learning » et de « fake » (qui signifie « faux » en anglais. Il désigne des contenus médiatiques d'apparence réaliste (photo, audio, vidéo, etc.) qui ont été modifiés, créés ou falsifiés par des techniques d'intelligence artificielle.

Droit d'auteur

Le droit d'auteur protège les prestations créatives, notamment dans le domaine de la culture et de l'art. Il régit l'exploitation économique des contenus créatifs, notamment par le biais de licences ou d'autorisations légales d'utilisation. Dans le cas des réseaux sociaux, le droit de reproduction et le droit de communication au public jouent un rôle central.

Duo

Par duo, on entend une fonction de TikTok permettant aux utilisateurs d'enregistrer des vidéos avec des vidéos TikTok existantes et de les lire simultanément, côte à côte.

Fake News

Les fake news sont de fausses informations diffusées dans les médias et sur Internet, en particulier sur les plateformes ou canaux de médias sociaux, dans un but de manipulation. Elles sont souvent motivées par des considérations politiques et servent à façonner l'opinion. Grâce à leur présentation professionnelle, ils ne sont souvent pas reconnaissables au premier coup d'œil.

Index

Fake-Shops

Derrière un Fake-Shop, ou fausse boutique, se cache une fausse plate-forme de vente sur Internet qui fait la promotion de bonnes affaires généralement très avantageuses pour des marchandises prétendument de grande qualité. Cependant, après le paiement par avance, la commande n'est pas livrée ou pas dans la qualité commandée.

Feed

Un flux dans les médias sociaux est un contenu continu de textes, d'images et de vidéos qui est affiché de manière centralisée pour les utilisateurs des plateformes de médias sociaux. Il peut s'agir de mises à jour d'amis ou de followers, ainsi que de contenus de pages ou de comptes suivis.

Fraude au CEO

La fraude au chef d'entreprise (CEO fraud en anglais) est une escroquerie qui consiste à inciter les collaborateurs d'une entreprise à verser une somme d'argent plus importante par e-mail ou par téléphone. Les criminels se font authentiquement passer pour un cadre supérieur.

Fuite de données, fuite de données, violation de données

Une fuite de données est un incident de sécurité résultant d'une erreur logicielle ou d'une action délibérée qui entraîne la perte ou la divulgation involontaire de données confidentielles et permet ainsi à des personnes non autorisées d'accéder à un fichier.

Gestionnaire de mots de passe

Un gestionnaire de mots de passe génère, stocke et gère des mots de passe complexes pour différents comptes en ligne de manière sécurisée et accessible. Un mot de passe maître sécurisé permet de garantir l'accès aux mots de passe complexes enregistrés.

GPS - Suivi ou localisation

GPS signifie « Global Positioning System ». Il s'agit d'un système de navigation par satellite qui permet de suivre en temps réel la position exacte d'un objet muni d'un tracker via la téléphonie mobile, le Wi-Fi ou les fréquences radio.

Hameçonnaage

Le phishing (de l'anglais fishing, pêche) est une cyberattaque qui utilise des e-mails frauduleux, des messages texte, des appels téléphoniques ou des sites web falsifiés pour inciter les gens à télécharger des logiciels malveillants ou à transmettre des données sensibles. Ceux-ci sont ensuite généralement utilisés à des fins illégales.

IA

L'intelligence artificielle (IA) est un domaine de l'informatique qui s'occupe du développement de systèmes faisant preuve d'une intelligence proche de celle de l'homme, comme l'apprentissage, la résolution de problèmes et la prise de décisions. Ces systèmes utilisent des algorithmes et des modèles pour apprendre à partir de données et exécuter des tâches de manière autonome.

Ingénierie sociale

L'ingénierie sociale consiste pour les cybercriminels à exploiter des caractéristiques humaines telles que la serviabilité, la confiance, la peur ou le respect de l'autorité pour manipuler les personnes afin de divulguer des informations confidentielles, de contourner des fonctions de sécurité, d'effectuer des virements ou d'installer des logiciels malveillants.

Le truc des grands-parents

Le truc des grands-parents ou du petit-fils ou de la petite-fille 2.0 est une escroquerie dans laquelle les auteurs se font passer pour des enfants ou des petits-enfants via Messenger et non plus, comme auparavant, par téléphone (truc des grands-parents version 1.0). L'auteur indique avoir un nouveau numéro de téléphone et demande à la victime de lui envoyer de l'argent en raison d'une situation d'urgence.

Leak ou **fuite**

Dans le cas d'une fuite, des contenus non autorisés sont rendus publics par une divulgation volontaire ou ciblée, alors qu'ils sont en fait confidentiels.

Let's Plays

Un let's play (de l'anglais « jouons ») permet aux spectateurs de participer à l'expérience de jeu d'autres personnes par le biais d'un enregistrement vidéo (screencast) drôle ou commenté de manière passionnante. Les lecteurs sont affichés dans un petit coin via une « facecam ».

Likes

Un like (mot anglais signifiant « J'aime ») est une évaluation positive d'une publication sur un réseau social. En comptant le nombre de likes, les utilisateurs peuvent savoir si un message posté a été bien accueilli.

Malware ou logiciel malveillant

Les logiciels malveillants (de l'expression anglaise « malicious software ») désignent des logiciels conçus dans le but d'exécuter des fonctions indésirables et généralement nuisibles sur un système informatique. Ils se propagent par le biais de pièces jointes à des e-mails, de pages web manipulées ou de supports de données.

Message ou notification push

Une notification push est un message généré par une application pour téléphone mobile lorsque l'application n'est pas ouverte. Elle s'affiche pour attirer l'attention sur un nouveau message, une mise à jour ou une offre promotionnelle.

Métadonnées

Les métadonnées sont des informations de niveau supérieur qui disent quelque chose sur d'autres données. Elles sont ajoutées à un fichier, comme par exemple le nom du fichier, la date de création, la taille du fichier ou de l'image ou encore des données géographiques. Mais les métadonnées comprennent également des informations telles que l'adresse IP ou l'information sur qui a communiqué avec qui et quand.

Navigateur (historique)

Un navigateur web permet d'afficher des pages web sur Internet. L'historique de navigation affiche les pages web visitées en dernier dans l'ordre chronologique. En outre, les métadonnées associées, telles que le titre de la page et l'heure de la visite, sont également stockées localement.

Nom clair

Un nom en clair est le nom qui figure sur les documents d'identité. Il se compose d'au moins un prénom ainsi que du nom de famille.

Pare-feu

Un pare-feu est un système de sécurité qui surveille le trafic de données et bloque les connexions indésirables ou dangereuses. Il protège le réseau contre les attaques et les menaces de tiers et permet une utilisation sécurisée du réseau.

Piège de l'abonnement

Le piège de l'abonnement est un type d'escroquerie sur Internet qui consiste souvent à conclure à son insu un abonnement payant dans le contexte d'une inscription en ligne.

Pornographie infantile

On parle de pornographie enfantine lorsque des photos ou des vidéos montrent des actes sexuels devant ou sur des enfants (de moins de 14 ans) ou lorsque des enfants commettent eux-mêmes de tels actes, par exemple parce qu'ils y sont contraints. Les photos ou vidéos montrant des enfants partiellement ou entièrement nus sont également considérées comme des contenus pédopornographiques.

Portée

La portée sur les réseaux sociaux est un indicateur du nombre d'individus qui ont vu une publication au moins une fois. Il convient de distinguer la « portée payée », c'est-à-dire le nombre de personnes sur l'écran desquelles des contributions payées ont été affichées.

Prank

Une farce désigne le fait de piéger délibérément une personne pour l'agacer, la provoquer ou l'effrayer. Sur les médias sociaux, les pranks sont connus parce que la préparation et les réactions des victimes sont filmées et mises en ligne.

Processeur

Un processeur (CPU) est une micropuce chargée d'effectuer des calculs et de traiter des données. En tant qu'unité centrale de calcul, il prend en charge la commande et la coordination de tous les processus du système.

Prompts

Un prompt est une demande formulée en langage naturel à une IA de fournir une réponse. Celui-ci est analysé par l'IA afin de générer une réponse basée sur l'entraînement précédent et le modèle appris à partir des données d'entraînement.

Pseudo

Un pseudo est nécessaire pour s'inscrire à des services en ligne, des messageries, des forums (de discussion) ou des plateformes. Il facilite la communication rapide et anonyme en ligne, sans divulguer de données personnelles.

Pseudonymisation

La pseudonymisation permet de protéger les données à caractère personnel. La pseudonymisation, par opposition à l'anonymisation, signifie que les personnes peuvent toujours être identifiées grâce à des informations supplémentaires qui font office de clés.

Réalité augmentée

La réalité augmentée désigne une perception ou une représentation assistée par ordinateur qui ajoute des aspects virtuels au monde réel par incrustation/superposition.

Index

Routeur (et sa configuration)

Un routeur est un dispositif matériel qui sert de point de connexion entre un réseau local (par exemple à la maison) et la connexion Internet physique sur le mur/la prise. La configuration du routeur consiste à configurer et à adapter un routeur afin de garantir des performances, une sécurité et une fonctionnalité optimales du réseau.

Scoring

Le scoring (évaluation en anglais) est l'estimation de la probabilité d'un certain comportement futur d'une personne physique, afin de décider si une relation contractuelle peut être établie avec cette personne. Le plus connu est le credit scoring, qui permet d'évaluer la solvabilité d'une personne.

Service cloud

Les services d'informatique en nuage (cloud en anglais) désignent les entreprises informatiques qui mettent à disposition des ressources accessibles via Internet, telles que la puissance de calcul, le stockage de données ou les applications. Pour garantir la disponibilité, les données à stocker sont souvent réparties dans des centres de données aux quatre coins du monde.

Sexting

Le mot « sexting » est composé des mots « sexe » et « texting » (de l'anglais « envoyer des messages ») et décrit le processus par lequel des personnes s'envoient mutuellement des messages, des photos ou des vidéos érotiques en ligne.

Sharenting

« Sharenting » est un terme issu de la contraction des mots « sharing » (partage en anglais) et « parenting » (parentalité). Il fait référence à la tendance des parents à partager des images, des vidéos ou des informations sur leurs propres enfants dans les médias sociaux.

Skins et tenues

Un skin (peau en anglais) dans les jeux en ligne, comme par exemple Fortnite, est une personnalisation cosmétique pour les personnages ou les objets présents dans le jeu. Les tenues sont appelées skins et permettent de personnaliser son personnage de jeu.

Story

Dans le domaine des réseaux médias sociaux, les stories (de l'anglais « histoires ») désignent de courtes séquences vidéo ou images qui se succèdent et qui sont utilisées comme messages de statut médiatiques et ne sont disponibles que pendant 24 heures. Les histoires peuvent être enrichies de manière créative par des emojis, du texte, de la musique, des autocollants, etc.

Tool

Un tool (de l'anglais « outil ») est un programme auxiliaire de petite taille qui effectue des tâches supplémentaires pour un système d'exploitation ou un programme d'application donné.

Tracking

Le tracking (de l'anglais « suivre ») désigne le suivi, l'enregistrement et l'analyse ultérieure du comportement des utilisateurs sur Internet. Dans ce contexte, il est intéressant pour les exploitants de sites web de savoir par quels sites web un visiteur est arrivé sur leur propre site, combien de temps une personne est restée sur le site, quelles pages ont ensuite été consultées et quelle est son adresse IP.

USK

L'USK (Unterhaltungssoftware Selbstkontrolle) est l'organisme officiel en Allemagne qui vérifie si les jeux conviennent à certaines tranches d'âge et les classe dans différentes catégories d'âge. Ces codes d'âge doivent aider à évaluer si un jeu est adapté aux enfants et aux adolescents.

Validation du site

Le partage de la localisation est une fonction du smartphone basée sur le GPS qui permet aux applications de savoir où se trouve l'utilisateur du smartphone, par exemple pour naviguer ou le localiser. Par le biais d'un Messenger, la position actuelle d'une autre personne ou d'un groupe peut être partagée en direct pendant une durée déterminée.

Views

View (de l'anglais « vues ») désigne le nombre de fois qu'un contenu publié a été vu. Il convient de faire la distinction entre les vues des stories, les vues de la page web et les vues de la vidéo. Ces derniers ne sont comptabilisés qu'à partir d'une durée de visionnage définie au préalable ou dès que la vidéo est lue, partagée, commentée ou que le compte est suivi. En règle générale, plus un article a de vues, plus sa portée et ses revenus sont importants.

Voice Monitoring

Voice Monitoring (de l'anglais « surveillance de la voix ») désigne la fonction d'écoute d'un appareil intelligent, comme une smartwatch par exemple. Dans ce cas, le microphone peut être activé à distance soit par une application, soit par une commande SMS, de sorte que toutes les voix et tous les bruits environnants peuvent être entendus sans être détectés.

Remerciements

Nous remercions chaleureusement toutes les personnes qui ont rendu possible le projet **#DigitaleVorbilder – Familien gehen online.** Nous tenons à remercier tout particulièrement les familles participantes qui ont partagé leurs expériences et leurs points de vue, ainsi que les experts qui ont largement contribué au succès du projet grâce à leurs connaissances et à leur soutien.

Nous remercions également nos partenaires, les membres du conseil consultatif et nos collègues qui nous ont accompagnés par leur aide active et leur confiance. Un saluons tout particulièrement l'Union européenne, qui a soutenu financièrement le projet et lui a ainsi apporté un soutien décisif. Ensemble, nous avons pu donner de précieuses impulsions pour le quotidien numérique des familles.

Un grand merci à tous ceux qui ont porté ce projet !



Mentions légales

Titre :
Guide d'orientation sur la protection des données Un guide destiné aux familles pour se repérer dans la jungle numérique (1ère édition, octobre 2024)

Publié par :
Le guide sur la protection des données a été élaboré par le projet européen #DigitaleVorbilder – Familien gehen online. (www.digitale-vorbilder.eu)

Un projet commun entre :
Le Délégué à la protection des données et à la liberté d'information du Land Mecklembourg-Poméranie occidentale
Werderstraße 74A, 19055 Schwerin
Tél. : +49 385 59494-0
E-mail : info@datenschutz-mv.de
Site web : www.datenschutz-mv.de

et

Le délégué hambourgeois à la protection des données et à la liberté d'information
Ludwig-Erhard-Straße 22, 20459 Hambourg
Tél. : +49 40 428 54 40 40
E-mail : mailbox@datenschutz.hamburg.de
Site web : www.datenschutz-hamburg.de

Rédaction : Lydia Roth, Christina Münster, Isabel Schlosshauer, Antje Kaiser
Couverture et graphiques : Eli Breuing
Droits photographiques : Sebastian Schmidt : EckiRaff |
Thomas Fuchs : Bildwerkstatt-Nienstedten
Mise en page : Caro Günther (Caros Colors)
Impression : WIRmachenDRUCK

Télécharger :
Le guide d'orientation peut être téléchargé en cliquant sur le lien suivant : https://datenschutz-hamburg.de/digitalevorbilder/mediathek.
Outre la version français, elle est également disponible au téléchargement en **allemande**, **anglais**, et **espagnol**.
Pour une commande, veuillez vous adresser à l'autorité de surveillance respective dans le Mecklembourg-Poméranie occidentale ou à Hambourg (voir les coordonnées ci-dessus).

Nous attirons votre attention sur le fait que, malgré le soin apporté au traitement des données, celles-ci sont fournies sans garantie et que toute responsabilité de l'éditeur est exclue.

La brochure est un produit du projet #DigitaleVorbilder - Familien gehen online. Financé par le programme « Citizens, Equality, Rights and Values » (CERV) de l'Union européenne.

La publication est placée sous la licence Creative Commons « Attribution - Pas d'utilisation commerciale - Pas de modification 3.0 Allemagne » (byncnd), ce qui signifie qu'elle peut être reproduite, diffusée et communiquée au public à volonté, sans modification, à des fins non commerciales, à condition de mentionner l'éditeur #DigitaleVorbilder. Le texte de la licence peut être consulté à l'adresse suivante : 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