Leena Simon und Philipp Uhlig

# Umgang mit Fotos

## safe – sane – consensual


digitalcourage

KURZ&MÜNDIG

Art d'Ameublement

Band 25

KOSTENFREI


**Das Internet ist voller Fotos.** Aber wie kommen die dorthin? Und wie schützen wir dabei unsere Privatsphäre? Die Kameras an unseren Smartphones werden immer besser, und fast alle Fotos landen im Netz. Weil aber ein Bild oft mehr sagt als tausend Worte, sollten Sie den Umgang mit Fotos kritisch hinterfragen. In dieser Kurz&Mündig-Ausgabe erklären wir, worauf es ankommt.

Dabei empfehlen wir, was wir nach unserer Expertise und Recherche für richtig halten. Dieser Text stellt allerdings keine Rechtsberatung dar.


## Impressum

1. Auflage 02-24, Art d'Ameublement, cc-by 4.0, ISBN 978-3934636-63-7

**Autorinnen:** Leena Simon, 🔗muendigkeit.digital, Philipp Uhlig

**Redaktion:** Katrin Schwahlen, 🔗katrinschwahlen.de

**Layout:** Isabel Wienold, 🔗iwi-design.de

**Bildlizenzen:** siehe Seite 26




## Beim Fotografieren und beim Verbreiten von Fotos gilt:

**safe** (sicher) → Wählen Sie zum Speichern einen sicheren Ort und entfernen Sie die Metadaten, ehe Sie ein Foto verbreiten.

**sane** (bewusst / vernünftig) → Machen Sie sich bewusst, dass sich ein Foto kaum jemals wieder zurückholen lässt. Was andere mit Ihren Fotos machen, können Sie nicht beeinflussen. Geben Sie keine Fotos von sich oder anderen weiter, mit denen jemand Schaden anrichten könnte.

**consensual** (einvernehmlich) → Holen Sie das Einverständnis aller Abgebildeten ein, ehe Sie ein Foto verbreiten.



# Fotos aufnehmen

Grundsätzlich sollten Sie auf Folgendes achten:

- Es gilt das Recht am eigenen Bild [🔗datenschutz.org/fotografieren-personen].
- Solange öffentliche Gebäude und Kunst an Hauswänden von öffentlichen Verkehrswegen aus zu sehen sind, dürfen sie in der Regel fotografiert und die Fotos veröffentlicht werden. Informieren Sie sich über Panoramafreiheit [🔗de.wikipedia.org/wiki/Panoramafreiheit].
- Bedenken Sie, dass das Smartphone Ihre Fotos ungefragt in die Cloud synchronisieren kann. Die abgebildeten Personen könnten etwas dagegen haben.
- Aufnahmen können für private Zwecke ohne ausdrückliches Einverständnis zulässig sein,
  - sofern Sie sie nicht verbreiten

  und
  - die Person sich nicht in einem gegen Einsehen geschützten Bereich aufhält

  und
  - nicht nackt und/oder minderjährig ist

  und
  - nicht eindeutig widersprochen hat

  und
  - nicht hilflos ist.

## Fotos speichern

Bewahren Sie Ihre Fotos zur Sicherheit nicht nur auf dem Smartphone oder in der Kamera auf, sondern auch anderswo. Dazu bieten sich viele Möglichkeiten, die Sie auch kombinieren können. Verzichten Sie aber auf die vorinstallierten kostenlosen Cloudangebote von Google, Apple und Co.

## Fotos lokal speichern (Back-up)

Eigene Fotos haben oft einen hohen emotionalen Wert. Das gilt ganz besonders für Bilder aus der eigenen Kindheit.

Egal, wo Sie diese Fotos speichern, auf eigenen Geräten oder in der Cloud: Legen Sie solche besonderen Dateien an mehreren Orten ab. Festplatten können zum Beispiel durch einen mechanischen Defekt unbrauchbar werden, Cloudanbieter können in rechtliche oder finanzielle Schwierigkeiten geraten und ihren Dienst einstellen.

Die beste Kontrolle über Ihre Fotos haben Sie, wenn Sie sie auf einer Festplatte daheim speichern. Denken Sie immer daran: Selbstgemachte Fotos sind unwiederbringlich weg, wenn sie einmal verloren gegangen sind!

Fertigen Sie deshalb (verschlüsselte) Kopien an und speichern Sie diese auf unterschiedlichen Medien. Mindestens ein Back-up-Datenträger sollte sich außerhalb Ihrer Wohnung oder Ihres Hauses befinden. Dadurch sichern Sie die Daten auch vor größeren Gefahren wie Brand, Überschwemmung, Blitzschlag oder Hausdurchsuchung.

Achten Sie darauf, zum Beispiel mit Hilfe einer Erinnerung im Kalender, das Back-up in regelmäßigen Abständen zu aktualisieren.

## Fotos im eigenen Netzwerk synchronisieren

Handys gehen schnell verloren. Viele Leute synchronisieren daher unterwegs gemachte Fotos auch mit ihrem Rechner, oft unter Einsatz eines kommerziellen Cloud-Dienstes. Das geht auch datenschutzfreundlicher:

Solange die Geräte sich im selben Netzwerk befinden, synchronisiert die freie App Syncthing [🔗syncthing.net] beliebige Dateien vollautomatisch und ohne Umwege. Wenn Sie ein Android-Gerät synchronisieren möchten, können Sie die App KDE Connect [🔗kdeconnect.kde.org] verwenden.

Beide Anwendungen synchronisieren Dateien so, dass sie dabei nie das eigene Netzwerk verlassen. Das gewährleistet Datensouveränität. Auch findet das Synchronisieren hier TLS-verschlüsselt statt, sodass selbst weniger vertrauenswürdige Geräte im selben Netzwerk nicht mitlauschen können.

Fortgeschrittene, die Programme gern selbst hosten, könnten mit Immich [🔗immich.app] glücklich werden.



## Fotos in einer Cloud speichern

Falls Sie eine eigene NextCloud betreiben, können Sie Ihre Fotos vollautomatisch dorthin übertragen lassen.

Aber es kommt darauf an, wo sich der Server befindet: zu Hause oder in einem Rechenzentrum. Sobald Sie Daten auf einen fremden Server laden, müssen Sie dem Anbieter ein Mindestmaß an Vertrauen entgegenbringen. Was auf einem fremden Server liegt, ist potenziell dem Zugriff Dritter ausgesetzt. Gerade Fotos können sensible Informationen enthalten und sollten daher nur wohlüberlegt aus der Hand gegeben werden.

Wenn Sie auf eine kommerzielle Cloud nicht verzichten können oder wollen, müssen Sie Ihre Fotos schützen. Am besten ist es, wenn die hochgeladenen Dateien nur für Sie selbst lesbar sind. Ver- und Entschlüsselung Ihrer Fotos sollten deshalb ausschließlich auf Ihren eigenen Geräten erfolgen. Wie das geht, können Sie im Blogbeitrag „Datenträger verschlüsseln“ auf 🔗digitalcourage.de lesen.

# Fotos teilen und veröffentlichen

Noch bevor Sie ein privates Foto mit irgendwem teilen, sollten Sie an die Metadaten denken, die Sie dabei womöglich übermitteln. Auch andere Informationen können aus den Fotos hervorgehen. Sie sollten immer bedenken, dass einmal versendete Fotos nicht „rückholbar“ sind. Wie groß das Risiko ist, müssen Sie von Fall zu Fall entscheiden und geeignete Vorsichtsmaßnahmen ergreifen.

## Kurz und bündig

Wenn Sie Fotos nur einer begrenzten Gruppe zugänglich machen (z. B. über einen Messenger):

- Auch bei Gruppenchats muss das Einverständnis der abgebildeten Personen vorliegen.
- Falls Sie verhindern möchten, dass jemand Bilder aus einem alten Chat benutzt, um Ihnen später zu schaden, aktivieren Sie „verschwindende Nachrichten“. Aber Vorsicht: Jemand könnte einen Screenshot angefertigt haben, der sich dann nicht mehr löscht.
- Entfernen Sie vor dem Veröffentlichen sämtliche Metadaten.
- Beachten Sie rechtliche Regelungen.
- Mit der PrivacyBlur-App [f-droid.org/packages/de.mathema.privacyblur] können Sie Gesichter auf Fotos sehr einfach verpixeln. Wählen Sie eine möglichst große Körnung, das verhindert das Zurückrechnen.

# Metadaten bereinigen

Private Fotos enthalten viele Informationen, die nicht auf den ersten Blick erkennbar sind. Diese sogenannten Metadaten werden weitergegeben, wenn Sie Fotos teilen. Dazu gehören u. a. Informationen zu Kamera und Gerät, Software und Hersteller, eindeutige ID der Nutzer.innen, Klarnamen und Standortdaten. Damit können die Metadaten z. B. verraten, wo das Kind auf dem Foto im Garten spielt oder das Foto von einem Papierstapel kann verraten, wo das Treffen der Journalistin mit einem Informanten stattgefunden hat.

Einbrecher.innen könnten anhand eines einzigen Fotos Ihren Wohnort herausfinden. Wenn sie den Namen im Foto dann noch mit den Klingelschildern abgleichen, finden sie sogar die richtige Wohnungstür. Und anhand der Gerätebezeichnung wäre schon vorher klar, ob sich der Einbruch lohnt.




Glücklicherweise lassen sich Metadaten sehr leicht entfernen.

Für Android ist die App Scrambled Exif [🔗f-droid.org/de/packages/com.jarsilio.android.scrambledeggsif] eine alltagstaugliche Hilfe. Sie funktioniert ganz einfach:

1. Wählen Sie im Teilen-Dialog „Scrambled Exif“ aus.
2. Danach öffnet sich der Teilen-Dialog erneut.
3. Nun können Sie die eigentliche App oder den Kontakt auswählen.
4. Das wars. Die Metadaten wurden automatisch entfernt.

Für iOS können wir leider keine App wirklich empfehlen. Suchen Sie mit einer Suchmaschine nach den Stichwörtern „exif“, „cleaner“ oder „Metadaten“.

Für Linux, macOS und Windows gibt es mit szTheorys Exif-Cleaner [🔗github.com/szTheory/exifcleaner] eine einfach zu bedienende Software. Nur auf Linux hat der Metadata Cleaner [🔗metadatacleaner.romainvigier.fr] eine besonders schöne Oberfläche.

Wer gern mit der Konsole arbeitet, kann mit dem ExifTool [🔗exiftool.org] auf dem Desktop [Linux, Mac, Windows] sehr schnell komplette Fotosammlungen bereinigen. Die genaue Anleitung finden Sie auf der Digitalcourage-Seite: 🔗digitalcourage.de/digitale-selbstverteidigung/fotos

# Fotos von Minderjährigen

Minderjährige sind rechtlich besonders geschützt. Bei jüngeren Kindern müssen die Eltern der Veröffentlichung zustimmen. Sobald das Kind in der Lage ist, mitzuentscheiden, brauchen Sie auch sein Einverständnis. Ab welchem Alter ein Kind als einsichtsfähig gilt, hängt von seinem Entwicklungsstand ab.

Ein rigoroses moralisches Verbot, Kinderfotos zu veröffentlichen, würde Kinder zwar schützen, sie und ihre Anliegen aber aus der digitalen und damit der öffentlichen Wahrnehmung drängen. Selbst im Kinderfernsehen dürften dann keine Kinder mehr zu sehen sein. Dies ist auch aus der Perspektive der Kinder nicht wünschenswert.

Auf den Einzelfall kommt es an:

- Veröffentlichen Sie keine Kinderfotos auf Social Media oder achten Sie zumindest darauf, dass das Gesicht nicht zu erkennen ist.
- Halten Sie sich auch in kleinen Messengergruppen zurück. Senden Sie Bilder nur im kleinen Kreis und achten Sie darauf, dass niemand bloßgestellt wird.
- Sprechen Sie mit dem Kind, sobald es fähig ist, zu verstehen, was passiert.
- Nehmen Sie die Wünsche des Kindes ernst und vermitteln Sie ihm, dass es selbst entscheiden darf.
- Verwenden Sie Fotos fremder Kinder mit äußerster Vorsicht. Auch wenn ein Foto als „frei“ lizensiert ist, wissen Sie nicht, ob das abgebildete Kind mit der Veröffentlichung einverstanden war.

Das Verbreiten von Fotos gegen den Willen der Abgebildeten ist strafbar, ganz besonders bei Minderjährigen. Allerdings hilft das den Betroffenen meist nicht. Juristische Auseinandersetzungen dauern, und in dieser Zeit wird der emotionale und soziale Schaden immer größer. Gerade hier gilt: Aufklärung und Vorsorge schützen am besten.

# Fotos in Beziehungen / intime Fotos

Intime Beziehungen finden immer öfter auch im Digitalen statt. Doch das birgt Probleme. Erinnerungen kann man nicht weitergeben. Fotos aber sehr wohl. Da eine Trennung oft mit verletzten Gefühlen einhergeht, können intime Bilder in falsche Hände gelangen. Wenn intime Fotos, die nie dafür bestimmt waren, in der Öffentlichkeit verbreitet werden, kommt es schnell zum Cybermobbing.



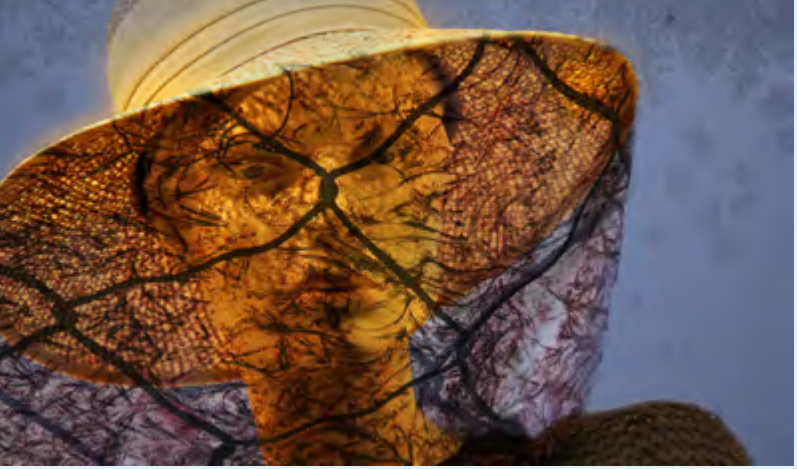
Das Verbreiten von Fotos gegen den Willen der Abgebildeten ist strafbar, ganz besonders bei Minderjährigen. Allerdings hilft das den Betroffenen meist nicht. Juristische Auseinandersetzungen dauern, und in dieser Zeit wird der emotionale und soziale Schaden immer größer. Gerade hier gilt: Aufklärung und Vorsorge schützen am besten.

Beim Weitergeben von Fotos bedeutet das, vorher zu überlegen, was mit einem Foto passieren kann, zum Beispiel wenn die Beziehung nicht mehr besteht.

Stellen Sie sich vor, was passieren könnte, wenn das Foto unabsichtlich an eine breite Öffentlichkeit gelangt.

- Sie selbst oder andere könnten in Lebensgefahr geraten? Geben Sie das Bild nicht weiter.
- Sie könnten Ihren Job oder eine.n Freund.in verlieren oder einige Monate an den Auswirkungen zu knabbern haben? Überlegen Sie, ob die Freude des Weitergebens dieses Risiko wert ist.
- Die Folgen wären zwar ein bisschen unangenehm, aber nach ein bis zwei Wochen vorbei? Riskieren Sie es, falls Ihnen danach ist.

**Wenn intime Fotos gegen den Willen einer Person verbreitet werden, braucht diese Unterstützung und emotionalen Halt, aber keine Vorwürfe. Wenn jemand gegen Ihren Willen ein Foto von Ihnen veröffentlicht, ist das nicht Ihre Schuld und keine Frage der Prävention.**



# Manipulierte Fotos

Bei fremden Bildern besteht immer die Möglichkeit, dass sie bewusst manipuliert wurden, sichtbar oder unsichtbar. Es gibt mehrere Ansätze, das aufzudecken.

## Metadaten-Analyse

In vielen Fällen sollten Sie bereits ohne Installation weiterer Software dafür ausgerüstet sein, Metadaten zu lesen:

- mit dem Dateimanager (Eigenschaften → Bild / Details)
- mit dem Bildbetrachter (Ansicht / Bearbeiten / Datei → EXIF / Metadaten)



In fast jeder Software gibt es eine entsprechende Option, im Zweifelsfall finden Sie die genaue Bezeichnung im Netz. Um Manipulationen anhand der Metadaten zu erkennen, prüfen Sie folgende Informationen auf Plausibilität:

- Software, Firmware, Hersteller
- Aufnahmedatum und -uhrzeit
- Änderungsdatum und -uhrzeit
- Standortdaten
- Bildbeschreibung

Nun geht es an die Plausibilitätsprüfung: Passen Metadaten und Bildinhalt zusammen? Gibt es Hinweise darauf, dass das Bild nachbearbeitet wurde? Im einfachsten Fall finden Sie einen Vermerk der Bearbeitungssoftware direkt in den Daten (z. B. GIMP, Adobe Photoshop). Wenn nicht, probieren Sie es mit weiteren Feldern der Metadaten.

Sollen Metadaten aus einer großen Menge von Dateien schnell und automatisch ausgelesen werden, geht das ebenfalls mit ExifTool (🔗exiftool.org).

### Vorsicht:

Metadaten sind kein Garant für Fakten. Mit etwas Aufwand können Böswillige beliebige Falschinformationen in die Metadaten schreiben und Sie auf eine falsche Fährte locken.

# Error-Level-Analyse

Die Error-Level-Analyse deckt auf, wenn Fotos durch Einfügen oder Entfernen von Inhalten manipuliert wurden. Digitale Fehler sehen im manipulierten Teil anders aus als im nichtmanipulierten. Das funktioniert allerdings nur bei sogenannten verlustbehafteten Bildern, zum Beispiel bei Fotos im JPEG-Format.

Wird ein Bild Pixel für Pixel gespeichert, nennt man das verlustfrei. Anders bei JPEG-Dateien. Hier wird das Bild in der Regel in mehreren Schritten komprimiert, um Speicherplatz zu sparen. Dabei nimmt man kleine Qualitätseinbußen in Kauf, in der Annahme, dass solche Verluste die Ästhetik des Bildes nicht allzu sehr beeinträchtigen.

So wie beim mehrfachen Überspielen analoge Datenträger leiden, leidet auch die Qualität von JPEG-Bildern unter wiederholtem Speichern. Dabei entstehen sogenannte Artefakte, optische Bildfehler. Je mehr dieser Artefakte dazukommen, desto höher wird der Error-Level. Wird beim erneuten Speichern der Inhalt nicht verändert, sollte der Error-Level des Bildes überall ungefähr gleichmäßig steigen. Wurden nachträglich Inhalte eingefügt, geändert oder gelöscht, ist die Chance hoch, dass der Error-Level der Änderungen nicht dem Error-Level des restlichen Bildes entspricht. Mit spezieller Software lassen sich solche Unterschiede sichtbar machen.



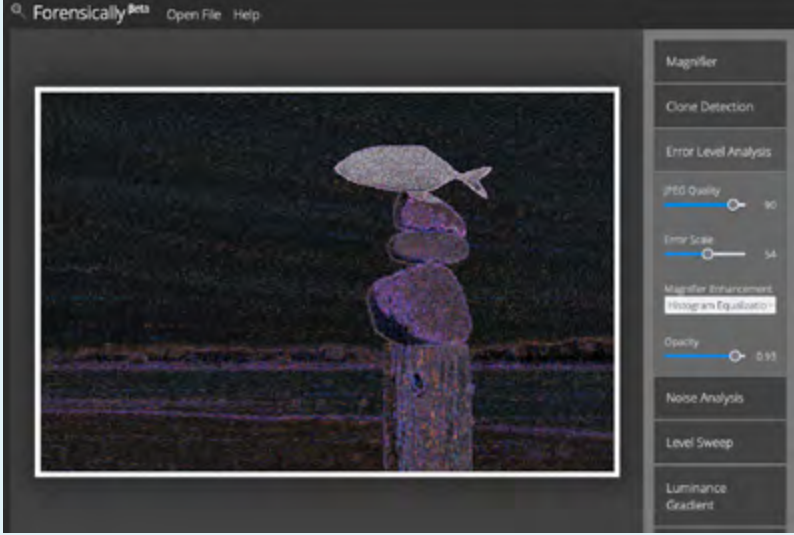
Für erste Versuche eignet sich Forensically [🔗29a.ch/photo-forensics/#error-level-analysis]. Dieses Online-Werkzeug analysiert die Bilder lokal im Browser, ohne sie auf fremde Server zu übermitteln. Lediglich die Suche nach eingebetteten Geotags, die den Standort der Kamera

angeben, baut eine externe Verbindung zu OpenStreetMap auf, um die Koordinaten auf einer Karte anzuzeigen (Stand August 2023).

Spielen Sie mit den Reglern „JPEG Quality“ und „Error Scale“. Wenn Objekte ab einem bestimmten Punkt deutlich heller oder dunkler sind als der Rest, wurde das Bild dort möglicherweise nachträglich verändert.

Benutzen Sie den Regler „Opacity“, um mehr vom Original zu sehen und zu erkennen, um welche Objekte es sich handelt. Im hier untersuchten Beispiel wurde der Fisch nachträglich eingefügt.






Forensically bietet noch weitere interessante Funktionen, zum Beispiel die Suche nach geklonten Inhalten oder das Auslesen von Metadaten.

## Hinweis:

Selbst wenn die Error-Level-Analyse die Manipulation eines Bildes zeigt, muss nicht unbedingt böse Absicht dahinterstecken. Es können auch – oft großflächige – Änderungen sein, die das Bild optisch aufwerten sollen.

# Bilder-Rückwärtssuche

Aus ihrem ursprünglichen Kontext gerissen, können Bilder komplett in die Irre führen. Beispiele zeigt die Bundeszentrale für politische Bildung in ihrem Video „Fake Fotos – Real or not?“ [🔗bpb.de/mediathek/video/314985/fake-fotos-real-or-not]

Wenn Sie herausfinden wollen, wo ein Foto im Internet in identischer oder ähnlicher Form verwendet wird, können Sie einen Dienst zur Bilder-Rückwärtssuche benutzen, zum Beispiel TinEye [🔗tineye.com]. Bedenken Sie aber, dass Sie die Fotos beim Hochladen einem kommerziellen Dienstleister übermitteln. Auch wenn TinEye verspricht, Ihre Fotos nach 24 Stunden zu löschen, könnten bis dahin Daten zu Werbezwecken analysiert oder mit Behörden geteilt worden sein.

Es gibt noch viele Profi-Tricks, zum Beispiel, wie man anhand des Sonnenstandes oder durch den Blick auf Nummernschilder Ungereimtheiten feststellen kann. Wenn Sie sich dafür interessieren, empfehlen wir das Video „Googeln wie die NSA – Tricks aus der Online-Rercheche-Praxis“ von Sebastian Erb bei [🔗digitalcourage.video].



# Deep Fakes

Die Möglichkeiten, Bilder zu manipulieren, werden täglich besser. KI-erzeugte Fotos und Videos sehen mittlerweile täuschend echt aus. Dem haben wir noch nicht viel entgegenzusetzen. Wir empfehlen, kritisch zu bleiben und Falschinformationen mit Medienkompetenz zu begegnen. Darüber hinaus müssen wir alle uns politisch für Transparenzvorgaben stark machen.

# Über die Autor.innen

**Leena Simon** ist Netzphilosophin (M.A.), Autorin und IT-Beraterin. Sie beschäftigt sich mit digitaler Mündigkeit und Technikpaternalismus. Sie hält Vorträge, gibt Workshops und arbeitet für Digitalcourage e.V. 🔗muendigkeit.digital

**Philipp Uhlig** studiert Psychologie und war ursprünglich IT-Administrator. Er schreibt ehrenamtlich zu Themen der digitalen Selbstverteidigung und organisiert die Digitalcourage-Hochschulgruppe in Bielefeld.

**Bildlizenzen:** Titel: Ketut Subiyanto on pexels.com, [M]; S. 2-3: iwi-design.de cc-by 4.0; S. 4: leohoho und Khamkeo Vilaysing on unsplash, [M]; S. 6-7: David Lamb on unsplash; S. 8: Gerd Altmann on publicdomainpictures.net; S. 9: Brett Sayle on pexels.com, [M]; S. 10-11: Courtney Cook on unsplash, [M]; S. 12: iwi-design.de cc-by 4.0; S. 14-15: pxhere.com, [M]; S. 16: Chermiti Mohamed on unsplash, [M]; S. 18: iwi-design.de cc-by 4.0; S. 21: iwi-design.de cc-by 4.0; S. 22: Kelly Sikkema on unsplash, [M]; S. 23: screenshot 29a.ch; S. 25: iwi-design.de cc-by 4.0; S. 26 oben: padeluun, unten: iwi-design.de cc-by 4.0
[M] = Montage: iwi-design.de cc-by 4.0


## Die kurz&mündig-Reihe wird herausgegeben von:

digitalcourage e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Seit 2000 verleihen wir die BigBrotherAwards. Digitalcourage ist gemeinnützig, finanziert sich durch Spenden und lebt von viel freiwilliger Arbeit.

Mehr zu unserer Arbeit finden Sie auf 🔗digitalcourage.de und 🔗bigbrotherawards.de

## In der kurz&mündig-Reihe sind bisher erschienen:

01 **Digitale Mündigkeit**
02 **Datenschutzrechte in Schulen durchsetzen**
03 **Faire Websites**
04 **Leitlinien für digitale Bildung in Schulen**
05 **Uploadfilter**
06 **Stalking, Hass, Kontrolle**
07 **Homeoffice**
08 **Digitale Bildungsangebote selbst erstellen**
09 **Digitale Angiffe im Büro**
10 **Digitale Sicherheit für Frauenhäuser**
11 **Versammlungsfreiheit**
12 **Nichts zu verbergen?**
13 **Apps selbst prüfen und bewerten**
14 **Überwachung in China**
15 **Solidarität im Netz**
16 **Fediverse. So geht Social Media**
17 **Einfach. Linux.**
18 **Smart Toys und Kinder-Tracking-Apps**
19 **Datenschutzbeschwerden richtig einreichen**
20 **Datenschutz in Kirchengemeinden**
21 **Videoüberwachung an Schulen**
22 **Digitale Selbstverteidigung für Mädchen***
23 **Workshops clever planen**
24 **Bodyshaming**
25 **Umgang mit Fotos**

Ein Bild sagt mehr als 1.000 Worte?
Deswegen nur sicher,
bewusst
und einvernehmlich
veröffentlichen

**Digitalcourage e.V.**
Marktstraße 18 | 33602 Bielefeld
mail@digitalcourage.de
digitalcourage.de
T: +49 521 1639 1639

9 783934 636637 >
5,00 Euro
5,00 CHF
ISBN 978-3934636-63-7

digitalcourage
k&m 25 Umgang mit Fotos