https://www.internet-abc.de/eltern/gefahren-kinder-im-internet/
aufgerufen Aug 21

Kinderfotos im Internet: Chancen und Risiken der Nutzung sozialer Netzwerke in Hinblick auf Fotos und andere Daten von Kindern

Erstellt am 2. Dezember 2011, zuletzt geändert am 2. Dezember 2011

Dr. Stephan G. Humer

Digitale Daten von Kindern sind immer besonders sensibel. Es gibt deshalb einige Grundregeln, die man beim Umgang mit Digitalisierung im Allgemeinen und Daten von Kindern in sozialen Netzwerken wie Facebook im Besonderen beherzigen sollte:

- **Die Digitalisierung ist revolutionär, nicht evolutionär!** Mißtrauen Sie allzu einfachen und gefälligen Analogien und Slogans. Viele Strategien und Methoden aus der nichtdigitalen Zeit bzw. Welt versagen im digitalen Raum, teilweise mit dramatischen Folgen. Die Beherrschung von Digitalisierung ist deshalb in meinen Augen so relevant wie Lesen und Schreiben, was unter anderem bedeutet, daß man nicht nach wenigen Stunden oder mit nur wenigen Handgriffen gleich ein Experte sein kann. Dies hat im Falle von Problemen und Fehlern verständlicherweise oft Frust, Ärger und Gedanken der Abkehr zur Folge. Sich bei Problemen oder nach Fehlschlägen von digitalen Geräten und Services abzuwenden, ist allerdings einer der größten Fehler, die man heutzutage überhaupt machen kann.

- Ein weiterer großer Fehler, den man meines Erachtens machen kann, ist, soziale Fragen von Technikern beantworten zu lassen. Das Motto sollte deshalb stets sein: **Technik ist zu wichtig, um sie nur Technikern zu überlassen**. Schon die (akademische) Ausbildung befähigt Techniker nicht zu gesellschaftlichen Analysen und reine Technikkenntnis ermöglicht kein Verständnis sozialer Handlungen und Zusammenhänge. Verlassen Sie sich deshalb nicht nur auf technische Tipps, sondern suchen Sie die gesamtgesellschaftliche Lösung.

- **Die Digitalisierung steht medienhistorisch betrachtet noch ganz am Anfang**, d.h. wir sehen gegenwärtig erst einen winzigen Bruchteil der Dinge, die noch auf uns zukommen werden. Sich der Digitalisierung zu verweigern ist kaum mehr möglich und unter dieser Prämisse auch kaum sinnvoll. Man wird höchstens einen immer größeren Berg von Herausforderungen vor sich herschieben, denn das Digitalisierungstempo und die Vernetzung der verschiedenen (Lebens-)Bereiche werden kaum abnehmen. Je früher, klüger, gelassener und effizienter deshalb eine sachliche Beschäftigung mit dem Thema begonnen wird, desto besser. Und da Digitalisierung keine

Ausweichmöglichkeiten parat hält, sondern ganz eigene Räume definiert (internationale Facebook-Freundschaften funktionieren nicht ohne Facebook, Geldabheben funktioniert nur noch am digitalen Automaten und nicht mehr am Schalter usw.), ist man entweder „drin“ – oder draußen.

- **Es ist keineswegs so, daß man heute keine Chance mehr hat, die Privatsphäre oder die eigene Kontrolle zu wahren**. Kontrollverlust ist trotz aller gegenläufigen Behauptungen in überraschend vielen Fällen immer noch etwas, das oftmals vom User und nicht vom Serviceanbieter ausgeht. Daß andere Mitwirkende – vor allem Wirtschaft und Politik – ganz andere Gestaltungsmöglichkeiten haben als ein einzelner User, ist freilich nicht überraschend. Doch man sollte bei der Digitalisierung weniger ein „Entweder – oder“ („Ich hab sowieso nix zu verbergen, also was solls?“), sondern eher ein „Sowohl – als auch“ in Betracht ziehen. Die schlechteste Position hat derjenige, der schon dann die Flinte ins Korn wirft, bevor die Herausforderung überhaupt absehbar ist. Wer meint, er habe „sowieso nichts zu verbergen“, irrt schon aus dem einfachen Grunde, daß er heute noch gar nicht weiß, was ihm morgen auf die Füße fallen kann. So waren die berüchtigten wilden Partyfotos für viele User lange ein klassisches Einstellungshindernis, weil Personaler bekanntlich auch im Netz surfen und man Angst hatte, als Bewerber hier den falschen Eindruck zu erwecken. Inzwischen wird sowas immer öfter *kontextuell* betrachtet: Man sieht im Falle privater Fotos (sofern sie nicht sämtliche Grenzen überschreiten), daß der Bewerber auch ein Privatleben hat, ein Mensch ist und nicht nur ein stromlinienförmiger Karrierist. Was also wann und wie von wem bewertet wird, unterliegt permanenten Veränderungen. Nach meinem Eindruck wird in Zukunft ein digitales Profil mit plausiblen Ecken und Kanten immer besser ankommen, da die Kontextualisierung und fallweise Bewertung von Daten eine immer größere Rolle spielen wird.

Für soziale Netzwerke wie Facebook und die Veröffentlichung von Kinderfotos bedeutet dies:

- **Was einmal im Netz ist, kann nicht wieder zurückgeholt werden!** Software wie der „Digitale Radiergummi“ oder Bilder mit „Ablaufdatum“ klingen vielleicht logisch und interessant, sind aber technisch nicht anderes als Unsinn und als wirkungsloses Placebo zudem Zeit- und Ressourcenverschwendung. Es ist technisch nicht machbar, digitale Bilder „zurückzuholen“ wie ein Polaroid vom schwarzen Brett, dessen Inhalt nur in den Köpfen der wenigen Betrachter existiert. Datensparsamkeit muß somit viel stärker beachtet werden. Vor einer Veröffentlichung besonders sensibler Bilder – und das sind ausnahmslos alle Kinderfotos, weil das Kind selbst noch keine sinnvolle Entscheidung treffen kann und die Eltern hier entsprechend gefordert sind – muß man sich umfassend informieren:

♦ Was ist der Zweck des Hochladens?

♦ Wer soll dieses Bild überhaupt sehen – und wer nicht?

♦ Wenn ich es jetzt und hier poste, welchen Bedingungen unterwerfe ich mich, wie viel Kontrolle habe ich?

♦ Verstehe ich all diese Bedingungen? Verstehe ich meine Kontrollmöglichkeiten?

♦ Bin ich nun in der Lage, hier eine sichere Entscheidung zu treffen, mich guten Gewissens dafür oder dagegen zu entscheiden?

♦ Oder gibt es sozialen Druck: weil alle mitmachen, ich nicht außen vor bleiben will oder ich schon zugesagt habe, ohne mich vorher ausführlich zu informieren?

♦ Oder gibt es andere Herausforderungen, die mich beeinflussen?

♦ Gibt es Alternativen zum bisherigen Vorhaben?

♦ Wie kann ich die mir aufscheinenden Risiken minimieren oder gar ganz ausschließen?

- Im Zweifel plädiere ich stets für **die Lösung, die dem einzelnen User** (und ggf. seiner „Zielgruppe“, also Verwandten, Freunden, etc.) **die meiste Kontrolle** läßt. So ist beispielsweise in wenigen Minuten (und für nur wenige Euro pro Jahr) eine eigene Website aufgesetzt, zusammen mit einem einfach zu verstehenden und zu bedienenden Content-Management-System wie WordPress, in Deutschland verortet und mit deutschen Datenschutz- und Vertragsbestimmungen, was einem User ungleich mehr Möglichkeiten bietet, z.B. einen passwortgeschützten Bereich, den nur enge Verwandte einsehen können. Hier sitzt kein Dienstleister wie eine Spinne im Netz und nutzt die eintrudelnden Daten z.B. für eigene Firmenwerbung. Datenmißbrauch fällt so deutlich schwerer. Der Arbeitsaufwand ist zudem überschaubar und lohnt sich auch langfristig. Facebook und Co. sind natürlich schön einfach – sonst würde man ja auch keine User anlocken, sondern abschrecken. Aber hier gilt der alte Slogan: **Wenn Sie nichts dafür bezahlen, sind Sie kein Kunde, sondern das Produkt!** Das vermeiden Sie z.B. mit einer eigenen Website, auf die auch im eigenen Facebookprofil mit einem Textlink hingewiesen werden kann – ohne nennenswerte Komforteinbußen. Nutzen Sie Facebook und Co. viel stärker in Ihrem eigenen Sinne, als Werbeplattform, deren Inhalte Sie bestimmen. Verweisen Sie auf Ihre Website und machen Sie diese zu ihrem Dreh- und Angelpunkt im Netz, nicht einen fremden Anbieter.

- Kinderfotos sind aus zahlreichen Gründen besonders sensible Daten, und das nicht nur in Hinblick auf ihre potentielle Nutzung durch Pädophile. Nicht selten wird die Verbindung zwischen sozialen Netzwerken und Pädophilie als Alarmismus oder Randerscheinung abgetan, doch schon die ersten Recherchen z.B. bei Wikipedia sollten Eltern erkennen lassen, daß hier durchaus eine nicht ganz unbedeutende Verbindung existiert:

„In einer Studie gaben 86,1 % der Teilnehmer an, Bildmaterial aus dem legalen und/oder illegalen Bereich zu nutzen.“ (1)

„Davison und Neale betonen, dass zur sexuellen Stimulation nicht zwangsläufig illegales Material nötig sei, vielmehr konstruieren Pädophile ihr eigenes sexuell erregendes Material aus Quellen, die allgemein als harmlos angesehen werden,wie z. B. Kinderbildern aus Versandhauskatalogen.“ (2)

Grundsätzlich halte ich die Digitalisierung für etwas weit überwiegend Positives und ich sehe die Freiheit des Individuums im Netz als ein sehr hohes Gut an, welche so weit wie möglich geschützt und keinesfalls unnötig eingeschränkt werden darf. Doch mit Freiheit geht bekanntlich Verantwortung einher. Wenn jemand vermeintlich harmlose Nacktfotos seiner am Strand spielenden Kinder bei Facebook veröffentlicht und das Profil samt Fotos z.B. durch simple Freundschaftsanfragen auch grundsätzlich völlig unbekannter Menschen zugänglich ist (3), stellt sich schnell die Frage nach der Sinnhaftigkeit eines solchen Vorgehens und ob hier nicht mehr Schaden als Nutzen entsteht. Hier helfen aber weder Verbote noch technische Placebolösungen, sondern hier ist vor allem die Verantwortung des Einzelnen gefragt.

Selbstverständlich gilt hier dieselbe Grundregel wie zuvor erwähnt: was einmal draußen ist, ist draußen. Das bedeutet natürlich nicht automatisch, daß jedes Strandbild eines planschenden Kindes direkt auf einem Pädophilen-PC landet – dieses Risiko ist und bleibt glücklicherweise eher gering. Doch meine Arbeitshypothese wäre im Falle einer Studie zu diesem Phänomen folgende: würde sich ein Mann mit Fotoapparat einem FKK-Strand nähern und dort spielende Kinder ablichten, würden die Eltern bei Entdeckung dieses Vorgehens zeitnah einschreiten. Daß mit viel weniger Aufwand und einem höheren Grad an Anonymität entsprechende Bilder digital „geerntet“ werden und Interessierte so deutlich erfolgreicher und umfangreicher vorgehen können, dürfte den meisten Eltern jedoch nicht in demselben Maße aufscheinen und demzufolge auch kein entsprechendes Einschreiten zur Folge haben. (Und da ein nachträgliches Einschreiten aus den genannten technischen Gründen nicht möglich erscheint, bleibt letztlich nur das Agieren *vor* einer Veröffentlichung.)

Nun kann (und soll) man Kinder nicht vor der Welt verstecken oder gar „in Watte packen“, doch im Unterschied zu Erwachsenen sind Kinder nun mal unmündig. Ein erwachsenes Unterwäschemodel kann, so die gängige Annahme, sich über die Konsequenzen seines Tuns – auch die vielleicht weniger schönen, nichtintendierten Folgen – informieren und eine ausgewogene Entscheidung treffen, ein Kind kann dies nicht. Es wird bei jeder Fotoveröffentlichung im digitalen Raum ungefragt zum „Model“. Dabei steht keinesfalls fest, daß sich das Kind später über diese Fotos freuen oder zumindest eine neutrale Haltung dazu einnehmen wird. Es dürfte, so meine These an dieser Stelle, einen signifikanten Unterschied ausmachen, ob man in der Jugend mit wenig erfreulichen Bildern aus der Kindheit konfrontiert wird und dazu die Information erhält, daß auch ein, zwei Tanten und Onkel hier einmal kurz drauf schauen und lachen durften oder ob zahllose Internetsurfer aus aller Welt diesen Schnappschuß auf ihrem heimischen Rechner oder ihrem Smartphone gespeichert haben und man nicht sagen kann, was mit dem Bild seitdem passiert ist.

Es muß also gar nicht der Worst Case, das Auftauchen von Kinderbildern auf einem Pädophilen-PC, eintreten. Es ist aus psychologischer Sicht schon schwierig genug, vermeintlich harmlose Kinderbilder der ganzen Welt (oder einem Unternehmen) zur Verfügung zu stellen und so die Kontrolle darüber zu verlieren. Papierfotos hätte man vor 20 Jahren wohl auch nicht so ohne weiteres einem Unternehmen zur freien Verwendung überlassen – warum hier also anders vorgehen?

- Die Thematik der Veröffentlichung von Kinderfotos ist schon schwierig genug, noch schwieriger wird es allerdings, wenn **Kinder eigene Profile bei**

Facebook oder anderen Anbietern bekommen. Abgesehen von der Fragwürdigkeit des Profils an sich (es wird jedem klar sein, daß sich hier die Eltern bzw. Sorgerechtsinhaber dahinter verbergen und nicht das Kind selbst, was bedeutet, daß man auch nicht das Kind mit seiner digitalen Präsenz „erlebt“, sondern die Ideen der Eltern wiederfindet): die Eltern übernehmen nicht weniger als die komplette Verantwortung für die digitale Identitätsarbeit des Kindes. Das Kind wird im Laufe seines Lebens somit weniger selbstbestimmt an Digitalisierung und Internet herangeführt, sondern muß sich ab einem bestimmten Zeitpunkt (spätestens, wenn es sich eigene Gedanken zur Internetnutzung und dortigen Identitätsgestaltung macht) zusätzlich Gedanken um seine bisher massiv fremdbestimmte Identitätsarbeit im digitalen Raum machen. Anders als bei den Fotos aus Papier im Fotoalbum, die physisch belegen, daß sie aus Alters- und Entwicklungsgründen nicht vom Kind angefertigt, arrangiert, kommentiert und präsentiert worden sein können und die Fremdbestimmtheit hier unzweideutig erkennbar sein dürfte, ist dies bei einer Onlineidentität in einem sozialen Netzwerk deutlich schwieriger zu bewerkstelligen, weil nicht nur technische Gründe eine Rolle spielen, sondern auch erneut die Frage der Kontrolle sowie die Abstraktions- und Imaginationskompetenz der Rezipienten: Was sehen sie in diesem Profil, was schlußfolgern sie? Wer garantiert, daß Facebook auch in zehn Jahren noch den gewohnten Zugriff auf das Profil gewährt? Und daß sich die Gesetze, denen Facebook folgt, nicht zum Nachteil der User ändern? Welche Vernetzungen mit anderen Services werden noch erfolgen? Die Facebook-Gesichtserkennung hat eindrucksvoll gezeigt, was im Hintergrund passieren und wie wenig man dagegen machen kann. Identitätsmanagement ist jedoch der Schlüssel zum individuellen Verständnis von Digitalisierung und sollte deshalb nicht unterschätzt werden. Es geht um mehr als nur eine Profilseite bei Facebook – es geht um die eigene Identität, das Selbst, das Individuum in seinem tiefsten Innern.

- Selbstverständlich gilt die umfangreiche **digitale Verantwortung nicht nur für die eigenen Kinder**, sondern auch für Kinder, die zu Besuch oder aus anderen Gründen zugegen sind, z.B. im Kindergarten oder in der Schule. Grundsätzlich sind die rechtlichen Regelungen – bspw. das Recht am eigenen Bild – hier eindeutig, **aber: vertrauen Sie nicht nur auf Recht und Gesetz!** Elementare Grundlagen der Digitalisierung wie die weltweite Vernetzung und das hohe Entwicklungstempo setzen dem Recht mit Leichtigkeit Grenzen. Zudem hinken zahlreiche gesetzliche Regelungen systembedingt permanent hinterher. Und das wird sich in Zukunft kaum ändern, da es nicht nur hochgradig unwahrscheinlich erscheint, einen weltweiten Rechtsraum mit entsprechenden Auswirkungen auf das Internet zu erhalten, sondern letztlich auch neue Entwicklungen vielfach noch gar nicht absehbar sind. Anbieter wie Facebook hören zwar auch immer wieder mal auf die Stimme der Masse und handhaben Features wie Gesichtserkennung vorsichtiger als es technisch oder aus Marketinggesichtspunkten notwendig wäre, doch auch dies ist ein Entgegenkommen, das einseitig aufgekündigt und auch nicht erzwungen werden kann. Setzen Sie deshalb auch nicht Ihr ganzes Vertrauen auf Privatsphäreeinstellungen oder die Integrität der Server von Facebook und Co. Hacker (4) werden sich für Ihre persönlichen Absichten kaum interessieren und Daten im Falle eines Falles trotzdem im eigenen Sinne nutzen.

- **Säubern Sie alle Bilder vor dem Hochladen von Detailinformationen technischer Art**. So können JPEGs mit Tools wie „ JPEG & PNG Stripper“ (5) von Zusatzinformationen gereinigt werden, die zur Identifikation von Personen beitragen können. Hier wird deutlich, daß technische Maßnahmen allein nicht ausreichen, sie als Teil eines ganzheitlichen Konzepts dem User aber dienlich sein können.

Wenn es bereits zu Datenmißbrauch gekommen ist:

- **Es gilt erneut: vertrauen Sie nicht nur auf Recht und Gesetz**. Natürlich ist es hilfreich, einen erfahrenen Medienanwalt (nicht einen digital ahnungslosen Anwalt!) um Rat zu fragen und ggf. tätig zu werden, doch vergessen Sie hier nicht den Streisand-Effekt (6), welcher dazu führen kann, daß der Versuch, Daten zu stoppen die Verbreitung erst recht befeuert: ein guter Medienanwalt wird diese Problematik ausführlich mit Ihnen besprechen. Fragen Sie lieber einmal zu viel als zu wenig nach, auch wenn gute Medienrechtler oftmals nicht gerade günstig sind.

- **Setzen Sie auf weitere Maßnahmen**, z.B. digitales Gegenwirken. Nutzen Sie die Foren anderer Betroffener, vernetzen Sie sich, überlegen Sie sich Strategien jenseits juristischer Schritte, bspw. Gegendarstellungen, Kommentare, eine eigene Website. Solche Maßnahmen helfen nicht nur inhaltlich, sondern auch emotional in dieser schwierigen Situation.

- **Überschreiten Sie keinesfalls rechtliche Grenzen!** Wer meint, anonym oder pseudonym erfolgreich gegen Datenmißbrauch vorgehen zu können (z.B. durch massive Diffamierung, einen digitalen Pranger oder die anonyme Androhung von Gewalt), verläßt sehr schnell sicheres Terrain! Es mag aus emotionaler Sicht verlockend erscheinen, eine Website, die die Bilder des eigenen Kindes mißbräuchlich einsetzt, mittels Hackerangriff lahmzulegen, doch die Risiken sind nicht nur aus juristischer Sicht enorm und deshalb kann davon nur abgeraten werden.

- Sogenannte **„Online-Reputationsmanager“ sind m.E. wenig hilfreich**. Die Aggregation von personenbezogenen Informationen kann man via Suchmaschine kostenlos selber ausreichend effizient durchführen und die weitergehenden Maßnahmen, die solche Anbieter offerieren, sind in den meisten Fällen zahnlose Tiger (z.B. schriftliche „Ermahnungen“ an einen Websitebetreiber). Sparen Sie sich das Geld und gehen Sie lieber gleich zu einem guten Medienanwalt. (Ganz abgesehen von der Tatsache, daß hier erneut ein Dritter in den Fall einbezogen wird, der beileibe nicht denselben Qualitätsansprüchen wie ein Medienanwalt genügen muß, z.B. Anbieter aus den USA.)

Den hier aufgeführten Informationen wohnt – wie fast allen Informationen den digitalen Raum betreffend – das Problem des vergleichsweise schnellen Veraltens inne. Zudem können alte Problemstellungen entfallen und bisher unbekannte hinzukommen. Deshalb kann der Text keinen Anspruch auf Vollumfänglichkeit oder langfristige Gültigkeit stellen, sondern soll vor allem als Orientierungsgrundlage und Denkanstoß dienen. **Sollten Sie Fragen haben oder bestimmte Aspekte vermissen, so zögern Sie nicht, nachzufragen.**

Suchen Sie ganz allgemein qualitativ hochwertige (wissenschaftliche) Informationen und Tipps zu Digitalisierung, Internet und sozialen Netzwerken, z.B. in der Medienpädagogik, Medienwissenschaft, Soziologie und Psychologie. Beschäftigen Sie sich langfristig und intensiv mit diesen Themen, denn sie werden zunehmend relevanter und ein Ausweichen wird immer schwieriger. Wie bereits gesagt: Lesen und Schreiben lernt man auch nicht an einem Tag – und die Digitalisierung ist, davon bin ich fest überzeugt, von derselben Relevanz. Nach dem heutigen Kenntnisstand (November 2011) würde ich u.a. die folgenden Themen im hiesigen Zusammenhang als mittelfristig besonders relevant bewerten:

- *Digitale Mobilität* (z.B. Internet nicht nur auf dem Smartphone, sondern auch im Auto/Navigationssystem; Location Based Services aller Art; weitestgehend nahtlose, digitale Mobilitätsangebote bei Bahn, Carsharing und Co.)
- *Digitale Identität* (z.B. eID-Funktion des neuen Personalausweises und anderer Anbieter, aber auch Gesichts- bzw. Ganzkörpererkennung in Überwachungsszenarien)
- *Digitale Ubiquität* (z.B. reaktive Werbe-Displays mit individuell zugeschnittener Werbung „im Vorbeigehen“, RFID-Chips in unzweideutig identifizierbaren Alltagsprodukten wie Kleidung und Lebensmitteln, weitestgehend unsichtbare Digitaltechnik im Wohnumfeld, bspw. Sturzmatten für Senioren)

Das Spektrum digitaler Möglichkeiten dürfte sich in absehbarer Zeit enorm erweitern. Je besser man sich also mit den digitalen Grundlagen und Entwicklungen auskennt, desto besser kann man agieren. Da Kinder und Jugendliche auch in Sachen Digitalisierung gute Vorbilder suchen, können (und sollten) Sie diese Vorbildfunktion einnehmen. Lassen Sie sich nicht von emotional geführten Post-Privacy-Diskussionen (7) oder anderen Skurrilitäten irritieren: Sie können viel bewegen, viel Kontrolle bewahren und positiv wirken, für Ihre Kinder und sich selbst, hier und jetzt. Und auch in Zukunft.

Zum Autor:

Dr. phil. Stephan G. Humer ist Universitätsdozent und Forschungsleiter in der Digitalen Klasse der Universität der Künste Berlin und als intimer Kenner der digitalen Kultur ein gefragter Interviewpartner und Gastautor. Er widmet sich seit mehreren Jahren der Analyse der Digitalisierung unserer Gesellschaft. Er ist Mitbegründer der Deutschen Gesellschaft für Informationsfreiheit e.V., aktiv im Forschernetzwerk “Surveillance Studies” und in der Arbeitsgruppe “Identitätsschutz im Internet” der Ruhr-Universität Bochum.

Website: http://www.internetsoziologie.de

(1)
https://de.wikipedia.org/w/index.php?title=P%C3%A4dophilie&oldid=95702997#Nutzung_legaler_und_illegaler_Medien_zur_sexuellen_Stimulation, abgerufen am 21. November 2011; Horst Vogt: *Pädophilie. Leipziger Studie zur gesellschaftlichen und psychischen Situation pädophiler Männer*. Pabst Science Publishers, 2006. S. 72.

(2)
https://de.wikipedia.org/w/index.php?title=P%C3%A4dophilie&oldid=95702997#Nutzung_legaler_und_illegaler_Medien_zur_sexuellen_Stimulation, abgerufen am 21.

November 2011; Gerald C. Davison, John M. Neale: *Klinische Psychologie*, Beltz PVU, Weinheim, 7. Auflage, 2007. S. 505–508

(3) http://www.heise.de/newsticker/meldung/Studie-Viele-Facebook-Nutzer-sind-sorglos-1370431.html, abgerufen am 21. November 2011.

(4) An dieser Stelle sei auf die Schwierigkeit einer Einteilung in „gute“ und „böse“ Hacker verwiesen: https://de.wikipedia.org/w/index.php?title=Hacker&oldid=95973633#Abgrenzung_zum_Begriff_.E2.80.9ACracker.E2.80.99, abgerufen am 23. November 2011. Der besseren inhaltlichen Handhabbarkeit halber wird diese Diskussion aber im Text nicht vertieft.

(5) JPEG & PNG Stripper: http://www.chip.de/downloads/JPEG-amp-PNG-Stripper_36774505.html

(6) https://de.wikipedia.org/w/index.php?title=Streisand-Effekt&oldid=95263903, abgerufen am 23. November 2011.

(7) http://wissen.dradio.de/buzzwordcheck-post-privacy.85.de.html?dram:article_id=13414, abgerufen am 23. November 2011.