



„Datenschutz geht zur Schule“

DaSou-Podcast-Folge mit Miriam Reichelt

Karina Filusch: Hallo und herzlich Willkommen beim DaSou-Podcast. Ich bin Karina Filusch, Datenschutzanwältin und externe Datenschutzbeauftragte. In jeder Folge sprechen wir mit einer Expertin oder einem Experten über Datensouveränität, abgekürzt DaSou.

Aileen Weibeler: Ich bin Aileen Weibeler und angehende Juristin. Ihr würdet uns einen riesigen Gefallen tun, wenn ihr uns auf Instagram und Twitter folgt und uns bei eurem Lieblings-Podcaster abonniert.

Karina Filusch: Heute sprechen wir mit Miriam Reichelt. Sie ist Referentin in einer Digitalagentur und geht mit ihrem Wissen über Digitalität und Datenschutz in Schulen und spricht mit Lehrerinnen und Lehrern sowie Schülerinnen und Schülern darüber, wie man sich sicher im Internet bewegt.

Aileen Weibeler: Außerdem haben wir mit ihr darüber gesprochen, wann man am besten beginnen sollte, Kinder und Jugendliche für Datenschutz zu sensibilisieren – kleiner Disclaimer: Nie früh genug. Zudem haben wir darüber gesprochen, wie man Fake-Accounts entlarvt und was passiert, wenn es schon zu spät ist und Nacktbilder oder peinliche Posts im Internet gelandet sind. Hier ist es wichtig, dass die Aufklärung an den Schulen, bei den Lehrern und Jugendlichen ganz früh startet.

Karina Filusch: Der aktuelle Fall mit Sarah-Lee Heinrich hat gezeigt, wie wichtig Aufklärung ist und wie wichtig es ist zu wissen, wie man sich sicher im Internet bewegt. Sie hat nämlich im Alter von 13 beziehungsweise 14 Jahren, Posts hinterlassen, die ihr heute auf die Füße fallen und genau über solche Dinge möchten wir heute mit Miriam sprechen.

Aileen Weibeler: Wie kam es denn dazu, dass du in die Schulen gegangen bist?





Miriam Reichelt: Zuerst möchte ich ein bisschen über Comspace sprechen. Comspace ist eine Digitalagentur aus dem Herzen von Bielefeld und wir entwickeln komplexe Weblösungen für Mittelständler und Großunternehmen. Unser Portfolio umfasst marktführende Technologien im Bereich CMS, also Sitecore, FirstSpirit und OpenText. Wir sind zudem Implementierungspartner für Celum und bieten auch hier Konnektoren, KI-betriebene Services und individuelle Lösungen an. Comspace stellt sich der Verantwortung, die das „digitale Unternehmertum“ mit sich bringt und hat deswegen CDR, also Corporate Digital Responsibility, auf die Agenda gesetzt. Das ist quasi mit Digitalverantwortung zu übersetzen. Manche sagen auch digitale Ethik. Ein Baustein der Corporate Digital Responsibility ist z.B. digitale Befähigung. Wir arbeiten unter anderem mit denjenigen, an die in diesem Kontext selten gedacht wird: Kinder und Jugendliche und beispielsweise Schulen. Daher besuche ich ab und an Schulen und schule die Lehrer auf Datenschutz sowie die Schülerinnen und Schüler in Bezug auf Internetsicherheit und digitale Kompetenzen.

Karina Filusch: In welchem Alter beginnt deiner Einschätzung und deinen Erfahrungen nach eigentlich der richtige Umgang mit Datenschutz?

Miriam Reichelt: Ich persönlich finde, dass man Datenschutz idealerweise in dem Maße „mitwachsen“ lassen sollte, in dem das Kind oder die Kinder Umgang mit dem Internet haben. Unser Kind beginnt jetzt im Internet zu surfen und weiß beispielsweise, was ein Cookie-Banner schreibt und wo es dann klicken soll. Es versteht auch schon ganz grob, worum es geht. Wir versuchen die Skills nach und nach weiterzuentwickeln und hoffen, dass das funktioniert. Das ist allerdings aktuell noch eine Art empirische Sozialstudie. Ob das wirklich funktioniert, müsst ihr mich in ungefähr zehn Jahren nochmal fragen.

Karina Filusch: Wie alt ist dein Kind denn?

Miriam Reichelt: Mein Kind ist jetzt acht.

Karina Filusch: Ah, okay, ein gutes Alter

Miriam Reichelt: Finden wir schon, ja.





Karina Filusch: Ich habe das große Glück gehabt, deine Vorträge schon zu hören. Du bereitest nämlich einen Vortrag für Lehrer und einen Vortrag für Schüler vor. Fangen wir doch mal mit den Lehrern an, weil unser Thema Datenschutz in der Schule ist. Was können Lehrer konkret tun? Oder vielleicht auch Eltern, um sie zu unterstützen und um bei Kindern das Thema Datenschutz irgendwie interessant zu machen?

Miriam Reichelt: Sie können sich erst mal selbst damit befassen, falls das noch nicht passiert ist. Was man nicht weiß, kann man auch nicht vermitteln und dann auch nicht zeigen, dass das Thema Relevanz hat. Das Wissen muss man dann genauso weitergeben, wie auch die anderen Dinge im Leben: also das Uhrenlesen, europäische Hauptstädte runterbeten, Schnürsenkel binden. Datenschutz braucht man im späteren Leben definitiv. Wenn es mit der Schleife nicht funktioniert, zieht man Schuhe mit Klettverschluss an. Für Datenschutz gibt es aber eben keine Klettverschluss-Lösung. Wenn man selber nicht weiß, wie man das vermitteln soll, dann gibt es eben Unterstützung in Form von Medienberater:innen für Kinder und Erwachsene und auch Datenschützer, die an Schulen gehen und dort unterstützen. Wir bei Comspace machen das manchmal auch.

Karina Filusch: Was ist denn eigentlich dein Eindruck von der aktuellen Generation? Wie gut aufgeklärt ist die aktuelle Generation denn, was Datenschutz angeht?

Miriam Reichelt: Da gibt es, glaube ich, wie bei allen gesellschaftlichen Themen nicht den einen Wissensstand. Mein Eindruck ist, dass jüngere Kinder logischerweise meistens weniger wissen als ihre Eltern. Sobald sie älter werden, wissen sie meistens ein wenig mehr, aber das Wissen wird ganz oft nicht genutzt. Da hat man ihnen im Zusammenhang mit Datenschutz nicht beigebracht, wie man damit umgeht, sondern nur, wie man das Thema umgeht, im Sinne von „Löscht alles, macht nichts, was Spaß macht oder gerade angesagt ist“. Das ist nicht lebensnah. So hätte ich in dem Alter auch keine Lust darauf gehabt und mich wahrscheinlich genauso verweigert. Dabei sind die meisten schon ziemlich interessiert und offen und das merke ich auch bei meinen Schulungen. Besonders im anschließenden Q&A. Da stellen sie dann manchmal Fragen, die Erwachsene auch haben, sich aber irgendwie nicht trauen würden zu stellen, zum Beispiel: Können meine Eltern über die Fritzbox sehen, ob ich Pornos geguckt habe?

Karina Filusch: Eine spannende Frage. Und Miriam, können sie?





Miriam Reichelt: Nein, im Normalfall eher nicht, aber es hängt auch ein bisschen davon ab, wie die Eltern das konfiguriert haben und was sie vielleicht sonst noch installiert haben, um das zu checken.

Karina Filusch: Was für eine intelligente Frage.

Miriam Reichelt: Ich finde die Frage intelligent und cool. Sie zeigt auch, wie offen und interessiert sie eigentlich an dem Ganzen sind.

Karina Filusch: Warum denkst du, ist es ganz besonders wichtig für Kinder und Jugendliche von Anfang an, so früh wie möglich, geschult zu werden, um auf ihre Daten aufpassen zu können? Welche Risiken siehst du, wenn man das nicht machen würde?

Miriam Reichelt: Bei meinen ersten Gehversuchen im Internet - damals, als die Gummistiefel sozusagen noch aus Holz waren - war das mit dem Internet noch recht unspektakulär. Die Webseiten waren weiß. Es gab einen rudimentären Menü-Baum und vielleicht noch ein fast verpixeltes Firmenbild im Header. An Daten wurde der offene sichtbare Besucher im Counter auf der Webseite gesammelt. Das hat sich gravierend geändert. Die aktuelle Generation ist die Generation, die schon als Strich auf dem Schwangerschaftstest online war, wenn die Eltern das gepostet haben. Ab diesem Zeitpunkt wurden dann Informationen über diese Menschen gesammelt. Das wissen auch die großen Internetkonzerne und führen die Kinder und Jugendlichen als „wertvolles und weitestgehend ungenutztes Publikum“. Es gibt auch schon eine Vielzahl von Strategiepapieren zu der „Nutzung“. Diese „Nutzung“ ist die Gewinnerzielung aus der allgegenwärtigen Verfolgung der Menschen und der daraus generierten Verhaltensprofile. Es ist also kaum möglich, dies komplett zu umgehen, wenn man nicht ohne Internet auf irgendeiner abgelegenen Alm lebt. Umso wichtiger ist das Wissen darum und um die ganzen Dynamiken.

Karina Filusch: Ja. Lass uns darüber sprechen, was man im Internet von sich posten oder verbreiten kann. Ich habe in meiner Ausbildung gemerkt, wie oft Mädchen von Jungs unter Druck gesetzt werden und Nacktbilder von sich per WhatsApp versenden, am besten so, dass man sie auch noch erkennen kann und nicht nur von dem Körperteil an sich. Diese werden dann plötzlich auf irgendwelchen anderen sozialen Medien gepostet oder ausgedruckt und in der Schule aufgehängt. Die Mädchen trugen dann





Rechtsanwältin Karina Filusch, LL.M. | Friedrichstraße 95, 10117 Berlin | T: 030 219 11 555

schwere psychische Schäden davon und mussten auch wirklich von Ärzten und Ärztinnen behandelt werden. Dann gibt es auch noch peinliche Selfies, über Nacktfotos hinaus. Was sagst du denn den Kindern und Jugendlichen, die du schulst? Vergisst das Internet wirklich nicht?

Miriam Reichelt: Ich persönlich habe schon wichtige und spannende Dinge im Internet nicht wiedergefunden, aber das lag sicherlich nicht am Internet, sondern höchstens daran, dass ich falsch gesucht habe. Das Internet ist schließlich kein viereckiger Raum, den man strategisch durchsuchen kann, um ihn dann gezielt auszumisten. Das heißt, dass Content, der mal generiert wurde, multipliziert und an verschiedenen Orten neu abgelegt wird. Er verschwindet dann zunächst auf den ersten Blick, kann dann aber später wieder auftauchen. Das ist problematisch. Blättert man heute in seinem Jugendtagebuch auf Papier, dann empfindet man ggf. ein sentimentales Gruseln, schämt sich ein wenig und stellt es zurück ins Regal. Diese Tagebücher heißen heute Facebook, Twitter und Instagram und speichern alles auf unseren Wunsch, in der Regel öffentlich. Diese Inhalte sind nicht darauf ausgelegt, vom Internet vergessen zu werden. Sie sind eigentlich darauf ausgelegt, gefunden zu werden. Höchstens wir vergessen etwas. Im schlimmsten Fall kann einem das, was man vergisst, in unpassenden Momenten wieder vor die Füße fallen. Das können unüberlegte Postings aus der Jugend sein, wenn man einen neuen Job antreten will oder eben Fotos, die man mal unbedarft verschickt hat.

Karina Filusch: Ja, das sieht man zum Beispiel gerade am aktuellen Fall von Sarah-Lee Heinrich, die neue Grünen-Sprecherin von der Grünen Jugend geworden ist. Mit 13 bzw. 14 Jahren hat sie unpassende Sachen gepostet. Was rätst du den betroffenen Personen, die ein Nacktfoto oder irgendwas Peinliches verschickt haben im Nachhinein?

Miriam Reichelt: Wenn das noch sehr zeitnah ist, dann sollte man den Empfänger oder die Empfängerin bitten, das im eigenen Beisein zu löschen. Wenn das ganze schon viral gegangen ist, muss man schnell sein. Je eher man davon erfährt und je schneller man reagiert, desto mehr Möglichkeiten hat man, den Schaden zu begrenzen. Hat man beispielsweise die URL des Bildes, kann man damit oft weitere Seiten finden und die Fundstellen dokumentieren. Man sollte die Inhaber in der Webseite nach Möglichkeit sofort kontaktieren und sie mit einer Frist dazu auffordern, die Bilder herunterzunehmen und zu löschen. Hat die Webseite kein Impressum, was sehr häufig der Fall ist, kann man über eine Domainabfrage Glück haben. Die unerwünschte Veröffentlichung und Verbreitung von beispielsweise Nacktbildern durch eine andere Person ist - korrigiere





Rechtsanwältin Karina Filusch, LL.M. | Friedrichstraße 95, 10117 Berlin | T: 030 219 11 555

mich bitte, wenn ich da falsch liege - eine Straftat. Da sollte man, auch wenn es unangenehm ist, gegen jede Person, die die Bilder gespeichert und weitergeleitet hat, Anzeige erstatten. Im besten Fall sollte man sich anwaltlichen Beistand suchen, um weitere rechtliche Schritte zu besprechen und vielleicht Schadensersatz etc. zu fordern. Ich weiß, „there is no glory in prevention“, aber besser ist es halt, wenn man anderen Menschen solches Material gar nicht erst überlässt. Früher wäre das ein einzelnes verpixeltes und irgendwann abgegriffenes Foto gewesen. Heute vermehrt sich das durch jedes Speichern. Das hat man nicht mehr unter Kontrolle. Auch nicht derjenige, der es initial verbreitet hat und seine Aktion 24 Stunden später vielleicht selbst nicht mehr gut findet. Wie du gerade gesagt hast, kann so etwas die Betroffenen psychisch schwer belasten. Es kann sie in Verruf bringen, es kann sie die Karriere kosten. Das hätte ein analoges Bild nicht so schnell geschafft.

Karina Filusch: Apropos Straftaten: du sagst es ganz richtig! Das wissen vielleicht nicht alle, aber wenn eine 13-Jährige ein Bild von sich verschickt und das dann jemand verbreitet, dann verbreitet diese Person Kinderpornos oder Jugendpornos, wenn die Abgebildete schon älter ist. Auch der Junge, der das Foto bekommen hat, macht sich strafbar. Das muss er auch bedenken. Lass uns noch über andere Daten sprechen: über Daten, die wir vielleicht unbewusst weitergeben. Zum Beispiel eine Markierung von einem Ort oder von einer Uhrzeit in den Insta-Stories. Theoretisch könnten die Leute dann bei mir zuhause vorbeikommen.

Miriam Reichelt: Die Frage ist heute ist eher: Welche Daten gibt man nicht weiter? Ein Sleep-Tracker zeigt, wann und wie wir geschlafen haben. Es gibt sogar elektrische Zahnbürsten mit einer App, die mitschneidet, wann und wie wir die Zähne putzen. Wir tragen vielleicht den Sex der letzten Nacht, bei dem eine Spotify Kuschel-Playlist lief, in die Zyklus-App ein. Wir wiegen uns mit der Waage, die die Daten zusammen mit unseren Schritten, Routen und dem getrackten Essen an eine App weitergibt. Es wird mitgeschnitten, wann wir online die Nachrichten lesen, unser Internetradio einschalten, wann wir angefangen haben zu arbeiten und ob wir parallel eine Serie geschaut haben oder vielleicht tatsächlich nur gezockt haben, statt den Monatsabschluss zu machen. Das lässt sich beliebig fortsetzen. Wir müssen uns bewusst machen, dass all diese Daten nicht verschwinden, sondern gesehen, gespeichert und genutzt werden. Die Firmen wollen natürlich „nur unser Bestes“: unser Geld, unsere Meinung, unsere Stimme, unsere Aufmerksamkeit, unsere Daten. Wenn wir taggen, mit wem wir gerade Essen gehen, dann wahrscheinlich, um ein bisschen mit unserem Leben zu flexen. Es wäre dann aber auch möglich, dass uns dort jemand aufsucht oder beobachtet. Das ist





Rechtsanwältin Karina Filusch, LL.M. | Friedrichstraße 95, 10117 Berlin | T: 030 219 11 555

dann schnell eher gruselig als cool. Wenn wir das nicht wollen, dann sollten wir es vielleicht einfach lassen.

Karina Filusch: Was würdest du uns für einen Tipp geben? Wie kann ich vorbildlich durchs Leben gehen oder möglichst anonym? Reicht es, wenn ich das regelmäßig lösche?

Miriam Reichelt: Komplett anonym unterwegs zu sein, ist schwer bis unmöglich. Man kann aber datensparsamer unterwegs sein, auch als nicht so technikaffine Person. Aktuell vermutlich online, noch am ehesten mit dem Firefox und einigen Add-ons. Statt Google kann man andere Dienste nutzen, beispielsweise DuckDuckGo. Muss man sich Cookie-Bannern stellen, dann sollte man nicht auf Akzeptieren klicken, sondern sich tatsächlich etwas intensiver damit befassen, auch wenn es nervt. Dass es nervt, liegt übrigens nicht am Datenschutz, sondern an den Seitenbetreiber:innen, die das ein bisschen missachten. Nirgendwo in der DSGVO steht, dass sie den Internetnutzern das Leben mit umständlichen und hinterhältigen Cookie-Bannern schwer machen sollen. Man muss sich nicht überall Kundenkonten anlegen. Man muss auch nicht jede App nutzen, nur weil sie gerade gefühlt jeder hat. Über Dienste wie z.B. Exodus-Privacy kann man vorher checken, welche Tracker in die Apps eingebaut sind und sich dann entscheiden, ob es einem das wert ist. Oft kann man Apps auch zahlreich die Berechtigungen entziehen und sie funktionieren immer noch. Wir haben zum Beispiel Wetter-Apps, die gerne Zugriff auf unser Adressbuch hätten. Wofür? Es funktioniert auch ohne Adressbuch. Es gibt nicht die eine Lösung. Außer vielleicht wir ziehen auf die Alm ohne Internet. Es gibt viele Stellschrauben.

Karina Filusch: Was kann man noch alles tun? Zum Beispiel vielleicht ein sicheres Passwort aussuchen? Oder was könnte mich noch schützen, damit andere mir im Internet nicht auf die Spur kommen?

Miriam Reichelt: Beim Thema Passwörter geht es erst einmal darum, komplexe Passwörter zu wählen und nicht den Geburtsnamen der Mutter oder den Namen des ersten Haustieres. Vor allen Dingen ist es wichtig überall ein anderes Passwort nutzen. Wer bei den Passwörtern nicht so kreativ ist - ich bin es nicht, der kann zum Beispiel einen Passwort-Generator benutzen. Entschuldige den Vergleich, aber Zugangsdaten bzw. Accountdaten sind so ein bisschen wie Unterhosen. Jeder sollte seine eigenen haben und sie lieber nicht teilen, auch nicht mit dem besten Freund und der besten Freundin.





Karina Filusch: Das ist ein schöner Vergleich. Den werde ich mir für die Zukunft merken. Kommen wir vielleicht noch zu einer anderen Maßnahme, die uns womöglich helfen könnte und mittlerweile zum Politikum geworden ist. Wie nenne ich mich im Internet? Es gibt in Deutschland die Möglichkeit, nicht mit Klarnamen im Internet aufzutreten. Das sieht das Gesetz sogar vor. Allerdings kommen dann soziale Medien, wie zum Beispiel die Medien aus der Facebook-Gruppe, die eine Klarnamenpflicht vorsehen. Was würdest du denn empfehlen, sich lieber Max Müller zu nennen oder lieber max.2000 oder sonst irgendeine kreative Abkürzung? Was sind die Vor- und Nachteile für dich?

Miriam Reichelt: Ich finde beides okay. Genauso trägt man manchmal eine Jogginghose trägt und manchmal eine Anzughose. Ich finde den Anlass entscheidend. Wenn man nicht einen deutlichen Vorteil daraus hat, mit seinem echten Namen aufzutreten, dann sollte man ihn vielleicht eher nicht nutzen. Ich trage auch keine Anzughose, wenn es nicht gerade sein muss. Vorteilhaft ist der echte Name vermutlich eher im geschäftlichen Kontext. Ich hatte aber auch schon mal einen Kunden, der mir von einer Mailadresse schrieb, die mit Don Porno begann. Das fand ich persönlich sehr witzig. Unter Umständen kann sowas aber den großartigen ersten Eindruck schon ein wenig trüben. Was Facebook angeht, habe ich bisher nicht mitbekommen, dass jemand ernsthafte rechtliche Konsequenzen hatte, weil er sich Micky Maus genannt hat und nicht seinen richtigen Namen genutzt hat. In Onlineshops sollte man hingegen den richtigen Namen nutzen, wenn man die Sachen auch bekommen möchte. In sozialen Netzwerken sehe ich darin aber keine Vorteile.

Karina Filusch: Ja, apropos Fake-Namen oder ausgedachte Namen... Woran erkenne ich denn jetzt, dass ein Account ein Fake-Account ist und mir vielleicht nichts Gutes will?

Miriam Reichelt: Hier kann man vermutlich am ehesten auf die sogenannten Red Flags achten. Wenn etwas zu gut klingt, um wahr zu sein, ist es in der Regel auch zu gut, um wahr zu sein. Das hat man häufig in Kleinanzeigen, in Immobilienanzeigen oder auch bei Shops. Bei vermeintlichen Shops sind Hinweise darauf, dass es sich um einen Fake Shop handelt beispielsweise zu günstige Preise, eine nicht existente Adresse im Impressum, falsche Telefonnummern und tote Email-Postfächer. In den sozialen Medien gibt es neben Bots auch Ghost-Accounts, die oft dem Ausspionieren deines Profils dienen, weil die Leute beispielsweise mit einem anderen Profil bei deinem geblockt sind oder es handelt sich dabei um Leute, die einfach nur so neugierig sind. Die haben häufig ein liebloses Profil, kein Profilbild oder irgendwas Anonymes, keine Infos, keinen oder kaum eigenen Content und auch keine Interaktion. Die wollen





Rechtsanwältin Karina Filusch, LL.M. | Friedrichstraße 95, 10117 Berlin | T: 030 219 11 555

schließlich auch, dass man vergisst, dass sie da sind. Die wollen nur gucken. Hat jemand sehr viele Follower, aber keine wirkliche authentische Interaktion, also wenige Likes und wenig echte Kommentare, ist das auch schon ein Hinweis. Da lohnt sich ein Blick in die Timeline. Manchmal geben auch Kommentare oder Postings Anhaltspunkte dafür, dass es sich eventuell um ein Fake handelt. Nicht selten verfolgen Fake Accounts ein Ziel. Das kann das reine Ausspionieren eines Profils sein oder aber Geld oder Passwörter. Wenn also jemand aktiv (vielleicht aber auch nur unterschwellig) oder passiv aggressiv nach irgendetwas fragt, dann sollte man kein schlechtes Gewissen haben, wenn man das abblockt. Man sollte sich nicht unter Druck setzen lassen, sondern von dieser Person Abstand nehmen. Hat man ein schlechtes Bauchgefühl, so sollte man darauf vertrauen.

Karina Filusch: Das sind gute Tipps von dir. Ja, die bösen Absichten, die Fake Accounts haben können, nicht wahr? Stichwort Social Engineering. Du hast es gerade so schön beschrieben. Die wollen Vertrauen erwecken und dann womöglich Geld von uns oder, dass wir Verträge abschließen. Ich hatte auch schon ein paar Mandantinnen und Mandanten, die zum Beispiel einer Einladung gefolgt sind oder auf einem Facebook- oder Instagram-Bild getaggt worden sind und dann irgendwie dazu gebracht worden sind, ein Abo abzuschließen, in dem sie ganz viele vertrauenserweckende Nachrichten bekommen haben. Wenn Fremde einem eine Einladung senden, sollte man vielleicht auch überlegen, ob man die annehmen will. Sowas kriegt man auch regelmäßig, nicht wahr? Vielleicht können wir das mal zusammenfassen: Was sind für dich die Do's und Don'ts im Internet?

Miriam Reichelt: Es ist definitiv ein Do für mich, den kritischen und gesunden Menschenverstand zu nutzen und das Bauchgefühl nicht zu missachten. Weiterhin sollte man Daten bewusst und gezielt weitergeben. Ganz besonders dann, wenn es um die Daten anderer Menschen geht. Da tragen wir eine große Verantwortung. Dann sollte man vielleicht tatsächlich nicht unbedingt alles mitmachen. Und wenn doch, dann sollte man gucken, wie man das in etwas weniger invasiver Form tun kann. Ansonsten: Wissen wird mehr, wenn man es teilt. Daher sollte man das auch tun. Man sollte das Thema vielleicht tatsächlich mal ansprechen und Ergebnisse mit anderen Leuten teilen.

Karina Filusch: Liebe Miriam, wer haftet denn eigentlich, wenn ein Kind oder Jugendliche auf eine Internetseite gehen, die eigentlich nicht erlaubt ist?

Miriam Reichelt: Generell sollte man Kindern beibringen, dass das Internet kein





rechtsfreier Raum ist und, dass das, was man im Internet tut, auch ganz reale Folgen haben kann. Ist ein Kind älter als 7, sind Verträge meiner Ausbildung nach schwebend unwirksam. Das bedeutet aber nicht, dass man nicht doch eventuell für Sachen zahlen muss, die man gekauft hat. Zumindest hat man ordentlich Arbeit damit, das alles rückabzuwickeln. Auch Rechtsverletzungen können ein Nachspiel haben, sofern das Kind darüber aufgeklärt wurde, was man darf und nicht darf. Wenn beispielsweise illegal Filme heruntergeladen werden oder fremde Bilder genutzt werden kann eine minderjährige Person hier eventuell schon selbst haften, wenn sie bezüglich der Rechtsverletzung als Einsichtsfähigkeit eingestuft werden kann. Bei der Verbreitung von Pornos oder Kinderpornographie und den schon erwähnten Nacktfotos kann man sogar eine echte Freiheitsstrafe bekommen. Wobei hier meines Erachtens dann doch meistens das Jugendstrafrecht gilt. Aber mal ehrlich, schlimm genug, oder? Dasselbe droht auch bei Mobbing. Haftung ist die eine Sache. Die andere Sache ist, wie viel Arbeit und Ärger man damit schafft oder ob man sogar Schlimmeres auslöst. In diesem Zusammenhang denke man daran, was für psychische Probleme bei Opfern von Mobbing oder der Verbreitung von Nacktfotos auftreten können.

Karina Filusch: Wir kennen alle diese Baustellenschilder, auf denen steht „Eltern haften für ihre Kinder“. Da kriegen Juristinnen und Juristen immer einen halben Anfall, weil zumindest in Deutschland die Regel gilt, dass jeder für sich selbst haftet. Auch ein Kind kann tatsächlich für sich selbst haften. Es ist nicht schön, wenn man schon im frühen Alter ein paar tausend Euro Schadensersatz abzahlen muss. Das ist ein schlechter Start ins Leben. Leider kann man das nicht auf die Eltern abwälzen. Da sind Kinder schon für sich selbst verantwortlich. Das ist ein großes Problem, vor allem im Internet. Deswegen ist es gerade so wichtig, dass die Kinder und Lehrer:innen geschult werden, so wie durch die großartigen Schulungen, die du anbietest. Das ist wichtig, damit sie einen guten Start haben und auch anderen nicht wehtun, so wie du es gerade auch nochmal schön beschrieben hast.

Miriam Reichelt: Ja, denn ich persönlich finde Schuld schlimmer als eine Geldstrafe. Also, wenn man Schuld auf sich geladen hat, weil man jemandes Leben zerstört, da wächst man nicht raus und das vergeht nicht.

Karina Filusch: Da hast du völlig recht. Miriam, gibt es noch ein anderes Thema, was du vielleicht ansprechen möchtest oder etwas, das du loswerden möchtest? Irgendwas, das wir noch unterbringen können oder sollten?





Miriam Reichelt: Ich persönlich würde mir wünschen, dass die Menschen die Angst vor dem Datenschutz verlieren. Ja, die DSGVO ist kein cooles Buch. Es macht keinen Spaß, die DSGVO zu lesen. Die Anwendung der DSGVO in der Praxis ist aber sehr spannend und Datenschutz ist extrem wichtig. Das muss nicht trocken und langweilig sein, überhaupt nicht. Deswegen sollte man sich einfach an das Thema herantrauen.

Karina Filusch: Was bedeutet für dich persönlich DaSou?

Miriam Reichelt: Datensouveränität ist für mich Teil der allgemeinen digitalen Souveränität, also das Erlangen von Wissen und Wegen, um einen gewissen Einfluss auf die Nutzung meiner Daten durch Unternehmen zu haben. Dazu gehört, dass ich zumindest eine grobe Vorstellung davon habe, wie und an wen meine Daten gehen und wie diese Daten genutzt werden können. In der analogen Welt müssen wir auch eine Menge lernen, verstehen und einschätzen können, um z.B. nicht beim ersten Versuch eine Straße zu überqueren, überfahren zu werden. Digital ist das nicht so viel anders.

Karina Filusch: Das ist ein schöner Vergleich, liebe Miriam. Vielen lieben Dank, dass du da warst und dir die Zeit genommen hast. Ich finde, jeder sollte so eine Schulung bei dir mitmachen, egal in welchem Alter oder egal welche Berufsgruppe. Du machst das echt super sympathisch, vor allem mit deinen Vergleichen, die einem noch mal aufzeigen, wie wichtig das ist. Vielen lieben Dank.

Miriam Reichelt: Ja, sehr gerne. Vielen Dank, dass ich zu Gast sein durfte. Es hat mir viel Spaß gemacht.

Aileen Weibeler: Ich finde v.a. die Konsequenzen für die jüngeren Menschen, von denen eben gesprochen worden ist, sehr erschreckend. Das sollte auf jeden Fall zum Nachdenken anregen, wirklich frühzeitig und präventiv zu handeln, gerade in den Schulen.

Karina Filusch: Ich hatte mit Miriam nach unserem Gespräch auch überlegt, wo ein Fach wie digitale Lehre wohl am besten zu verorten sein würde. Es passt nicht so richtig in den Politik- oder Sozialkundeunterricht. Eine Stunde im Jahr wäre auch viel zu wenig für das Thema, daher wäre es gar nicht so schlecht, das im Lehrplan zu verorten und vielleicht ein Schulfach daraus zu machen.





Rechtsanwältin Karina Filusch, LL.M. | Friedrichstraße 95, 10117 Berlin | T: 030 219 11 555

Aileen Weibeler: Ich glaube ja, dass das ein bisschen zu sehr in den Lehrplan in den Schulen eingreift, vielleicht könnte man eher über so eine Art Projektwoche, eine AG oder eine Art Seminar nachdenken, wo die Schüler am Ende einen Schein erwerben können, um einfach die Basics zu vermitteln. Den kann man gelegentlich wieder auffrischen, aber das sollte eher unabhängig vom Unterricht ablaufen.

Karina Filusch: Das finde ich eine sehr gute Idee. Ich hoffe euch hat die Folge Spaß gemacht und sie war hilfreich, hört doch beim nächsten Mal wieder rein, wenn wir wieder über DaSou sprechen. Wenn ihr Fragen zu DaSou habt, schickt uns eine E-Mail an hallo@dasou.law oder schickt uns einfach eine Twitter- oder Instagram-Nachricht und abonniert uns natürlich.

Aileen Weibeler: Bis bald.

Karina Filusch: Bis bald. DaSou ist eine Produktion der Kanzlei Filusch. Mehr Infos findet ihr auf unserer Webseite dasou.law. Die Redaktion besteht aus Anja Lindenau, Aileen Weibeler und Karina Filusch. Der Jingle wurde komponiert von Mauli. Die Idee zu DaSou hatte Axel Jürs. Das Cover hat Hélène Baum erstellt. Beraten wurden wir von Susan Stone. Editiert wurde der Podcast von Christoph Hinners.

