

## „Update verfügbar – ein Podcast des BSI“

Transkription für Folge 67

**Titel: Deepfakes & bildbasierte sexualisierte Gewalt**

*Moderation: Schlien Gollmitzer und  
Hardy Röde*

*Gast: Jacqueline Sittig, Deutscher Juristinnenbund e. V.  
(djb)*



---

**Schlien Gollmitzer:** Hardy?

**Hardy Röde:** Schlien?

**Schlien Gollmitzer:** Wie gut bist du in so TikTok-Tänzen?

**Hardy Röde:** Ach, also wenn du mich vor fünf Jahren gefragt hättest, hätte ich gesagt, ist das irgendwas, was im Schwarzwald hergestellt wird? Die Antwort ist auch im Jahr 2026 nicht besonders gut, weil ich weniger anschaue.

**Schlien Gollmitzer:** Also du weißt, was ich meine mit TikTok-Tänzen, wenn so die jungen Leute immer irgendwelche Choreografien bei Social Media durchtanzen. Und ich finde, es sieht immer so leicht aus. Aber wenn ich da mal damit anfangen, dann merke ich halt dann doch ganz schnell, dass der Disco-Fox von früher immer noch hart in meinen Knochen steckt und noch so einiges anderes anscheinend, was meine Beweglichkeit jetzt mit Mitte 40 mittlerweile etwas eingeschränkt.

**Hardy Röde:** Und das musst du dir auf TikTok rausschütteln, weil eigentlich müsstest du ja gar nicht mehr TikTok-Tanzen, wenn du noch Disco-Fox kennst. Und es gibt doch außerdem, falls du doch das bedarfst, das heißt jetzt die passenden KI-Tools, da musst du nur ein Foto von dir hochladen und dann wird ein Video von dir erstellt, in dem es genauso aussieht, als wärst du TikTok-Zielgruppe Mitte 20 und könntest panterhaft, agil jeden Dance-Move der Erde stehend in der Luft tanzen.

**Schlien Gollmitzer:** Mit meiner panterhaften Agilität. Ja, ganz genau. Das habe ich tatsächlich noch nie probiert. Aber auf die Art könnten wir uns ja zusammen vielleicht mal so eine Choreo erstellen, um dann auch diesen Podcast trennen zu lassen, vielleicht auf TikTok. Und dann wäre so ein Deepfake von uns zumindest mal zu was Sinnvollem gut. Denn in sehr vielen anderen Fällen sind diese Deepfakes ziemlich problematisch. Und darüber sprechen wir heute.

Das ist „Update verfügbar“. Ein Podcast des BSI. Für Sicherheit im digitalen Alltag. Mit Schlien Gollmitzer und Hardy Röde.

**Hardy Röde:** Wenn du mich nach meiner Lieblingschoreografie auf KI fragst, da wäre ich natürlich sehr dabei, wenn wir diese Szene, wo die beide so in der Luft schweben, bei The Matrix zusammen nachspielen. Und du weißt, was ich meine. Also ich bin der eine.... Aber wichtig ist, wenn ich es richtig sehe, du hast von problematischen KI-Simulationen gesprochen, dass wir beide wahrscheinlich einverstanden sind, bevor wir so eine Martial-Arts-Szene gemeinsam hier in die Luft legen.

**Schlien Gollmitzer:** Richtig. Und dann müssen wir aber selbstverständlich auch noch offenlegen, dass es sich um einen KI-generierten Inhalt handelt. Und da sind wir jetzt schon bei einigen wichtigen rechtlichen Fragen rund um sogenannte Deepfakes. Was wir uns heute allerdings noch genauer anschauen möchten in dieser Folge – und jetzt wird's ernst – sind sexualisierte Deepfakes. Und damit verlassen wir den Fun-Part der Unterhaltung und steigen in einen deutlich dunkleren Bereich der KI-generierten Netzinhalte ab. Vorher erklärt Hardy euch aber noch mal kurz die genaue Definition.

**Hardy Röde:** Deepfakes sind täuschend echt aussehende Medien, die mit künstlicher Intelligenz erzeugt oder manipuliert wurden. Meist sind es Videos, Bilder oder Audios, in denen Gesichter, Stimmen oder Bewegungen so verändert oder künstlich erzeugt wurden, dass sie zum Beispiel aussehen und klingen wie echte Personen. Dafür werden sogenannte neuronale Netze genutzt, die aus riesigen Mengen an Bild- und Tonmaterial lernen. Deepfakes werden zum Beispiel genutzt, um sich online als eine andere Person auszugeben, etwa für Betrug, Erpressung oder Identitätsdiebstahl. In anderen Fällen geht es Menschen darum, Falschinformationen zu verbreiten, etwa Politikerinnen oder Politikern Aussagen in den Mund zu legen, die sie nie gemacht haben. Ein besonders schwerwiegender Fall sind sexualisierte Deepfakes, bei denen echte Personen ohne Einwilligung in pornografische Szenen eingefügt werden. Weil Deepfakes so real wirken, wird es immer schwerer, Wahrheit von Fälschung zu unterscheiden.

**Schlien Gollmitzer:** Bevor wir jetzt weiter ins Thema einsteigen und ihr unsere Interviewpartnerin der heutigen Folge kennenlernt, möchte ich noch kurz den Hinweis an euch geben: Es geht in unserem Gespräch um sexuelle Gewalt. Wenn ihr selbst oder vielleicht jemand in eurem Umfeld Gewalterfahrungen machen musstet und ihr wisst, dass es euch schwerfällt, darüber zu hören, holt euch vielleicht noch jemanden mit dazu, damit ihr nicht allein seid oder skippt die Folge. Die wichtigsten Hinweise zur Hilfe für Betroffene setzen wir euch in die Shownotes.

**Hardy Röde:** Schlien hat mit Jacqueline Sittig gesprochen. Sie ist promovierte Juristin, Mitglied der Strafrechtskommission des Deutschen Juristinnenbunds und Expertin für bildbasierte sexuelle Gewalt, worüber sie auch ihre Doktorarbeit geschrieben hat, mit besonderem Fokus auf KI.

**Schlien Gollmitzer:** Eine wirklich beeindruckende Frau mit einem beeindruckenden Wissen über Paragrafen und Zusammenhänge, unser Thema betreffend, das in diesem Jahr ja nochmal besonders an Fahrt aufgenommen hat. Jacqueline, herzlich willkommen bei „Update verfügbar“ und danke, dass du dir die Zeit nimmst für uns.

**Jacqueline Sittig:** Ja Vielen Dank, Schlien. Ich freue mich heute mit dir über dieses spannende und hochaktuelle Thema zu sprechen.

**Schlien Gollmitzer:** Ja, hochaktuell ist es. Vor allem ist es dieses Jahr auch schon sehr hoch gekocht durch verschiedenste Fälle. Der bekannteste, Collien Fernandes, liegt auf dem Tisch.

Da werden wir auch noch ein bisschen drauf eingehen, auf jeden Fall. Aber das Thema Deepfake ist allgemein gesellschaftlich sehr hoch gekocht und durch KI natürlich immer aktueller geworden. Je weiter die KI fortschreitet, desto schlechter sind Deepfakes mittlerweile von der Realität zu unterscheiden.

Jacqueline, es ist ja dein Fachgebiet, auch das Thema, wofür du rechtlich absolut brennst. Kannst du uns mal so ein bisschen erklären, was verstehen wir denn unter bildbasierter sexualisierter Gewalt?

**Jacqueline Sittig:** Also bildbasierte sexualisierte Gewalt, das ist ein Überbegriff für viele Erscheinungsformen, die an sich gar nicht so neu sind. Also beispielsweise, wenn ein Exfreund nach dem Ende der Beziehung ursprünglich einvernehmlich erstellte Nacktbilder unbefugt verbreitet, dann ist das etwas, das wir als Phänomen, als Rache-Pornografie kennengelernt haben und das es auch schon seit Jahrzehnten gibt.

Das gibt es natürlich in analoger Form. Und nun mit der Digitalisierung bekommt das eben eine neue Tragweite, weil die Verbreitung im Netz von solchen Bildern, wir kennen es alle, einmal im Internet rasend schnell voranschreitet. Wir haben da eine Lawine der Verbreitung von solchen Aufnahmen.

Und bildbasierte sexualisierte Gewalt beschreibt Audio- oder visuelle Inhalte von den abgebildeten Personen, die quasi zur Sexualisierung herangezogen werden. Eine weitere Erscheinungsform ist zum Beispiel das sogenannte Upskirting und Downplousing. Also Upskirting, das meint mit einer Kamera –meistens mit so winzig kleinen Spy-Cams, denn das ist jetzt technologisch möglich –unter den Rock zu filmen oder zu fotografieren oder eben auch „down the blouse“, also in die Bluse hinein zu fotografieren.

Bekannt geworden ist das Phänomen damals im Rahmen von einer Petition, in der es darum ging, eben dieses strafrechtlich zu erfassen. Wir hatten dann tatsächlich auch einen Straftatbestand, der eingeführt wurde. Und all diese vereinzelt Ausprägungen der Erscheinungsformen von bildbasierter sexualisierter Gewalt haben natürlich eine neue Komponente bekommen, eine ganz neue Dimension durch den Einsatz von künstlicher Intelligenz, nämlich im Rahmen von sexualisierten Deepfakes.

Und während es da auch Unschädliche gibt, gibt es vor allem Schädliche, wenn das Einvernehmen fehlt, um diese Deepfakes zu erstellen. Und dann sprechen wir von nicht einvernehmlichen sexualisierten Deepfakes, die eben mit dem bloßen Auge gar nicht mehr zu erkennen sind. Aber wir alle können mittlerweile in pornografische Inhalte hineinretuschiert werden.

**Schlien Gollmitzer:** Du hast ja auch viel mit Betroffenen zu tun. Wenn du sagst, wir alle können da irgendwo Opfer davon werden: Wen betrifft denn bildbasierte sexualisierte Gewalt in erster Linie?

**Jacqueline Sittig:** Bildbasierte sexualisierte Gewalt betrifft uns alle, aber eben nicht alle gleich. Es ist ganz wichtig, das zu betonen, denn in erster Linie denkt man erst mal an die Betroffenen. Für die stellt das eine riesige Verletzung durch diese sexuelle Objektivierung dar. Das kann zu psychischen und aber auch zu körperlichen Schäden führen. Also natürlich betrifft es die Psyche, dass es etwas mit den Betroffenen macht. Das kann zu körperlichen Beschwerden führen und vor allem auch weitreichende Folgen haben, beispielsweise wenn personenbezogene Daten wie Handynummer oder E-Mail-Adresse mit solchen Aufnahmen veröffentlicht werden, dann sind die Betroffenen häufig auch finanziell geschädigt, wenn sie sich darum bemühen müssen, eben diese Daten zu ersetzen. Und betroffen sein kann potenziell jeder, denn es braucht nur ein paar Bilder im Internet, um einen qualitativ hochwertigen sexualisierenden Deepfake von uns zu erstellen.

Über diese Ebene, diese individuelle Ebene hinaus, gibt es auch eine gesamtgesellschaftliche Perspektive auf das Phänomen. Denn wir sehen in Studien, dass nicht nur diejenigen, die selbst betroffen sind von Hass im Internet oder von solchen Taten, sondern eben auch diejenigen, die sie nur wahrnehmen, also erleben, dass Personen diffamiert werden, beispielsweise mit solchen Deepfakes oder anderen Taten, dass die sich aus dem Internet zurückziehen. Und wenn wir uns dann anschauen, wer eigentlich besonders betroffen ist von diesen nicht einvernehmlichen sexualisierten Deepfakes, dann sehen wir, dass die Meinungsvielfalt im Internet zurückgeht.

Was meine ich damit? Wir haben genau drei Studien, die überhaupt erfassen, wer von nicht einvernehmlichen sexualisierten Deepfakes am meisten betroffen ist. Und nach diesen Zahlen von all den Deepfakes, die erstellt werden, sind ungefähr 93, 96 oder 98 Prozent der Inhalte pornografische Inhalte. Das heißt, diese humoristischen Bilder oder auch die Bilder, mit denen wir uns beschäftigen, im Rahmen von Meinungsfreiheit, das ist eigentlich nur die Spitze des Eisbergs.

Darunter liegen eben diese pornografischen Deepfakes, die ja fast nahezu alle Deepfakes ausmachen, die im Netz verbreitet werden. Wenn wir uns diese eben jetzt anschauen, dann sehen wir, dass nach den Studien ungefähr 99 Prozent all dieser sexualisierenden pornografischen Deepfakes Frauen darstellen. Bei dieser besonderen Betroffenheit sind es dann eben Frauen und auch weitere marginalisierte Gruppen.

Das kennen wir nämlich schon. Wir müssen hier das Rad nicht neu erfinden. Bei der digitalen Gewalt sind Frauen auf eine besondere Art und Weise betroffen, genauso wie weitere marginalisierte Gruppen, vulnerable Gruppen, wie beispielsweise Personen mit Migrationshintergrund. Wir sehen antisemitische und rassistische Vorgänge. Und es sind diese Personen, die sich in Folge von solcher digitalen Gewalt aus dem Internet zurückziehen. Und diese Meinungen finden dann eben in diesen virtuellen Räumen nicht mehr statt. Bildbasierte sexualisierte Gewalt betrifft uns alle auf der Individual- und auf der gesamtgesellschaftlichen Ebene.

**Schlien Gollmitzer:** Jetzt ist es ja so, du sagst, es betrifft uns alle. Es betrifft manche Personen eben ganz im Besonderen oder sehr persönlich. Und wir haben ja, ich habe es gerade schon angesprochen, einige bekannte Fälle aktuell auch auf dem Tisch liegen. Du hast auch diese bekannten Fälle auf dem Tisch liegen, unter anderem. Collien Fernandes ist jetzt dieser Fall, der in diesem Jahr sehr hoch gekocht ist und der jetzt auch zu einiger Bewegung in dieser Diskussion geführt hat. Es sind aber ja nicht nur Promis. Man hat immer so ein bisschen im Kopf: „Naja, gut, das sind halt sehr bekannte Personen. Deswegen kann denen so was passieren.“ Sondern es sind eben, keine Ahnung, die ganz normale Schliens aus München beispielsweise. Richtig?

**Jacqueline Sittig:** Du sprichst damit einen Punkt an, der sehr wichtig ist, denn digitale, geschlechtsspezifische Gewalt – und dazu gehört bildbasierte, sexualisierte Gewalt – ist Ausdruck und Fortsetzung bestehender Machtstrukturen und die trifft eben nicht nur die Personen des öffentlichen Lebens. Ganz klar muss man sagen, dass die Vorwürfe, die jetzt auch Collien Fernandes erhoben hat, Zeugnisse davon sind, dass es oft Personen des öffentlichen Lebens sind, die die Stärke haben, die Ressourcen haben, finanziell und vielleicht auch emotional abgehärteter sind, in der Sache nach außen zu treten, wenngleich natürlich persönlich nicht minder betroffen von diesen Taten, dass es die sind, die sich diesen Fällen aussetzen, die wirklich die Verfolgung suchen. Aber man kann nicht davon sprechen, dass nur Personen des öffentlichen Lebens von sexualisierenden Deepfakes betroffen sind. Ganz im Gegenteil. Diese Machtstrukturen, die bestehen auf allen Ebenen, in allen Altersklassen, in allen Schichten. Und diese Taten gehen eben häufig mit anderen Gewaltformen einher. Sie sind häufig Ausdruck von Kontrollverhalten. Sie kommen häufig aus dem sozialen Nahraum, wie beispielsweise die Vorwürfe von Collien Fernandes ja auch zeigten und sind eben einfach eine Fortsetzung von bestehenden Machtstrukturen.

Die Wissenschaftlerin Prasad sprach davon, dass man im Rahmen digitaler geschlechtsspezifischer Gewalt häufig eine Renaissance des „Victim-Blamings“ erlebe. Und damit hat sie vollkommen recht. Denn früher vor KI konnte man noch sagen: „Naja, wenn sie eben nicht möchte, dass Nacktbilder von ihr verschickt werden, dann soll sie eben einfach keine erstellen.“ Das ist natürlich in Zeiten von Deepfakes komplett hinfällig. Mittlerweile sind

wir alle potenziell Betroffene von solchen Deepfakes und wir alle begegnen diesen Deepfakes auch jedes Mal, wenn wir uns im virtuellen Raum bewegen.

**Schlien Gollmitzer:** Wenn wir uns mal die rechtliche Lage dahinter anschauen, speziell in Deutschland, welche Rechte werden denn hier verletzt beziehungsweise wo gibt es denn da auch noch Lücken im Strafrecht? Inwieweit ist das Ganze abgedeckt?

**Jacqueline Sittig:** Wenn wir uns rechtlich dem Phänomen von nicht einvernehmlichen sexualisierten Deepfakes widmen, dann wird es ganz schön kompliziert. Also ich puzzle gerne und genauso puzzeln muss man auch, wenn man sich den rechtlichen Rahmen anschaut. Denn wenn wir uns rechtlich den Schutzrahmen anschauen, dann ist das kein eigener Rechtsbereich, sondern eine Querschnittsmaterie.

Und wenn ich mich als Juristin dem Thema widme, dann schaue ich erst mal, welche Rechtsgüter sind denn da eigentlich verletzt? Da denke ich in erster Linie an das Recht auf sexuelle Selbstbestimmung, das uns aus dem Grundgesetz, dem höchsten deutschen Recht, zuspricht. Aber auch das allgemeine Persönlichkeitsrecht zum Beispiel, das Recht am eigenen Bild oder das Recht an der eigenen Stimme und dem Selbstdarstellungsschutz kann von Deepfakes erfasst sein. Genauso eben auch das Recht auf Nichtdiskriminierung, wenn wir anerkennen, dass es eben diese geschlechtsspezifische Dimension gibt.

Gleichzeitig das Recht auf informationelle Selbstbestimmung und natürlich auch das Recht auf körperliche Unversehrtheit, gerade wenn eben psychisch starke Belastungen auf so eine Verbreitung folgen oder eben auch in körperliche Beschwerden umschlagen. Und dann auf der anderen Seite gibt es vermeintlich eine Abwägung, dass man sich fragt, naja, ist das nicht eigentlich nur Ausdruck von Meinungsfreiheit? Kann das denn noch Ausdruck von Kunstfreiheit sein, wenn ich solche Deepfakes verbreite? Das sind so die Grundrechte, mit denen wir im Kern beginnen. Also ein Puzzleteil.

Und dann denken wir natürlich zunächst an das schärfste Schwert des Staates, an das Strafrecht und fragen uns, wie sind denn eigentlich Betroffene strafrechtlich geschützt vor der Herstellung, vor der Verbreitung oder vor anderweitigen Verwendungsformen im Rahmen von Deepfakes? Denn das muss man ganz klar sagen. Also natürlich gibt es das Herstellen und das Gebrauchen, aber es gibt auch anderweitige Verwendungsformen. Also typischerweise sind Begleittaten das Hacking, also das Beziehen von solchen Daten, um an diese Bilder zu kommen.

Wir haben das sogenannte Doxing, das Veröffentlichen von personenbezogenen Daten. Personenbezogene Daten sind all die Daten, die eine Identifizierung zulassen, zum Beispiel der Klarname, die Adresse, E-Mail-Adresse oder auch die Handynummer. Dann haben wir häufig Beleidigungsdelikte.

Beispielsweise, wenn solche Inhalte auf Foren verbreitet werden, in denen es Kommentarfelder gibt und dann dazu eingeladen wird, sich abfällig eben über diese Inhalte auszutauschen oder auch im Rahmen von Sextortion. Also wenn ich von dir, Schlien, jetzt zum Beispiel ein Deepfake erstelle, einen pornografischen Deepfake, und ich dich damit erpresse, um an echte Nacktaufnahmen von dir zu gelangen, weil ich eben sage, naja, wenn du mir die nicht schicken möchtest, dann schicke ich die an deine ArbeitskollegInnen und verbreite sie eben in deinem privaten Umfeld. Und das ist auch in den Vorwürfen von Collien Fernandes thematisiert worden, der Identitätsmissbrauch und der Diebstahl.

Ein weiteres Beispiel dazu wäre, wenn Deepfakes von Lehrkräften erstellt werden und dann auf Dating-Plattformen weiterverbreitet werden. Also es gibt allerlei Begleittaten. Und wenn wir uns das strafrechtlich anschauen, dann sehen wir, dass der strafrechtliche Schutz, zumindest für erwachsene Betroffene, fragmentiert, unübersichtlich und oft unzureichend ist.

Was meine ich konkret damit? Wir haben eine ganze Bandbreite von analogem Strafrecht, das jetzt auf digitale Lebensrealitäten trifft. Schauen wir uns zum Beispiel den Straftatbestand an, der die Verbreitung von gewaltpornografischen Inhalten abdeckt. Denn was zeigen solche Deepfakes? Das sind ja nicht nur unschuldige Bikini-Fotos, das können auch brutale, gewaltverherrlichende Gruppenvergewaltigungen sein. Dann könnten wir über diesen Straftatbestand sprechen. Aber natürlich ist da der Schwerpunkt eben auf der Verletzung des Persönlichkeitsrechts der dargestellten Person und deswegen nicht hinreichend zutreffend.

**Schlien Gollmitzer:** Es wird einem total schwindelig, wenn man sich durch all diese verschiedenen Gesetze durchhangeln muss und immer genau abwägen muss. Kann es drauf passen? Passt es absolut gar nicht? Oder streift es eventuell dieses Gesetz nur? Das ist ja absurd. Also das eine große Gesetz, das verbietet, dass beispielsweise einfach mit meinem Foto jetzt ein pornografischer Inhalt erstellt wird, gibt es nicht in dem Sinne?

**Jacqueline Sittig:** Nein, man muss das ganz klar sagen, und Schlien, wenn dir da schwindelig wird, dann bist du damit nicht alleine.

Man muss ganz klar sagen, das Herstellen wird derzeit nicht erfasst, unter Umständen das Verbreiten und anderweitige Verwendungsformen. Aber nicht systematisch, nicht in dieser Betroffenheit, wie wir sie erleben und vor allem auch wirklich fragmentiert im Einzelfall. Und das ist natürlich sehr ernüchternd für die Betroffenen, die sich dann fragen, ist denn mein Einzelfall dabei?

**Schlien Gollmitzer:** Ja, dann gehen wir doch mal in genau diesen Bereich, wo diese sexualisierten Deepfakes erstellt werden können. Welche Rolle spielen denn da die Anbieter entsprechender KI-Tools?

**Jacqueline Sittig:** Damit thematisierst du schon das, was auch die EU im Blick hat. Denn die EU sieht auch die Plattform in der Verpflichtung. Und wenn wir das nationale Recht betrachtet haben, also das Strafrecht, dann fragen wir uns natürlich, wie kommen die Betroffenen überhaupt an ihre Rechte heran? Und da greift das Zivilrecht. Für die zivilrechtlichen Unterlassungsansprüche, also Beseitigungs- und Unterlassungsansprüche, ist es ganz relevant, dass wir erst mal diese strafrechtlichen, rechtsverletzenden Inhalte überhaupt haben. Aber dann stellt sich natürlich die Frage, wie setzen wir diese durch? Einerseits könnten sich Betroffene an die Täter:innen direkt richten, aber diese sind häufig anonym und deswegen gar nicht greifbar für die Betroffenen. Und dann bleiben natürlich die Plattformen, auf denen diese Inhalte verbreitet werden.

Und hier sagt das EU-Recht mit Tools wie z.B. dem Digital Services Act (DSA), wie solche Meldeverfahren ausgestaltet sein müssen, dass Betroffene Inhalte niedrigschwellig melden können, damit diese Inhalte entfernt werden? Ganz konkret: Wir alle kennen diese drei magischen Punkte über jedem Inhalt, auf die klickt man drauf. Dann gibt es ein so genanntes Meldeverfahren. Und das EU-Recht sieht eben ganz konkret vor, wie diese ausgestaltet sein müssen.

Und auch da zeigt sich, so richtig ernst wird das nicht genommen und den Plattformen dafür ziemlich leicht gemacht. Denn geht man auf diese drei Punkte, sieht man meistens nur eine Oberfläche, die einem wie ein Multiple-Choice-Test zur Verfügung stellt, welcher rechtsverletzende Inhalt jetzt vorliegt. Dabei ist es eigentlich ganz klar, denn der DSA sagt, die Plattformen können in Kenntnis gesetzt werden.

Und wenn sie eben eine solche substantiierte Meldung erhalten haben, also dass ein rechtsverletzender Inhalt vorliegt, also positive Kenntnis davon, dann müssen sie diese Inhalte nach dem Notice-In-Action-Verfahren eigentlich direkt löschen. Diese Meldeverfahren sind aber so ausgestaltet, dass man durch die paar Klicks eigentlich gar nicht in der Lage ist, hinreichend darzulegen, wo denn jetzt die Rechtsverletzung besteht. Das heißt, wir haben hier Probleme, dass die Plattformen gar nicht hinreichend in Kenntnis gesetzt werden und die sich dann eben leicht rausreden können, dass sie ja gar nicht wussten, worin der rechtsverletzende Inhalt genau liegt.

Wir sehen hier vor allem auch eine Verlagerung der Verantwortung auf die Betroffenen selbst, die eigentlich eine juristische Einschätzung von ihrem Fall selbst abgeben müssen, um sagen zu können, worin die Rechtsverletzung jetzt in diesem fragmentierten Strafrechtsbereich überhaupt liegt. Was macht das mit der Praxis? Die Betroffenen haben häufig gar nicht die Möglichkeit, diese Meldungen an die Plattformen zu erstatten, weil sie einfach bei diesen ganzen Puzzlestücken gar nicht durchblicken können. Und was bleibt ihnen dann übrig? Sie haben die Möglichkeit, sich anwaltliche Beratung zu holen, die sehr kostspielig ist.

Nur wenige Anwäl:innen arbeiten noch unter 250 Euro Stundensatz. Das heißt, sie müssen eine Anwältin, einen Anwalt finden, der mit ihnen eine sogenannte Aufforderung zur Abgabe einer Unterlassungserklärung abgibt und diese dann quasi an die Plattform richtet. Und auch da sehen wir, dass es derzeit nicht so leicht ist. Wir kennen Fälle aus der Rechtsprechung, zum Beispiel die Politikerin Renate Künast, die derzeit vor dem BGH klagt, die eben auch versucht, Falschzitate von sich aus dem Internet entfernen zu lassen, ganz konkret von der Plattform Facebook von Meta. Und wir hatten das eben auch sehr viral, jetzt mit dem Fall von Dr. Eckart von Hirschhausen, der sich gegen Deepfake-Werbung auch auf Facebook gewährt hat. Hier wird jetzt gerade in der Rechtsprechung präzisiert, wann genau die Plattformen eigentlich handeln müssen und ob auch eine aktive Prüfpflicht besteht, nachdem erstmals ein Inhalt gemeldet wird.

Denn das muss man ganz klar sagen, die Inhalte verbreiten sich über die ursprüngliche Plattform hinaus und auch auf der ursprünglichen Plattform gibt es zahlreiche Kopien. Die Plattformen reden sich derzeit noch raus, dass selbst wenn sie einen Inhalt gelöscht haben, es keine Verpflichtung gäbe für sie, diese Kopien ebenfalls zu entfernen. Das heißt für die Betroffenen, dass sie wegen einem Deepfake wegen jeder Kopie neu losziehen müssten und jedes Mal wieder eine anwaltliche Beratung in Anspruch nehmen müssten, um diese Inhalte entfernen zu können.

**Schlien Gollmitzer:** Das bedeutet ja, dass das Opfer dafür verantwortlich ist, beispielsweise über eine Google-Rückwärtssuche rauszufinden, wo denn ein Bild überhaupt schon überall erschienen ist. Aber das Gleiche könnten doch die Plattform machen. Also gerade wenn es um Meta geht beispielsweise, da haben wir ja dann WhatsApp, Instagram, Facebook, alles zusammen.

### **Jacqueline Sittig:**

Also technisch ist es den Plattformen meinem Verständnis nach ohne Weiteres möglich, eben auch diese Kopien zu entfernen. Derzeit müssen sie es nach dem Recht aber nicht. Und solange wir die Rechtsprechung hier nicht haben, also vor allem vor unserem höchsten Gericht, vor dem Bundesgerichtshof, wo jetzt gerade das Verfahren von Renate Künast anhängig ist, werden sie auch erst mal keine Verpflichtung dergestalt haben, denn sie genießen das sogenannte „Host-Provider-Privileg“.

Das eben bedeutet, wenn sie als Plattform eine Plattform bieten, dann haften sie nicht direkt für die Inhalte, die verbreitet werden, weil sie ja quasi nur einen Ort zur Verfügung stellen,

wo andere ihre Inhalte verbreiten dürfen. Wie steht dieses „Host-Provider-Privileg“ zu unserer Verletzung von Datenschutzrechten? Also ist das Datenschutzrecht schwerer zu wiegen als dieses „Host-Provider-Privileg“? Und hier hat der EuGH tatsächlich jetzt grünes Licht gegeben für den Fall von Renate Künast und hat auch in einem anderen Verfahren, im „Russmedia-Urteil“, jetzt entschieden, dass das Datenschutzrecht tatsächlich höher zu werten ist als das „Host-Provider-Privileg“.

Das heißt, hier gibt es schon auch Hoffnung, je nachdem, wie sich der BGH jetzt entscheiden wird. Was wir in dem Kontext vor allem auch sehen, wenn Betroffene immer wieder wegen jeder Kopie losziehen müssen, ist eine große Reviktimisierung. Das sind ja belastende Inhalte für die Betroffenen. Sich jedes Mal erneut beispielsweise mit einer Deepfake-Gruppenvergewaltigung oder mit anderen sexualisierenden Objektivierungen auseinanderzusetzen, sorgt für eine große Reviktimisierung bei den Betroffenen, die jedes Mal wieder rechtssichere Beweise herstellen müssen, die jedes Mal wieder diesen Prozess bei den Plattformen durchlaufen müssen oder jedes Mal wieder anwaltliche Beratung in Anspruch nehmen müssen. Und da sieht man eben auch, warum es vor allem Personen des öffentlichen Lebens sind, die sich wehren, weil es eben extreme Ressourcen erfordert, jedes Mal gegen diese Inhalte vorzugehen.

**Schlien Gollmitzer:** Du hast das „Host-Provider-Privileg“ beschrieben. Das bedeutet dann ja im Grunde, solange sie es nicht selbst erstellt haben, sind sie nicht dafür verantwortlich, wenn ich das jetzt mal so richtig übersetze. Wenn wir uns das Ganze aber im Fall von X ehemals Twitter anschauen und diesem Grok-Bot, der hier erstellt wurde, der KI-Bot, der plötzlich dazu geführt hat, dass Personen Fotos von Kindern und jungen Frauen beispielsweise genommen haben und sie entweder in Bikinis oder nackt dargestellt haben. Wer ist dafür verantwortlich?

**Jacqueline Sittig:** Die Plattformen genießen eben dieses „Host-Provider-Privileg“, das ihnen zugesteht, dass, bis sie nicht positive Kenntnis von den Betroffenen erlangt haben, sie für diese Inhalte nicht haften. Also positive Kenntnis darüber, dass rechtsverletzende Inhalte verbreitet werden für jeden individuellen Inhalt, für jeden individuellen Post. Und worauf du ansprichst, das war eben die Causa Grok, dass der Grok-Chatbot Ende letzten Jahres, Anfang dieses Jahres mit Echtzugriff auf die Daten von der Plattform missbraucht wurde von Nutzenden, die diese generative KI genutzt haben, um nicht einvernehmliche sexualisierte Deepfakes von Personen zu erstellen.

Innerhalb kürzester Zeit wurden viele Bikini-Bilder von minderjährigen Frauen erstellt. Wir haben Erfassungen für den kurzen Zeitraum von fünf Tagen. Beispielsweise findet Grok darin über 50.000 Erwähnungen.

Und wenn wir uns diese 50.000 Erwähnungen anschauen, dann waren ungefähr 53 Prozent davon Bilder in minimalster Kleidung, also klassische Bikini-Fotos. Und auch da hatten wir wieder 81 Prozent Personen, die weiblich dargestellt waren, also weibliche Personen. Also wir sehen diese riesige geschlechtsspezifische Komponente.

Und auch hier greift natürlich das EU-Recht rein. Und zwar der DSA, den wir schon kennen, der Digital Service Act. Demnach muss derjenige, der eine KI anbietet, der einen Chatbot anbietet, vorher eine richtige Risikobewertung machen. Du musst Risiko mindern und du hast natürlich auch entsprechende Transparenzpflichten nach dem Digital Service Act. Und hier hat die EU-Kommission jetzt eine Prüfung eingeleitet, eine Untersuchung, inwiefern X dem nicht nachgekommen ist. Denn ganz klar war, X hat nicht reagiert auf die Kritik, dass diese „New-Defying-Funktion“ möglich war, sondern hat dieses Tool nach wenigen Tagen zu einem Geschäftsmodell gemacht. X sagte, diese Funktion könnt ihr weiter benutzen, aber nur innerhalb eines Abonnements, bei dem ihr Geld dafür bezahlt. Es ist ganz wichtig, das

zu betonen, denn bildbasierte sexualisierte Gewalt ist ein Geschäftsmodell für Plattformen. Solche Inhalte, die trenden, die gehen viral, die polarisieren. Und polarisierende Inhalte sorgen für mehr Aufmerksamkeit und bringen den Plattformen etwas. Deswegen ist es auch so wichtig, die Plattformen in Haftung zu nehmen. Denn sie sind letztlich diejenigen, die mit diesen Inhalten auch Geld verdienen. Durch Werbung und andere Möglichkeiten. Die EU reagiert nun auch weiterhin, denn bis Ende des Jahres muss die KI-Verordnung, also eine Verordnung über künstliche Intelligenz, umgesetzt werden.

Die KI-Verordnung sieht für Deepfakes tatsächlich nur ein minimales Risiko, was dazu führt, dass sie auch lediglich Transparenzpflichten, Kennzeichnungspflichten trifft. Und sie sagt eben, wer Deepfakes erstellt, der muss hinreichend kenntlich machen, dass es sich um ein Deepfake handelt. Ja, ein Witz für die Betroffenen, muss man ganz klar sagen. Denn ob das wirklich hilfreich ist für Betroffene, wenn auf meinen sexualisierten Deepfakes oben draufsteht, dass es sich um ein Deepfake handelt – ich wage es zu bezweifeln. Vor allem kann es auch technisch schnell umgangen werden. Denn diese Kennzeichnungspflicht kann nicht nur wie ein Wasserzeichen auf dem Bild sein, sondern darf auch in den Metadaten sein.

Und da treffen wir eben wieder auf den Umstand, dass man KI oder Deepfakes nicht nur rechtlich erfassen kann, sondern auch mit einem technischen Verständnis an die Situation herangehen muss. Denn diese Metadaten werden zum Beispiel überschrieben, wenn ich es über verschlüsselte Messenger schicke, wie beispielsweise WhatsApp. Wir haben da eine Ende-zu-Ende-Verschlüsselung. Habe ich da eine Kennzeichnung in den Metadaten, dann geht die mit einem Versand über WhatsApp verloren. Und da muss man natürlich sagen, da greift der AI-Act, also die KI-Verordnung, einfach zu kurz. Was die KI-Verordnung allerdings Positives bringt, ist, dass die EU nun im Rahmen der Verabschiedung beschlossen hat, dass sie auch ein Verbot von solchen Notification-Apps einführen möchte. Das heißt, das Herstellen sollte zumindest minimal schwieriger werden.

Jetzt ist es nur so, die Plattformen müssen sich natürlich auch daranhalten, diese Inhalte hinreichend zu schützen. Mit leichten Prompts kann man viele Barrieren, die Plattformen und Chatbots schon jetzt haben, auch umgehen. Ich kann auch mit ChatGPT, wenn ich weiß, wie ich den Prompt anpassen muss, auch immer noch solche Bilder erstellen, obwohl das eigentlich plattformintern nach der Regulierung nicht möglich sein sollte. Das heißt, wir haben hier auch wieder viele Lücken. Wir wissen auch, dass diese Apps natürlich auch über das Darkweb funktionieren.

Das heißt, nur weil es dann illegal ist, heißt es nicht, dass diese Inhalte nicht mehr erstellt werden. Generell gilt, dass wir viele Verbreitungsformen haben. Und auch hier sehen wir, wie misogynen Netzwerke dazu beitragen, dass sich solche Inhalte rasend schnell verbreiten.

Was ich damit meine, ist, dass es Bewegungen gibt, wie zum Beispiel die Incel-Bewegung. Incel steht für „involuntary celibate“, also unfreiwillig enthaltsam. Und das ist eine Bewegung, die vom Begriff her fast schon ein bisschen veraltet ist, aber die von einem Weltverständnis ausgeht, in dem Männer beispielsweise einen Anspruch auf Geschlechtsverkehr mit Frauen haben und die Frauen böse seien, weil sie ihnen das enthalten. Und aus diesem Gedankengut haben sich viele Untergruppen entwickelt, die wir heute unter dem Begriff „Manosphere“ zusammenfassen. Und diese Gruppen, die betreiben Netzwerke. Ein sehr bekannter Fall ist zum Beispiel der „deutsche Pelicot-Fall“, der kürzlich vor dem Landgericht I in München verhandelt wurde.

Worum ging es da? Das war ein Telegram-Netzwerk, das sich „Fahrschule“ nannte, mit mehreren Tausend Gruppenmitgliedern, die sich mit bildbasierter, sexualisierter Gewalt beschäftigt haben. Es ging in diesem „deutschen Pelicot-Fall“, ähnlich zu dem Fall von Frau Pelicot aus Frankreich, darum, wie man unter Intoxikation starke Vergewaltigungen

vornehmen kann. Und solche Plattformen waren dann dafür da, um sich darüber auszutauschen, nicht nur, wie viel Betäubungsmittel man bräuchte, sondern auch darum, Bildinhalte zu teilen, die man von diesen Vergewaltigungen erstellt hat.

Nur, um ein Verständnis dafür zu geben, wie der Ton in solchen Gruppen ist, wie die Sprache ist, mit der wir uns dort beschäftigen, wie das Umfeld ist: In dieser Gruppe wurden beispielsweise Frauen, wenn sie romantische Freundinnen oder Partnerinnen dieser Männer waren, als „Privatautos“ bezeichnet wurden. Wurden Frauen in diesen nicht einvernehmlichen Aufnahmen abgebildet, die besonders attraktiv waren, dann wurde von ihnen als „Luxusautos“ gesprochen. Frauen im betäubten Zustand wurden als „tote Schweine“ bezeichnet.

Diese Gruppe ist kein Einzelfall. Es gibt riesige Pornografie-Netzwerke. Die BBC berichtete im Februar beispielsweise von einer Plattform, bei der man besonders hervorheben muss, dass dort auch beworben wurde, dass man diesen Streams anschauen kann. Also Nutzende von solchen Plattformen teilen sich dann darüber aus, dass man sich ja käuflich, gewerblich in diese Streams einkaufen kann und dann eben auch sagen kann, was mit diesen Frauen passieren soll, wenn sie in einem betäubten Zustand sind.

Das alles gehört zum großen Weitblick von bildbasierter, sexualisierter Gewalt, von dem Klima, das online herrscht und das vor allem keine Randerscheinung ist. In dem Fall von der BBC, welcher jetzt im Februar dort verbreitet wurde, gab es 62 Millionen Aufrufe allein im Februar 2026. Und daran sehen wir, wie viel Interesse an diesen Ausprägungen bildbasierter sexualisierter Gewalt herrscht. Wir müssen davon ausgehen, dass sich eben auf solchen Plattformen, also seien es Mainstream-Pornografie-Plattformen, seien es nicht Mainstream-Pornografie-Plattformen, seien es öffentliche soziale Medien oder nichtöffentliche Plattformen wie Telegram oder WhatsApp, diese Inhalte verbreiten.

**Schlien Gollmitzer:** Was würdest du sagen, Jacqueline? Ist uns das jetzt schon alles entglitten? Kommen wir da überhaupt noch hinterher, rechtlich und gesellschaftlich?

**Jacqueline Sittig:** Ja, wir werden dem auf jeden Fall gerecht werden. Ich denke, dass es nichts bringt, den Kopf in den Sand zu stecken. Das wäre kontraproduktiv und würde auch nicht dem gerecht werden, dass es so viele mutige Menschen gibt, die öffentlich mit diesen Fällen umgehen. Denn das muss man ganz klar sagen. Es braucht ein gesamtgesellschaftliches Umdenken. Wir müssen gesamtgesellschaftlich anders mit diesem Thema umgehen. Aber allen Betroffenen steht das Recht trotzdem noch zur Seite. Wir versuchen, diese Strafrechtslücken zu schließen. Frau Dr. Hubeck hat nun ja auch einen Gesetzesentwurf aus dem Bundesjustizministerium vorgelegt, der viele Lücken schließen soll. Davon umfasst sind etwa das Herstellen von nicht einvernehmlichen sexualisierten Deepfakes. Das heißt, hier werden Lücken geschlossen werden. Genau so sollen auch Lücken geschlossen werden im Bereich bildbasierter sexualisierter Gewalt von Upskirting, Downplousing. Denn hier hatten wir die obskure Situation, dass solche Fälle von Orten, in denen wir regelmäßig nackt sind, wie Saunen, nicht unter diesen Straftatbestand gefallen sind. Also wurde ich in einer Fitnessstudio-Umkleide heimlich gefilmt, dann wurde es eben nicht erfasst, was ja eine absurde Situation ist, wenn man sich das vorstellt. Wie gesagt, hier haben wir jetzt viele Bemühungen sowohl national in Deutschland als eben auch in anderen Fällen. Es wird da wahrscheinlich die Herstellung miterfasst werden. Das Problem ist natürlich nur, man sieht häufig, dass das Verständnis für die geschlechtsspezifische Dimension fehlt. Das erkennt man etwa daran, dass man jetzt den Betroffenen auch in dem kommenden Straftatbestand auferlegt, dass es zu einer erheblichen Ansehensschädigung kommt. Also die Inhalte müssen dafür geeignet sein – und das sind natürlich weitere Hürden, die Betroffene erleben werden. Gleichzeitig gibt es oder gilt bis Juni nächstes Jahr noch eine weitere EU-Richtlinie umzusetzen. Das ist die Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häusliche Gewalt. Und auch die sieht einen

größeren Schutz vor. Also ganz so überraschend ist es nun nicht, dass so viel Engagement in der nationalen Gesetzgebung derzeit herrscht, denn das EU-Recht gibt eben einen Mindeststrafrahmen vor, eine Mindestregulierung vor, und Deutschland muss diesen einhalten bis zum nächsten Juni. Das heißt natürlich aber auch, dass Deutschland entscheiden kann, für einen höheren Schutz in Deutschland zu sorgen. Ich glaube nicht, dass wir machtlos dem Gegenüberstehen. Die Zeichen stehen trotzdem gut und mit all den Schäden, die KI hervorrufen kann, können wir KI auch nutzen, um uns eben vor solchen Deepfakes zu schützen.

**Schlien Gollmitzer:** Jacqueline, wir haben uns ja vor diesem Interview schon miteinander unterhalten und wir haben eigentlich gesagt, dass wir gar nicht so sehr den Fokus auf Betroffene legen wollen, sondern eigentlich die Täter adressieren, die in den Mittelpunkt stellen, nach dem Pelicot-Satz, den Giselle Pelicot gesagt hat: „die Scham muss die Seiten wechseln“. Trotzdem würde ich dich ganz gerne nochmal fragen. Was können denn Betroffene tun? Wo findet man Unterstützung? Diese drei Melde-Buttons, die man bei Instagram, Facebook und wo auch immer findet, haben wir schon gesagt, das ist ein bisschen schwierig, damit umzugehen. An wen kann man sich denn wenden? Und was sollte ich vor allem vor dieser Meldung bei der Plattform selbst unternehmen?

**Jacqueline Sittig:** Betroffenen würde ich raten, dass sie zunächst sich – mit Unterstützung oder alleine – rechtssichere Beweismittel erstellen. Wann sind denn Beweismittel rechtssicher? Es ist ganz wichtig, dass solche Screenshots oder Videos, die man von so einem Inhalt erstellt, die URL enthalten und das Datum, an dem der Inhalt gepostet wurde. Gegebenenfalls auch den Kontext, weitere Kommentare, weitere Einordnungen und auch das Datum, an dem dieser Screenshot dann erstellt wurde. Das sollte man vielleicht nicht alleine machen. Man sollte da auf jeden Fall auch um Hilfe bitten, wenn man sich jemandem anvertrauen kann. Denn auch hier gibt es wieder eine hohe Reviktimisierungsrate, denn häufig sind es ja mehrere Inhalte. Sich diese Inhalte immer wieder anzuschauen, das kann sehr belastend sein. Zum Glück gibt es ja aber Tools wie zum Beispiel das Tool von Netzbeweis, das es einem niedrigschwellig zugänglich macht, ganze Seiten kostenlos festhalten zu können. Gut, wenn ich das Beweismittel erstellt habe, dann sollte ich mich auf jeden Fall an so einer substantiierten Meldung versuchen. Ich sollte zumindest versuchen, die Plattform eben in diese positive Kenntnis von dem rechtsverletzenden Inhalt zu bringen. Und vielleicht löscht es die Plattform auch schon direkt. Wenn das nicht funktioniert, dann gibt es immer die Möglichkeit, sich auch anwaltliche und psychologische Hilfe zu suchen. Und da kann ich nur empfehlen, sich an NGOs wie beispielsweise Hate Aid zu wenden. Hate Aid ist eine NGO, die sich für die Rechte von Betroffenen digitaler Gewalt einsetzt. Und die helfen wirklich konkret psychologisch und rechtlich weiter. Die prüfen auch solche Fälle schon mal an. Und dann ist es ganz wichtig, sich im Weiteren Hilfe zu suchen und natürlich auch Hilfe anzubieten, wenn man von solchen Fällen hört, da solidarisch zu bleiben, weil es eben ein sehr schambehaftetes Thema immer noch ist. Und Schlien, du hast es schon gesagt, keinesfalls finde ich, dass da auch irgendeine Verantwortung bei den Betroffenen liegt. Leider ist es faktisch so, dass die diejenigen sind, die sich vor allem damit auseinandersetzen müssen. Aber natürlich liegt die Schuld und die Scham bei den TäterInnen, die solche Inhalte erstellen. Und da ist es eben gesamtgesellschaftlich unsere Aufgabe, wie gehen wir denn damit um, wenn wir davon hören, wenn wir solche Inhalte sehen.

**Schlien Gollmitzer:** Gott sei Dank gibt es Personen wie dich, die sich einsetzen für genau diese Rechte und dafür sorgen, dass wir künftig noch mehr solche Rechte bekommen und gerade als Betroffene geschützt sind, aber eben auch die Täter, die Plattformen, die Anbieter in die Verantwortung genommen und in den Fokus gestellt werden.

**Jacqueline Sittig:** Das ehrt mich natürlich, ich muss aber auch sagen, dass es ein hohes zivilgesellschaftliches Engagement gibt. Auch abseits vom juristischen Bereich sind es

NGOs wie Hate Aid, die sich unermüdlich dafür einsetzen und denen die Förderung gestrichen wird. Also wir haben Programme, denen die Förderung derzeit entzogen wird. In Zeiten wie diesen natürlich ein fatales Zeichen gegen digitale Gewalt oder den fehlenden Schutz. Und natürlich auch einzelne PolitikerInnen. Ganz wichtig ist es aber, dass wir alle, vor allem auch wir rechtsanwendenden Personen, und damit meine ich Staatsanwaltschaft, Richterschaft und auch diejenigen, die einen Erstkontakt zu den Betroffenen haben, wie die Polizei etwa oder Fachberatungsstellen, hinreichend geschult sind. Bisher gibt es keine verpflichtenden Schulungen für Richterschaft und Staatsanwaltschaft und Polizei im Bereich digitaler, geschlechtsspezifischer Gewalt. Und wenn ich schon kein Verständnis dafür habe über diese geschlechtsspezifische Komponente, dann kann ich Betroffene nicht hinreichend beraten. Wenn ich keine Informationen über die technischen Hintergründe habe, wie gerade solche Kennzeichnungspflichten funktionieren, dann kann ich eigentlich nicht gut beraten und da muss man ganz klar sagen, das geht auch über jede Argumentation der richterlichen Freiheit hinaus. Also wir müssen dieses Wissen einfach in alle Kreise bekommen.

**Schlien Gollmitzer:** Die Links, die Jacqueline gerade genannt hat, die werden wir euch auf jeden Fall auch in die Shownotes noch mit reinsetzen, zum Beispiel zu [Netzbeweis.de](http://Netzbeweis.de). Jetzt, Jacqueline, wollen wir aber trotzdem auf die Täter eingehen. Wir haben gesagt, wir wollen nicht die Betroffenen in den Mittelpunkt stellen, sondern die Täter.

**Jacqueline Sittig:** Ganz wichtig ist es, sich anzuschauen, warum macht man sowas überhaupt? Das scheint ja absurd. Wer würde jemandem sowas antun? Und da haben wir jetzt die ersten Zahlen und da will ich nur ganz kurz darauf eingehen, denn das zeigt nämlich auch, wie vielfältig dieses Phänomen ist. Vier Hauptbeweggründe werden genannt, wenn es um das Erstellen von solchen nicht einvernehmlichen sexualisierten Deepfakes geht. Und da wird als erstes der Vermögensvorteil genannt. Also dass tatsächlich das eben auch eingesetzt wird, um sich Vermögensvorteile zu erschaffen. Das zweite ist eine Schädigungsabsicht, gerade im Bereich von Rache. Es geht darum, dass man ja nach Intimbeziehungen oder zurückgewiesenen romantischen Annäherungen solche Inhalte erstellt hat und sie haben eben selbst auch angegeben, dass es da um Demütigung, um Rufschädigung, um Machtausübung und auch um die soziale Verstärkung durch die Peer Group geht. Also gerade junge Personen gaben an, dass es um so ein Bedürfnis der Zugehörigkeit und des Status geht, also so ein bisschen der Wettbewerb um Kreativität. Und den besonderen Grund, da habe ich wirklich aufgehört, als ich das gelesen habe in der Studie, da ging es um die Neugier und diese technologische Experimentierfreude. Das kann man sich gar nicht vorstellen, aber viele gaben an, und das wurde eben nur von den Tätern geschildert, dass es darum geht, solche technischen Möglichkeiten zu erproben. Also es ging um den Reiz dieser niedrighwelligen Zugangsschwelle und diese einfache Umsetzung. Und die Befragten, die gaben an, dass sie so ein „godlike feeling“ hatten. Also das Gefühl, Gott zu sein, weil sie solche Inhalte erstellen konnten. Also eine Kombination aus Kreativität und Technikinteresse. Besonders auffällig war, dass es vor allem ältere Täter waren, die das angaben. Also die Generation 35+, die eigentlich nicht direkt mit Computern aufgewachsen ist und diese fehlende, frühere Technikverfügbarkeit jetzt als Anreiz gesehen haben. Und das zeigt es eben.

**Schlien Gollmitzer:** Die Late Millennials, die sehr technisch interessiert sind.

**Jacqueline Sittig:** Genau, das zeigt warum sich diese Innovation so schnell verbreitet, so schnell verbessert, weil es eben auch dieses große technische Interesse gibt. Zusammengefasst, es ist rechtlich, technisch und gesamtgesellschaftlich ein Problem und auf diesen Ebenen müssen wir auch eine Lösung dafür finden und ich glaube, das ist auch gut möglich.

**Schlien Gollmitzer:** Dann darf ich mich ganz herzlich bedanken bei dir, Jacqueline. Danke, dass du dir die Zeit genommen hast.

**Jacqueline Sittig:** Vielen Dank für das Gespräch, Schlien.

**Hardy Röde:** Ja auf den ersten Blick denke ich mir als Nichtjurist, um Gottes Willen, wie kommt man denn da durch, durch dieses Gesetzeswirrwarr, wo, wie es Jacqueline ja im Interview mit Schlien sagte, dass sie sich da wie in einem Puzzle eine gesetzliche Grundlage zusammenstückeln muss, um tatsächlich so einen Fall von sexualisiertem Deepfake anzugehen.

**Schlien Gollmitzer:** Ja, wie sie ja gesagt hat, es werden im Grunde analoge Gesetze auf die digitale Welt angewandt und da haben wir auf jeden Fall noch Nachholbedarf und das muss angepasst werden.

**Hardy Röde:** Aber sie hat ja auch gesagt, dass dran gearbeitet wird an diesen Anpassungen, dass vom Gesetzgeber her die Notwendigkeit gesehen wird, dass das Thema ernst genommen wird. Siehst du es auch so?

**Schlien Gollmitzer:** Definitiv. Das hat mich auch sehr beruhigt. Also gerade, dass es Menschen wie Jacqueline gibt oder auch Hate Aid und dass die Gesetzgebung da durchaus dran arbeitet, dass die das also im Blick haben. Der Zug ist also noch nicht abgefahren. Wir müssen halt jetzt mal zusteigen, langsam, aber sicher. Aber wir sind auf dem richtigen Weg. Das habe ich jetzt mal so mitgenommen aus diesem Interview. Und ich möchte auch nochmal betonen, unsere drei konkreten Tipps für heute beinhalten nicht den Ratschlag, keine Fotos von sich im Internet zu veröffentlichen, weil das zu kurz gedacht wäre und dann eben zu diesem Chilling- oder Silencing-Effekt führt, sodass bestimmte marginalisierte Gruppen im Internet nicht mehr stattfinden.

**Hardy Röde:** Und das führt dann letztendlich auch wieder zu dieser Täter-Opfer-Umkehr, über die ihr im Gespräch auch gesprochen habt.

**Schlien Gollmitzer:** Ganz wichtig, die Verantwortung muss bei den Tätern bleiben. Wir alle haben schon irgendwann mal Fotos hochgeladen. Viel wichtiger sind unsere drei konkreten Tipps. Wissen, welche Schritte im Ernstfall zu gehen sind. Ich fasse es nochmal zusammen: Punkt Eins: Sich jemandem anvertrauen und gemeinsam Beweise sichern. Das ist das Wichtigste gleich zu Beginn. Zum Beispiel über Netzbeweis. Jacqueline hat diese Seite schon genannt. Punkt Zwei: Offizielle Meldung bei der Plattform, auch ganz wichtig. Hört euch gerne noch mal im Interview die Stelle an. Jacqueline hat es erklärt, warum das so wichtig ist. Und Punkt Drei: Rechtliche und psychologische Beratung suchen. Zum Beispiel bei Hate Aid eben. Und auf jeden Fall mit den Beweisen auch umgehend an die Polizei wenden.

**Hardy Röde:** Ja, das hatten wir jetzt schon oft bei solchen Themen bei „Update verfügbar“, dass eine Anzeige bei der Polizei zu erstatten immer, immer, immer notwendig ist, der richtige Weg und euch dann letztendlich, wenn ihr Opfer seid von so einer Tat, im Endeffekt auch schützt und euch eine Sicherheit gibt. Und weil es aber auch uns alle treffen kann, müsst ihr nicht die Schuld bei euch suchen. Also die Scham muss die Seite wechseln. Dieser große Satz, der hat hier definitiv Gültigkeit.

**Schlien Gollmitzer:** Und das war's jetzt, das war unsere Folge 67 von „Update verfügbar“. Wie gesagt, alle wichtigen Informationen und Hilfestellungen zum Thema Umgang mit sexualisierten Deepfakes, vor allem für Betroffene, bekommt ihr natürlich auf der Seite des BSI. Und hier in den Shownotes setzen wir euch noch sämtliche Links mit rein. Auch das, was Jacqueline genannt hatte, Netzbeweis, dieses Tool.

**Hardy Röde:** Und wenn ihr euch für Sicherheit im Netz interessiert, dann könnt ihr uns auch folgen auf Instagram, Mastodon oder YouTube. Da gibt es mehr Infos zu allen

sicherheitsrelevanten Fragen vom BSI. Und abonniert doch bitte auch diesen Podcast, damit ihr keine neue Folge verpasst. Wir hören uns im nächsten Monat wieder, sagen Tschau und bis zum nächsten Update.

**Schlien Gollmitzer:** Bis zum nächsten Update!