Martin-Luther-Universität Halle-Wittenberg
Naturwissenschaftliche Fakultät III
Institut für Informatik

Seminar

Informatik und Gesellschaft

Sommersemester 2019

geleitet durch Prof. Dr. Paul Molitor

Sexuelle Ausbeutung von Kindern und Jugendlichen im Internet

Leonie Collmann

Inhaltsverzeichnis

Gender-Hinweis: Die weibliche Form ist der männlichen Form in dieser Arbeit gleichgestellt; lediglich aus Gründen der Vereinfachung wurde die männliche Form gewählt.

Überarbeitung durch den Dozenten: Der vorliegende Text entspricht im Wesentlichen dem ursprünglichen durch Frau Collmann erstellten Bericht. Der Dozent hat lediglich einige wenige Schreib- und Kommatafehler entfernt sowie Formatierung angepasst.

1 Hintergrund

Das Internet hat auf fast alle Bereiche des persönlichen und öffentlichen Lebens Einfluss. Ob dieser Einfluss positiver oder negativer Natur ist, ist meist keine leicht zu beantwortende Frage. Unweigerlich ist jedoch, dass durch die Vernetzung neue Wege für die Verbreitung von Daten entstehen und dass diese Daten erreichbarer für alle vorhandenen Nutzergruppen werden. Durch die rapide Verbreitung von mobilen Endgeräten haben inzwischen 78 % aller Deutschen ein Smartphone [1], d.h. sie können fast überall auf das Internet zugreifen, Dinge teilen und Inhalte konsumieren.
Auf vielen Smartphones installiert sind Social Media Applikationen (kurz: App), die zur Selbstdarstellung im Netz oder zur Kommunikation dienen. Die Hemmschwelle für das Teilen von sensiblen und privaten Inhalten sind seit dem Popularitätszuwachs solcher Apps wie WhatsApp[1], Snapchat[2] oder Instagram[3] gesunken. Anstatt, dass Fotos von den eigenen Kindern in physischen Fotoalben gesammelt und zu besonderen Anlässen angeschaut werden, teilen viele Eltern schon kurz nach der Geburt ungeachtet von Persönlichkeitsrechten Bilder ihrer Kindern mit Freunden und Bekannten, manchmal sogar über öffentliche Statusmeldungen oder Bildergalerien (z.B. über Instagram). [2] Dies macht es potenziellen Tätern einfach, Bilder von fremden Kindern zu erlangen und ohne das Wissen der Eltern weiterzuverbreiten.
Auch wenn einige Eltern nur Fotos teilen, auf denen nicht das Gesicht ihres Kindes zu sehen ist, kann dies weitreichende Folgen haben. Wenn beispielsweise die Ortsbestimmung auf dem Gerät aktiviert ist, mit dem das Foto aufgenommen wurde, können andere Nutzer, die auf das Bild zugreifen, den Wohnort des Kindes metergenau herausfinden.
Wie lassen sich solche Risiken mit einer digitalen Kultur vereinbaren, in der das Teilen von privaten und zum Teil sensiblen Inhalten unterstützt, gefordert und als Form der Selbstvalidierung Teil eines neuen Selbstverständnisses wird? Und wie können Kinder und Jugendliche vor den Gefahren geschützt werden, die durch die Vernetzung möglich werden, und die man meist erst erkennt, wenn es zu spät ist?

[1] Nachrichtendienst mit der Zusatzfunktion, Bilder als Status allen Kontakten zugänglich zu machen
[2] Dienst zum Teilen von Inhalten, die dem Empfänger nur für kurze Zeit zur Verfügung stehen.
[3] Dienst zum Verbreiten von Grafikinhalten

1.1 Rechtslage

Um sich diesen Fragen zu stellen ist es zunächst nötig, die relevanten Gesetze darzustellen. Das Strafgesetzbuch beschreibt verschiedene Formen von Kindes- und Jugendmissbrauch. Im Umfang dieser Arbeit sind insbesondere die Paragraphen 176, 182, 184b und 184c relevant.
Generell ist nach dem Jugendschutzgesetz ein Kind definiert als eine Person, die noch nicht 14 Jahre alt ist, ein/e Jugendliche/r ist definiert als Person, die 14, aber noch nicht 18 Jahre alt ist. [3]

§ 176 Sexueller Missbrauch von Kindern

In § 176 wird definiert, dass sexuelle Handlungen an/mit Kindern sowie der Einfluss auf Kinder, sexuelle Handlungen an Dritten vorzunehmen, strafbar sind. Des Weiteren ist es strafbar, mittels Informations- und Kommunikationstechnologien (wozu das Internet zählt) auf Kinder sexuell einzuwirken, d.h. sie zu sexuellen Handlungen zu bringen oder mittels pornographischer Inhalte zu beeinflussen. [4]

§ 182 Sexueller Missbrauch von Jugendlichen

Als sexueller Missbrauch von Jugendlichen ist nach § 182 definiert, durch Ausnutzen einer Zwangslage eine Person unter 18 Jahren durch sexuelle Handlungen zu missbrauchen oder sie dazu zu bringen, sexuelle Handlungen an Dritten zu verüben. Außerdem ist es strafbar, wenn eine Person, die älter ist als 21 Jahre, sexuelle Handlungen an einer jugendlichen Person unter sechzehn Jahren verübt, wenn dabei die fehlende sexuelle Selbstbestimmung des Opfers ausgenutzt wird. [5]

§ 184b Verbreitung, Erwerb und Besitz kinderpornographischer Schriften und § 184c Verbreitung, Erwerb und Besitz jugendpornographischer Schriften

Als kinderpornographische Schrift („Schrift“ hier: beliebige Form von Medium) ist definiert, was sexuelle Handlungen an oder vor einem Kind als Inhalt hat, oder „die Wiedergabe eines ganz oder teilweise unbekleideten Kindes in unnatürlich geschlechtsbetonter Körperhaltung oder die sexuell aufreizende Wiedergabe der unbekleideten Genitalien oder des unbekleideten Gesäßes eines Kindes“ zeigt [StGB, § 184b.1 Abschnitte b und c]. Als jugendpornographische Schrift ist definiert, was „sexuelle Handlungen an oder

vor einer jugendlichen Person zwischen 14 und 17 Jahren zeigt, oder die Wiedergabe einer nackten jugendlichen Person in unnatürlich geschlechtsbetonter Körperhaltung.“ [7] Die Erstellung, Verbreitung und der Besitz kinder- und jugendpornographischer Medien ist strafbar. [6] Die einzige Ausnahme bilden jugendpornographische Inhalte, die nicht weitergegeben/veröffentlich werden und mit Einwilligung der dargestellten Person/en erstellt wurden. Da die Veröffentlichung von Jugendpornographie weiterhin strafbar bleibt, ist sie auch Thema dieser Arbeit.

1.2 Begriffsklärung

Gaslighting

Das Gaslighting stellt eine extreme emotionale Manipulation des Opfers dar, das dazu gebracht werden soll, an seiner Realitätswahrnehmung zu zweifeln. Generell wird es von einem einzelnen Täter ausgeführt mit dem Ziel, nach und nach das Selbstbewusstsein des Opfers zu schwächen, sodass es in der Unterscheidung zwischen wahr und falsch verunsichert wird. [8] Der Täter stellt sich als Vertrauensperson dar, Eltern/Familie und Freunde des Opfers werden in schlechtes Licht gerückt, damit sich das Opfer von diesen entfremdet. In vielen Fällen fühlt sich das Opfer selbst schuldig und vereinsamt, die Wiederherstellung des verlorenen Vertrauens in die Familie kann ein schwieriger Prozess sein.

Cybersex

Als Cybersex wird sexueller Kontakt über Computertechnologie bzw. über das Internet bezeichnet. Dies schließt sowohl Kommunikation via Chat/Voicechat, Videochat als auch das Senden von Nacktbildern mit ein. [9]

Grooming

Grooming, auch Cyber-Grooming genannt, ist eine Taktik, um das Opfer an missbräuchliches Verhalten zu gewöhnen, indem der Täter graduell die Schutzmechanismen des Opfers desensibilisiert. Zuerst sehr positives, freundliches Verhalten dem Opfer gegenüber wird langsam durch negatives, missbräuchliches Verhalten ersetzt, sodass das Opfer zwar durch den Tonwechsel verunsichert werden kann, aber aufgrund der Menge an positivem Einfluss nicht alarmiert wird. Mit der Zeit kann die Interaktion sehr

fordernd und übergriffig werden, was vom Opfer durch das langsame Heranführen an solches Verhalten nicht als unangemessen wahrgenommen wird. [10]

Posing

Posing ist ein besonders im deutschen Sprachraum genutzter Begriff, der das sexualisierte Darstellen von Kindern und Jugendlichen beschreibt. Das Posing erfüllt die Definition von Kinderpornographie, da es Kinder/Jugendliche in sexualisierter Weise zum Beispiel in Badesachen, Unterwäsche oder Reizwäsche zeigt. Posing wird oft von Missbrauchstätern genutzt, um Bilder anzufertigen, die sie in Netzwerken teilen oder selbst nutzen.

2 Das Internet als Instrument zum Missbrauch

2.1 Smartphones in Kindeshand

Bereits kleine Kinder werden mit Tablets an die digitale Welt gewöhnt. Hierzulande beträgt der Anteil an Kindern im Alter von 6-7 Jahren mit Tabletnutzung schon 78 %. Im Alter von 10 Jahren haben dann bereits 75 % aller Kinder ein eigenes Smartphone und sind selbständig im Internet unterwegs. 78 % der 10- bis 18-Jährigen nutzen Foto- und Videofunktionen ihrer Smartphones. Besonders beliebt sind WhatsApp, TikTok[4], Instagram und Snapchat. [11] Dies führt dazu, dass Jugendliche und vor allem Kinder, die sich ihres Handelns noch nicht vollständig bewusst sind, Inhalte teilen, die potenziell von Pädophilen und Missbrauchs-Tätern gesucht und gefunden werden können. [12] Auch wenn viele Apps inzwischen eine Altersprüfung einbauen, können diese von jungen Kindern leicht umgangen werden, indem sie ein früheres Geburtsdatum angeben, als sie tatsächlich besitzt. [13] Eine Lösung bestände darin, Kindern bis zu einem gewissen Alter komplett den selbständigen Zugriff auf der Internet zu verwehren oder zumindest von Eltern- und Lehrerseite ein hohes Maß an Aufklärung zu betreiben, wie sich Kinder verhalten müssen, um sich und ihre Privatsphäre zu schützen. In einigen Fällen dreht sich jedoch die Problemstellung um, und zwar dann, wenn die Eltern weniger Ahnung von der Materie haben, als ihre Kinder.

[4] App, bei der kurze Videos geteilt werden, die meist Lippensynchronisation von Liedern zum Inhalt haben

2.2 Unkenntnis der Eltern

Ein großes Problem stellt es dar, wenn Eltern die Bilder ihrer Kinder (z.T. Bilder, in denen die Kinder nackt zu sehen sind, am Strand oder beim Spielen mit Wasser) online posten. Auch wenn es sich hier offensichtlich nicht um Kinderpornographie handelt, da die Kinder in einem Kontext ohne sexuelle Komponente fotografiert wurden, kann es sein, dass Pädophile diese Bilder nutzen und ohne das Wissen der Eltern weiterverbreiten. Abgesehen von diesem Faktor geschieht das Teilen der Fotos auch oft gegen den Willen der Kinder, die sich in sehr jungem Alter noch nicht bewusst sind, was genau ein Foto an Bedeutung hat und dass einmal geteilte und gespeicherte Fotos quasi für immer persistiert sind.
„Kinder selbst haben oftmals genaue Vorstellungen davon, ob, wann und mit wem Bilder von ihnen geteilt werden sollten. Allerdings werden sie von den Eltern in der Regel nicht an Entscheidungen beteiligt, wenn diese Fotos von ihnen verbreiten. Die Rechte von Kindern spielen insofern im Rahmen von Medienerziehung in der Familie oftmals kaum eine Rolle.“ [Studie zu Persönlichkeitsrechte von Kindern im Kontext der digitalen Mediennutzung in der Familie vom deutschen Kinderhilfswerk] [15] Das Phänomen nennt sich „Sharenting“ (zusammengesetzt aus „parent“ und „sharing“) und ist in den letzten Jahren immer öfter zum Thema von Debatten geworden. [14]
Diese Diskrepanz zwischen den Medienverständnissen von Kindern und Eltern führt möglicherweise dazu, dass Kinder und Jugendliche ihre Eltern nicht involvieren, wenn sie im Internet in unangenehme Situationen geraten. Solche Situationen können von Mobbing und Streitereien bis hin zu Missbrauch durch Unbekannte gehen. Die Opfer fühlen sich von ihren Eltern nicht verstanden und verheimlichen die Situation lieber, auch aus Angst, dass ihre Eltern sie in der Schuld sehen.

3 Missbrauch im direkten Kontakt

Zum Missbrauch an Kindern und Jugendlichen durch sexuelle Annäherung kann es kommen, wenn ein Täter in direktem Kontakt mit einem Kind/Jugendlichen steht. Meist wird ein solcher Kontakt über Chats, Social Media oder Messengerdienste hergestellt. Dabei gibt es verschiedene Wege, wie ein potenzieller Täter an die Kontaktdaten möglicher Opfer gelangen kann.

3.1 Chats

Eine dieser Möglichkeiten besteht durch öffentliche Chaträume. Obwohl solche Chats in den letzten Jahren stark an Nutzern verloren haben, bieten sie trotzdem den Raum für Missbrauchstäter, Kontakt zu Opfern zu knüpfen.
Anhand einer Platform wie `Knuddels.de` lässt sich zeigen, wie Täter agieren, um Kontakt zu fremden Kindern und Jugendlichen aufzubauen. Zunächst kurz etwas zur Geschichte der Seite: `Knuddels.de` wurde 1999 gegründet, um eine neue, interessante Chaterfahrung zu bieten. Dies beinhaltete Chaträume für viele verschiedene Themen und interaktive Chatspiele. Anfang der 2000er hatte die Platform zwischenzeitlich Millionen aktiver Nutzer, was in den letzten Jahren auf ca. 200.000 bis 300.000 gesunken ist. In den Anfängen gab es auch Chaträume für Kinder, die sich dort mit gleichaltrigen austauschen konnten. Auch so genannte „Flirt-Channels“ wurden eingerichtet. 2013 wurde das Mindestalter für die Anmeldung auf 14 Jahre angehoben und die Kinder-Chaträume entfernt. Nutzer unter 16 Jahren müssen zudem einen Jugendschutz-Test ablegen, bevor sie uneingeschränkt chatten können. Alter und Geschlecht werden seit 2010 im Profil eines Nutzers angezeigt und sind frei einsehbar. Chats zwischen Kindern und Erwachsenen werden mit Hilfe eines Wortfilters überwacht, d.h. sobald bestimmte Wörter genutzt werden, wird das Gespräch blockiert. Für einige Chaträume wird eine Altersverifizierung mit der Eingabe von Daten aus dem Personalausweis durchgeführt, diese sind dann die einzigen Bereiche, auf die nur eindeutig identifizierte Personen mit korrekt angegebenem Alter zugreifen können. [25]
Die Seite stand in ihrer Geschichte oft in der Kritik, Pädophilen und anderen Tätern einfachen Zugang zu Kindern zu bieten. Auch durch die Tatsache, dass man bei Registrierung zwar sein Alter angeben muss, aber ohne eine Verifizierung (z.B. per Personalausweis) anmelden kann, können Kinder unter 14 Jahren die Regeln umgehen und trotzdem registrieren. Das gleiche gilt für die Täter, die sich oft als Kinder ausgeben. [26] Während öffentliche Chaträume noch durch Moderatoren überwacht werden, kommen bei privaten Chats oft nur automatische Filter zum Einsatz, die leicht von den Tätern durch Euphemismen umgangen werden können.
Typischerweise suchen Täter in öffentlichen Chaträumen nach möglichen Zielen, die sie über eine Funktion für private Nachrichten direkt anschreiben. Nach einer anfänglichen Kontaktaufnahme wird oft versucht, das Opfer auf einen Messengerdienst umzuleiten, sodass der Kontakt jenseits von moderierten oder gefilterten Portalen abläuft. Durch Einsatz von Cyber-Grooming wird das Opfer zunächst mit Komplimenten, Smileys, und

freundlichen Angeboten in einer falschen Sicherheit gewogen, danach lässt der Täter nach und nach missbräuchliches Verhalten einfließen und äußert unangemessene Forderungen wie z. B. nach einem Videochat oder Fotos. [16] Kinder können nicht immer differenzieren, was als gefährliches Verhalten zu deuten und zu melden ist, und melden solche Vorfälle nur selten ihren Eltern. Falls der Täter nach längerem Gesprächsverlauf genug Einfluss auf das Opfer hat, besteht das Risiko, dass er über Gaslighting das Opfer so weit verunsichern, dass es das Vertrauen in die Eltern oder das soziale Umfeld verliert und ein zu großes Vertrauen dem Täter entgegenbringt. Im schlimmsten Fall kommt es zu einem Treffen zwischen Täter und Opfer, was körperliche Misshandlung und schlimmeres zur Folge haben kann. Um so etwas zu verhindern, sind Polizei und Portale bemüht, gefährliche Konversationen herauszufiltern und einzugreifen, bevor ein Täter auf private Messengerdienste wie Facebook, WhatsApp oder Snapchat umlenken kann.

3.2 Lösungsansätze gegen missbräuchlichen Kontakt

Ein Problem, auf das deutsche Behörden beim Aufspüren von Tätern stoßen, sind die gesetzlichen Vorgaben. Nach deutschem Recht kann ein Täter strafrechtlich nur dann verfolgt werden, wenn er tatsächlich mit einem Kind auf missbräuchliche Weise kommuniziert hat. Wenn Beamten sich in Chaträumen als Kinder ausgeben, um Kontakt zu potenziellen Tätern zu knüpfen, können diese nur strafrechtlich verfolgt werden, wenn bei ihnen der Besitz von Kinderpornographie oder ein anderer Verdacht nachweislich besteht. Ansonsten können die Behörden auf diese Weise nur Daten sammeln und die auffälligen Konten sperren lassen. Diese tauchen jedoch schnell wieder auf, weil die Schwelle zur Erstellung eines neuen Nutzerkontos niedrig ist.

3.2.1 Privalino und ähnliche Technologien

Projekte wie Privalino, eine KI, die mittels Analyse von Messenger-Texten gefährliche Inhalte analysieren und melden kann, bieten das Potenzial, Online-Messaging sowohl in Chats, als auch über Messenger wie WhatsApp sicherer zu machen. Im Einsatz im Produkt WhatsSafe der Kitext GmbH läuft die Software über Server, die nach einer Koppelung zu WhatsApp die eigentlich verschlüsselten Chats analysieren und bei einem potenziell gefährlichen Verlauf die Eltern per Mail informieren kann. [27] Eine solche Lösung bietet hohe Effizienz, bricht aber die Verschlüsselung des Dienstes und sendet den Gesprächsverlauf an Server, um sie zu analysieren. [28] Diese Art der

Analyse führt unweigerlich zu Datenschutzrisiken. Außerdem kann die Nutzung eines derartigen Service das Vertrauensverhältnis zwischen Eltern und Kind einschränken, da die Eltern bei einem Verdacht auf missbräuchlichen Kontakt informiert werden und angehalten sind, auf dem Endgerät des Kindes den Chatverlauf nachzulesen.

3.2.2 Ausweispflicht

Eine Lösung, die sowohl zum Einhalten von Altersrichtlinien, als auch zum Verhindern von multiplen Accounts durch Missbrauchstäter eingesetzt werden kann, ist ein Ausweisabgleich. Hierbei wird über die Identifikationsnummer das Alter ausgelesen und die Angaben über Prüfziffern verifiziert. Dies würde Nutzern unter 18 Jahren die Nutzung von Chatseiten und ähnlichen Portalen verwehren, aber im Gegenzug die Schwelle für Täter deutlich anheben. Allerdings sind solche Verfahren nicht vollständig sicher, da eine gültige Nummer gefälscht werden kann [29]. Für die Seitenbetreiber stellt dies ein Risiko dar, da sich viele Nutzer von einer solchen Identitätsprüfung abschrecken lassen und lieber andere Angebote nutzen.

3.2.3 Weiterbildung

Die vermutlich einfachste und weitreichenste Lösung stellen Weiterbildungen für Eltern, Kinder und Lehrkräfte dar. Anlaufstellen wie „Kein Raum für Missbrauch“ [30] bieten Informationen und Materialien, die im Unterricht eingesetzt werden können, um Kinder für Missbrauchsmuster zu sensibilisieren und ihnen helfen sollen, das nötige Selbstbewusstsein aufzubauen. Eltern sollten sich damit beschäftigen, was ihre Kinder online tun und ihnen die Möglichkeit bieten, ohne Verurteilung über alles zu reden. Durch transparenten Diskurs können Eltern und Kinder eine Vertrauensbasis aufbauen, die es ermöglicht, dass diese selbstständig online unterwegs sind.

4 Kinder- und Jugendpornographie

Untersuchungen des Kieler Uniklinikums haben gezeigt, dass im Gehirn von Pädophilen bei Betrachtung von Bildern von Kindern nach Verarbeitung im visuellen Cortex das Belohnungszentrum aktiviert wird. [17] Dieser Vorgang gilt als typisches Muster der Pädophilie und kann zur Prävention eingesetzt werden, indem potenzielle Pädophile mit einer Untersuchung darauf aufmerksam gemacht werden und therapiert werden können, bevor es überhaupt zu einer sexuellen Annäherung kommt. Es wird allerdings vermutet,

dass weit mehr Personen pädophil sind, als man es in offiziellen Statistiken liest: Circa 1 Prozent der erwachsenen Männer sollen pädophil veranlagt sein. [17] Obwohl sich viele Betroffene mit pädophilen Veranlagungen freiwillig therapieren lassen, gibt es eine große Zahl unentdeckter Täter. „Nach einer Studie der Universität Regensburg geben rund 730.000 Erwachsene zu, Onlinekontakte mit sexuellen Motiven zu Kindern unter 14 Jahren zu haben. 'Rechnet man konservativ mit zwei bis fünf Kontakten pro Täter, reden wir über weit mehr als drei Millionen betroffene Kinder und Jugendliche', sagt die Psychologin Julia von Weiler vom Verein Innocence in Danger."[Auszug aus der Studie zur digitalen Mediennutzung in Familien vom Deutschen Kinderhilfswerk] [16] Da viele der Fälle als Dunkelziffer nicht an die Behörden gelangen, ist das tatsächliche Ausmaß des kriminellen Verhaltens im Internet ungewiss.

Den größten Teil der kinderpornographischen Inhalte im Internet machen Bilder aus. Diese werden oft über Foren, Linklisten oder Bildergalerien in pädophilen Kreisen geteilt. [21] Ein Profil einer solchen Seite hat oft mehrere tausend Bilder, die durch Web-Crawling[5] gesammelt wurden. Solche Sammlungen zu finden ist Ziel von Sonderermittlungen, bei denen Ermittler des Bundeskriminalamts und der Landeskriminalämter Webseiten nach kinder- und jugendpornographischen Inhalten durchsuchen und zur Anzeige bringen. [18] Oft werden die Behörden von ausländischen Stellen kontaktiert, die entweder selbst Inhalte hosten oder Social Media Platformen betreiben und bei Scans ihrer Inhalte auf bekanntes oder neues Material stoßen und diese Informationen an die zuständigen Strafverfolgungsbehörden weiterleiten. [19] Unterstützt wird die Polizei dabei von öffentlichen Meldestellen wie `netzverweis.de` [20], die einfache Möglichkeiten bieten, verdächtige Webseiten und Inhalte schnell und einfach zu melden.

Auch wenn ein strafrechtlich relevantes Bild klar identifiziert werden kann, ist das Verbrechen nicht immer verfolgbar. Wenn die Hosting-Server in anderen Ländern stehen, was in 84 % der Fälle zutrifft, ist nicht immer die deutsche Rechtssprechung zuständig und die Inhalte können nicht gelöscht und gemeldet werden. Nur in 16 % der Fälle werden die Inhalte auf deutschen Servern gespeichert und können somit ohne weiteres in Deutschland verfolgt werden. [21] Sollte der Täter über ein so genanntes Onion-Routing[6] verfügen, kann die Identität nicht festgestellt werden und er kann nicht

[5] Web-Crawler: Programm, das über verlinkte URLs automatisch das Internet durchsucht und Webseiten analysiert

[6] Routing-Verfahren, bei dem die Verbindung über mehrere Schichten von Routern gesendet wird, wobei jeder Router nur die Adresse des vorhergehenden und nachfolgenden Knotenpunkts kennt. So kann eine IP sich innerhalb der Übertragung mehrfach ändern. Da nicht alle Router zusammenarbeiten,

verfolgt werden. Die Bilder können zwar kurzfristig entfernt werden, aber kursieren potenziell vielfach in anderen Netzwerken weiter.

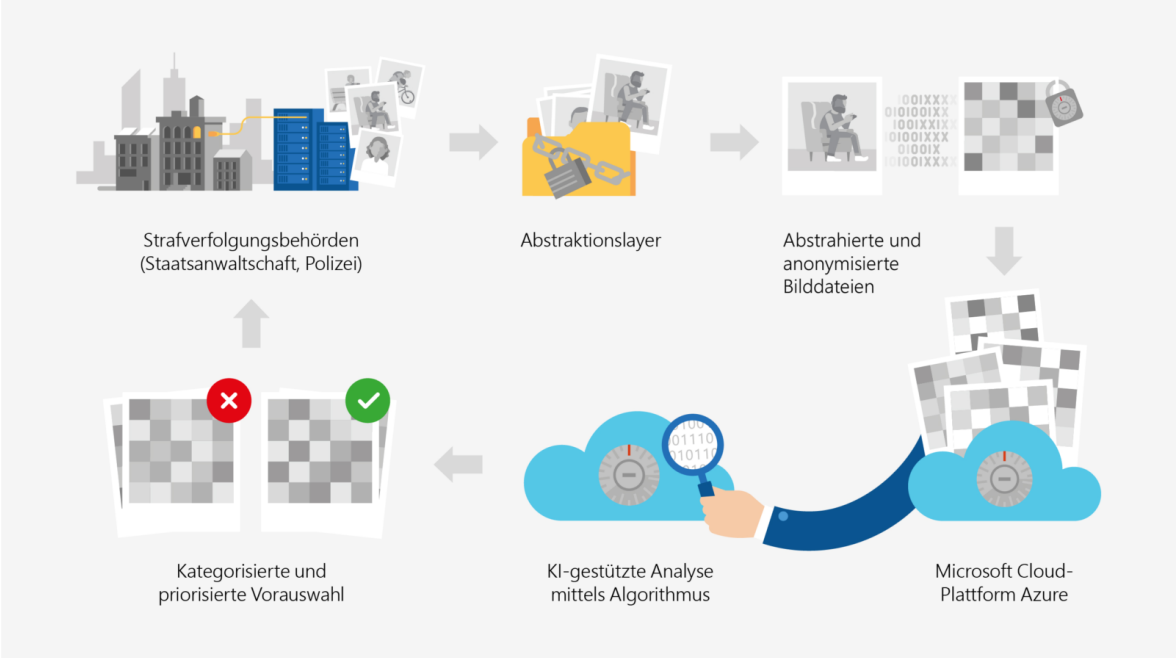
Lösungsansätze gegen Kinder- und Jugendpornographie

Trotz der Bemühungen in der Verfolgung von Kinder- und Jugendpornographie ist es nicht immer möglich, Täter eindeutig zu identifizieren oder bei Bildern zwischen normalen Fotos und Posing zu unterscheiden. Hier besteht eine Grauzone, was genau als sexuelle Pose definiert wird. Um solche Entscheidungen zu treffen, bedarf es Teams geschulter Polizeibeamter, die Bildersammlungen danach einschätzen müssen, was als strafrechtlich relevanter Inhalt zur Anzeige und Strafverfolgung gebracht werden kann. Diese Untersuchungen bedeuten großen psychischen Stress für die Beamten, da sie sich mit einer großen Zahl von Darstellungen des Kindesmissbrauchs auseinandersetzen müssen. Um sowohl die Suche nach illegalen Inhalten zu skalieren, als auch die Belastung auf die Beamten zu reduzieren, wurde durch eine Pressemitteilung am 5.8.2019 ein gemeinsames Projekt von Microsoft und dem Land NRW vorgestellt, das mittels KI-Algorithmen solche Inhalte analysieren kann.

4.1 Microsofts KI gegen Kinderpornographie

Die neue Lösung von Microsoft in Kooperation mit dem Land NRW verbindet Technologien des Cloud Computing mit KI (neuronale Netze), um strafrechtlich relevante Inhalte zuerst zu anonymisieren und zu dekonstruieren, um sie dann in einer Cloud zu analysieren und in einer kategorisierten und prioritisierten Vorauswahl an die Strafverfolgungsbehörden weiterzuleiten. [22]
Durch eine Abstraktionsschicht werden Bilder auf wenige Pixel herunter reduziert, dadurch anonymisiert und sind nicht mehr auf einen ursprünglichen Inhalt zurückzuführen. Diese minimalen Bilder können an die Azure Cloud weitergeleitet werden, wo durch Algorithmen erkannt wird, ob es sich um strafrechtlich relevantes Material handelt. „[...] [So] sind die im Rahmen des Projektes entwickelten Algorithmen von Microsoft in der Lage, in den dekonstruierten Bilddateien Inhalte zu erkennen. Am Ende entscheiden menschliche Experten zunächst basierend auf dieser Vorauswahl, ob tatsächlich strafrechtlich relevantes Bildmaterial vorliegt, und sichern diese Dateien als gerichtsfestes Beweismaterial.“ [22]

kann man von außen nicht mehr nachvollziehen, wer hinter der Verbindung steckt.



Quelle: https://news.microsoft.com/de-de/ki-im-einsatz-gegen-kinderpornografie/

Die Abstraktion der Bilder ist nötig, da es sonst zu Problemen mit Rechtsvorschriften kommen kann, nach denen kinderpornographische Inhalte nicht an Dritte weitergeleitet werden dürften. Durch die Reduzierung auf wenige Pixel sind die übertragenen Daten frei von Inhalt und können ohne Risiko an die Cloud weitergegeben werden.
Das System wirkt vielversprechend, befindet sich aber noch im Training. Die Algorithmen, die die abstrahierten Grafiken analysieren und eine Vorauswahl treffen, werden noch über Referenzbilder in ihrer Genauigkeit verbessert. Nachdem die relevanten Bilder an die Behörden gemeldet wurden, müssen die Inhalte noch von Beamten gesichtet werden, um eine letzte Auswahl zu treffen. Demnach ist eine vollautomatisierte Lösung noch nicht in Sicht, dieses Projekt bildet aber einen großen Schritt in die richtige Richtung.

4.2 Project Arachnid

Project Arachnid ist ein Web-Crawler des Canadian Centre for Child Protection, der auf `Cybertip.ca` verlinkte Seiten durchsucht und dort nach strafrechtlich relevanten Inhalten sucht. Wenn das Programm einen solchen Inhalt findet, wird eine Meldung an den Provider geschickt, damit der Inhalt so schnell wie möglich gesperrt und die Information an Behörden weitergeleitet werden kann. Inhalte werden mit Hashes[7] von bereits bekannten illegalen Inhalten abgeglichen und können so schnell erkannt werden. [23]

[7]Hash: Berechneter Wert, der aus den Details einer Datei eine einzige Zeichenfolge erstellt, von der aus nicht mehr auf den eigentlichen Inhalt geschlossen werden kann.

4.3 Netzwerke gegen Ausbeutung und Meldestellen

Arbeit für den Kinder- und Jugendschutz leisten die Meldestellen und Netzwerke wie „Keine Grauzonen im Netz“, die sich aus verschiedenen Verbänden wie eco, FSM e.V. oder jugendschutz.net zusammenstellen. Sie bieten Informationen, Aktionstage und Meldeportale sowie Hotlines, um eine schnelle Kontaktaufnahme für Betroffene und zur allgemeinen Meldung von relevanten Inhalten zu bieten. Durch einfach aufgebaute Webseiten wie jugendschutz.net werden Eltern und Kindern Ressourcen geboten, wie mit kindesgefährdenden Situationen umgegangen werden kann. [24]

5 Fazit

Besonders in den letzten Jahren hat sich die Technologie in großen Sprüngen weiterentwickelt und bietet dadurch immer neue Wege der Kommunikation. Gleichzeitig bieten sich aber auch neue Wege, diese Kommunikation auszunutzen und anonymisiert Straftaten zu begehen. Wege zur Bekämpfung dieser Straftaten, oft gestützt durch neue KI-Konzepte, werden erst nach und nach ergründet. Um die schleichenden Gefahren für Kinder und Jugendliche gering zu halten, ist es nötig, dass sich Eltern und Lehrer informieren und ihr Wissen an die nächsten Generationen weitergeben. Trotz der möglichen Risiken muss man Kindern die Möglichkeit bieten, die digitale Welt für sich selbst zu entdecken und mitzugestalten. Eine zu starke Kontrolle kann sonst zur Entfremdung zwischen Eltern und Kind führen.

Literatur

[1] Taylor, Kyle und Silver, Laura: Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally. 05.02.2019, Abgerufen am 09.07.2019, von https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

[2] Landolt, Claudia: Kinderfotos im Netz – wie man sie sicherer teilt. 09.11.2017, Abgerufen am 11.08.2019, von https://www.fritzundfraenzi.ch/medien/mediennutzung/kinderfotos-im-netz-wie-man-sie-sicherer-teilt

[3] § 1.1 JuSchG. Abgerufen am 12.07.2019, von https://www.gesetze-im-internet.de/juschg/BJNR273000002.html

[4] § 176 StGB. Abgerufen am 12.07.2019, von https://www.gesetze-im-internet.de/stgb/__176.html

[5] § 182 StGB. Abgerufen am 12.07.2019, von https://www.gesetze-im-internet.de/stgb/__182.html

[6] § 184b StGB. Abgerufen am 12.07.2019, von https://www.gesetze-im-internet.de/stgb/__184b.html

[7] § 184c StGB. Abgerufen am 12.07.2019, von https://www.gesetze-im-internet.de/stgb/__184c.html

[8] Duignan, Brian: Gaslighting. 03. Oktober 2017, Abgerufen am 08.07.2019, von https://www.britannica.com/topic/gaslighting

[9] Wiktionary: Cybersex. Abgerufen am 08.07.2019, von https://de.wiktionary.org/wiki/Cybersex

[10] Samsel, Michael: Grooming. Abgerufen am 08.07.2019, von https://www.abuseandrelationships.org/Content/Behaviors/grooming.html

[11] Bitkom Research: Mit 10 Jahren haben die meisten Kinder ein eigenes Smartphone. 28.05.2019, Abgerufen am 14.08.2019, von https://www.bitkom.org/Presse/Presseinformation/Mit-10-Jahren-haben-die-meisten-Kinder-ein-eigenes-Smartphone

[12] Demling, Alexander und Hua, Sha: TikTok - Wie eine chinesische App deutsche Jugendliche und Werber begeistert. 27.02.2019, Abgerufen am 12.08.2019, von https://www.handelsblatt.com/unternehmen/it-medien/tiktok-wie-eine-chinesische-app-deutsche-jugendliche-und-werber-begeistert/24035480.html?ticket=ST-188846-7FAz1NcxffFvfQOKuRx4-ap4

[13] Fuest, Benedikt: Ü13-Regel für TikTok manövriert die Eltern in ein neues Dilemma. 01.03.2019, Abgerufen am 12.08.2019, von https://www.welt.de/wirtschaft/webwelt/article189584913/TikTok-Jetzt-bekommen-Eltern-ein-Problem.html

[14] Matthes, Marie-Charlotte: Sharing is Caring? Kinderfotos im Netz verletzen die Persönlichkeitsrechte der Kinder. 27.11.2018, Abgerufen am 12.08.2019, von https://netzpolitik.org/2018/sharing-is-caring-kinderfotos-im-netz-verletzen-die-persoenlichkeitsrechte-der-kinder/

[15] Deutsches Kinderhilfswerk: Studie zur digitalen Mediennutzung in Familien. Abgerufen am 12.08.2019, von https://www.dkhw.de/schwerpunkte/medienkompetenz/studie-kinderbilderrechte/

[16] BR Fernsehen: Gepostet, geklaut, missbraucht. 27.02.2019, Abgerufen am 12.08.2019, von https://www.br.de/mediathek/video/kinderfotos-im-netz-doku-gepostet-geklaut-missbraucht-av:5c3f13601cc4200018f062aa

[17] Wellhöner, Jens: MRT kann Pädophilie erkennen. 26.02.2012, Abgerufen am 12.08.2019, von https://www.deutschlandfunkkultur.de/mrt-kann-paedophilie-erkennen.1067.de.html?dram:article_id=175786

[18] Bruns, Henrik: Den Missbrauch „ausblenden“. 13.03.2015, Abgerufen am 12.08.2019, von http://www2.weserreporter.de/artikelid5368_den-missbrauch-quotausblendenquot.html

[19] Bundeskriminalamt: Kurzclips zum Thema Auswertung und Ermittlungen im Bereich Kinderpornografie, Abgerufen am 14.08.2019, von https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Kinderpornografie/Kurzclips/kurzclips_node.html

[20] Netzverweis, Meldestellte für Internetkriminalität. Abgerufen am 12.08.2019, von https://www.netzverweis.de/Meldestelle/

[21] Bericht der Bundesregierung über die im Jahr 2017 ergriffenen Maßnahmen zum Zweck der Löschung von Telemedienangeboten mit kinderpornografischem Inhalt im Sinne des § 184b des Strafgesetzbuchs. September 2018, Abgerufen am 12.08.2019, von https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Statistiken/Download/Bericht_Loeschen_statt_sperren_2017.pdf?__blob=publicationFile&v=1

[22] Richter, Isabel: Automatische Bilderkennung hilft im Einsatz gegen Kinderpornografie. 05.08.2019, Abgerufen am 12.08.2019, von https://news.microsoft.com/de-de/ki-im-einsatz-gegen-kinderpornografie/

[23] Project Arachnid. Abgerufen am 12.08.2019, von https://projectarachnid.ca/en/

[24] Keine Grauzonen im Netz. Netzwerk gegen sexuelle Ausbeutung von Kindern im Internet, Abgerufen am 12.08.2019, von https://www.jugendschutz.net/sexuelle-ausbeutung/keine-grauzonen-im-netz/

[25] Wikipedia-Eintrag über Knuddels.de, Abgerufen am 12.08.2019, von https://de.wikipedia.org/wiki/Knuddels

[26] Köble, Miriam: Knuddels, ein Paradies für Pädophile? – Die Chatplattform im Interview. 23.05.2019, Abgerufen am 12.08.2019, von https://www.medienbewusst.de/internet/20130523/knuddels-ein-paradies-fur-padophile-die-chatplattform-im-interview.html

[27] Privatlino-KI. KI zur Analyse von Online-Kommunikation, um toxische Inhalte herauszufiltern. Abgerufen am 12.08.2019, http://www.kitext.de/

[28] WhatsSafe. Dienst zum Überwachen von WhatsApp. Abgerufen am 12.08.2019, https://www.whatssafe.de/

[29] Pruefziffernberechnung Deutscher Personalausweis. Abgerufen am 12.08.2019, von http://www.pruefziffernberechnung.de/P/Personalausweis-DE.shtml

[30] Kein Raum für Missbrauch. Website des Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs, Abgerufen am 12.08.2019, von https://www.kein-raum-fuer-missbrauch.de/