

Faktenblatt zur Plattform Take It Down

Versenden von sexuell explizitem Material und dessen Konsequenzen

Das Versenden von persönlichen Bildern oder Videos mit sexuellem oder intimmem Inhalt über elektronische Medien, das sogenannte Sexting¹, kann verschiedene Folgen haben, je nach Modus Operandi:

- Rachepornografie²: Die Person gibt das Bild oder das Video, das ihr anvertraut wurde, an Dritte ohne die Einwilligung der betroffenen Person weiter oder veröffentlicht es online.
- Sextortion³: Die Person nutzt das Bild oder das Video, das ihr anvertraut wurde, um die betroffene Person zu erpressen.
- Grooming⁴: Die Person nutzt das Bild oder das Video, das ihr anvertraut wurde, um die betroffene Person zu nötigen, ihr mehr intime Fotos und Videos zu senden.

Obwohl Sexting seit dem Inkrafttreten des neuen Sexualstrafrechts am 1. Juli 2024 unter bestimmten Bedingungen nicht mehr strafbar ist, ist neu **Rachepornographie** strafbar. Ebenso sind sowohl die **Erpressung** (Sextortion, siehe oben) mit bereits bestehendem explizitem Material als auch die **Nötigung** (Grooming, siehe oben) strafbar.

Unabhängig von der Strafbarkeit führt der Missbrauch von Sexting oft zu schwerwiegenden emotionalen, sozialen und beruflichen Konsequenzen für die Opfer. Für sie bedeutet dies nicht nur, dass ihr Vertrauen missbraucht wurde, sondern auch, dass sie damit leben müssen, die Kontrolle über ihr Bild oder ihr Video im Internet verloren zu haben und diese missbraucht werden können.

Ausmass und Verbreitung

Laut der JAMES-Studie 2022⁵ (Befragung von 12-19-Jährigen) betrifft diese Praxis Jugendliche folgendermassen:

- Pornografie und Erotik: Etwa zwei Fünftel der Jugendlichen haben schon einmal erotische Fotos oder Videos von anderen erhalten. Deutlich weniger Jugendliche (ca. 12%) geben an, schon selbst erstelltes erotisches Foto- oder Videomaterial verschickt zu haben: 1% in der Altersgruppe 12-13, 6% in der Altersgruppe 14-15 und 18% in der Altersgruppe 16-17.
- Cybermobbing und sexuelle Belästigung im Internet: Genau ein Drittel der Jugendlichen wurde schon mindestens einmal von einer fremden Person aufgefordert, erotische Fotos von sich selbst zu verschicken.

Neue und erste (sexuelle) Erfahrungen zu machen, aber auch Grenzen zu überschreiten gehört zum Leben junger Menschen. Am sichersten wäre es, keine kompromittierenden oder nackten Fotos oder

¹ <https://www.skppsc.ch/de/themen/sexuelle-gewalt/illegale-pornografie-pornosucht/>

² <https://www.skppsc.ch/de/themen/sexuelle-gewalt/illegale-pornografie-pornosucht/>

³ <https://www.skppsc.ch/de/themen/internet/sextortion-erpressung/>

⁴ <https://www.skppsc.ch/de/themen/sexuelle-gewalt/sexuelle-gewalt-kindern/>

⁵ https://www.zhaw.ch/storage/psychologie/upload/forschung/medienpsychologie/james/2018/Bericht_JAMES_2022_de.pdf

Videos an andere zu verschicken. Aber Jugendliche tun es dennoch. Wenn man jemandem ein nacktes Bild oder Video schickt, der es dann irgendwo online veröffentlicht oder damit nötigt oder erpresst, welche Möglichkeiten gibt es dann, die Folgen zu minimieren oder gar die Kontrolle zurückzugewinnen?

Was kann man tun?

Bevor es passiert: Um die Risiken zu minimieren bzw. die negativen Konsequenzen im Zusammenhang mit Sexting zu verhindern, empfehlen wir Jugendlichen:

- möglichst darauf verzichten, erotische Bilder oder Videos einer anderen Person zu versenden;
- nur online teilen, was sie auch offline mit Fremden teilen würden und
- auf Social Media sowie beim gemeinsamen Chatten, Gamen und Streamen aufzupassen: echte Freundschaften können auch online entstehen, jedoch weiss man nie, wer sich hinter einem Profil verbirgt.

Wenn das gesendete Material missbraucht wurde, also wenn man jemandem ein intimes Bild oder Video trotzdem schickt, der es dann ohne Einwilligung online veröffentlicht oder damit nötigt oder erpresst, empfehlen wir:

- nicht allein zu bleiben und mit einer erwachsenen Vertrauensperson aus der Familie oder der Schule darüber zu sprechen.
- sich bei Unsicherheiten oder Fragen bei der Schweizerischen Kriminal Prävention⁶ oder bei der Meldestelle clickandstop.ch⁷ zu melden.
- Anzeige bei der Polizei zu erstatten und
- technische Massnahme zu verwenden, um die Verbreitung von Bildern oder Videos zu verhindern bzw. zu minimieren, wie die Plattform Take It Down⁸ von NCMEC⁹ (siehe unten).

NCMEC und Take It Down

Das **National Center for Missing & Exploited Children** (NCMEC) ist eine private, amerikanische Non-Profit-Organisation. Ihr Ziel ist es, die sexuelle Ausbeutung von Kindern zu verringern und die Viktimisierung von Kindern zu verhindern. NCMEC überwacht das Internet aktiv auf Kinderpornografie und meldet den zuständigen Behörden jedes kinderpornografische Video oder Bild, das es findet. In der Schweiz meldet NCMEC illegale Aktivitäten über fedpol den Strafverfolgungsbehörden.

Mit dem neuen kostenlosen und anonymen Dienst **Take It Down** bietet nun NCMEC Kindern und Jugendlichen die Möglichkeit, nackte, teilweise nackte, oder sexuell eindeutige Bilder oder Videos, die von ihnen aufgenommen wurden als sie unter 18 Jahre alt waren, zu melden und auf den grössten öffentlichen oder unverschlüsselten Plattformen zu suchen. Das Ziel ist die Weiterverbreitung dieser

⁶ <https://www.skppsc.ch/fr/contact/>

⁷ www.clickandstop.ch/de

⁸ <https://takeitdown.ncmec.org/de/>

⁹ <https://www.missingkids.org/home>

Bilder über die Plattformen verhindern zu können. Die Dienstleistung kann auch genutzt werden, wenn man nicht sicher ist, ob ein Bild oder ein Video missbräuchlich verbreitet wurde.

Wie funktioniert Take It Down¹⁰? Hier ein Beispiel: Jemand nötigt oder erpresst einen Jugendlichen mit einem Nacktbild von ihm oder das Bild wird ohne seine Einwilligung online veröffentlicht. Wenn er dies bei Take It Down melden möchte, muss er nicht das Bild hochladen und schicken, sondern es wird nur der eindeutige digitale Fingerabdruck, der so genannte Hashwert der Datei, generiert und zu einer Liste hinzugefügt, die bei NCMEC gespeichert wird. Niemand sieht also die Inhalte auf den Bildern oder Videos. Die am Take It Down-Dienst teilnehmenden Online-Plattformen¹¹ haben Zugang zu dieser Liste und können einen Abgleich zu den Hashwerten der Bilder und Videos auf deren Online-Plattformen machen. Die Plattform-Betreiber können bei einem Treffer entsprechende Massnahmen einleiten, um deren Verbreitung einzuschränken oder ganz zu verhindern, d.h. das Material löschen und gegebenenfalls NCMEC melden. Beim Erhalt der weitergeleiteten Daten meldet es NCMEC an fedpol, wenn das entsprechende Bild von einem Schweizer Server aus online gestellt wurde. fedpol übernimmt dann die weitere Bearbeitung des Falls beim Prüfen die eingehende Meldung auf einen Tatverdacht nach Schweizer Gesetz und leitet sie gegebenenfalls an die zuständigen kantonalen Strafverfolgungsbehörden.

Die Schweizerische Kriminalprävention (SKP) hat eine schweizerische Firma beauftragt, in Form eines **technischen Gutachtens** zu überprüfen, ob wirklich nur der Hashwert übertragen wird und nicht das Bild bzw. das Video, das auf dem Gerät des Nutzers verbleibt. Die Firma sagt aus: «Die Sicherheitsüberprüfung ergab keine kritischen oder hoch bewerteten Probleme, die die Vertraulichkeit oder Integrität der ausgetauschten Informationen beeinträchtigen würden. Es wurde auch festgestellt, dass keine Dateien über das Netzwerk übertragen werden, was bedeutet, dass alle Dateien nur lokal verarbeitet werden.»¹².

Zusätzlich wurde der Dienst von einer Staatsanwältin auf den **rechtlichen Aspekt** hin beurteilt: «Rechtlich wird (derzeit) nur der Hashwert übermittelt, weshalb hier keine strafrechtlichen Bestimmungen (Pornografie etc.) einschlägig sind gemäss meiner Einschätzung. Offenbar weist das Firma daraufhin, dass die Lage sich theoretisch auch ändern könnte (wofür ich keinen Anlass sehe), dann müsste das entsprechend neu beurteilt werden. »

¹⁰ [FAQ - Take It Down \(takeitdown.ncmec.org\)](https://www.takeitdown.ncmec.org)

¹¹ Stand Oktober 2024: Clips4Sale, Facebook, Instagram, OnlyFans, Pornhub, TikTok, Yubo, Snap Inc., Threads und RedGIFs.

¹² Auf Englisch im Text: *The security review revealed no critical or high-rated issues that would compromise the confidentiality or integrity of exchanged information. It has also revealed that no files are transferred through the network, meaning that all files are only processed locally.*