HOCHSCHULE MITTWEIDA
University of Applied Sciences

Rechtsgrundlagen Cybercrime

Bundeskriminalamt

Prof. Dr. Dirk Labudde

Kinderpornographie konsequent bekämpfen

Beschluss

des Bundesfachausschusses Innere Sicherheit

vom 9. Dezember 2019

Dezember 2019

Wer schweigt, soll bestraft werden

Presse

https://www.sueddeutsche.de/politik/kindesmissbrauch-kinderpornografie-cdu-bundesfachausschuss-1.4722694

Wie Statistiken belegen, nehmen Fälle von sexueller Gewalt und Missbrauch von Kindern sowie die Verbreitung von Kinderpornographie weiter zu, erfolgen dabei weltweit und durchziehen alle Gesellschaftsschichten. Bei diesen Taten tun sich wahre Abgründe unserer Gesellschaft auf. Diese Verbrechen an Schutzbefohlenen sind an Abscheu nicht zu überbieten. Laut der Polizeilichen Kriminalstatistik wurden 2018 136 Kinder in Deutschland gewaltsam getötet. Bei Taten der sexuellen Gewalt wurden 14 606 Kinder als Opfer registriert. Die erfassten Fallzahlen des Besitzes und der Verbreitung kinderpornografischen Materials stiegen im Vergleich zum Jahr 2017 um 14 Prozent auf 7 449 Fälle. Allein im Jahr 2018 erhielt das Bundeskriminalamt rund 70 000 Hinweise auf Verdachtsfälle zu Dateien mit kinderpornographischen Inhalten von der US-amerikanischen Nichtregierungsorganisation National Center for Missing and Exploited Children (NCMEC). Das bedeutet im Vergleich zu 2017 eine Verdopplung der Hinweise auf Kinderpornographie bzw. Missbrauchsabbildungen mit Bezügen nach Deutschland. Diese beinhalten reale Missbrauchshandlungen an Kindern, die zum Zeitpunkt der Verdachtsmeldung ggf. noch weiter andauern. Das bedeutet, dass betroffene Kinder sich in akuten Gefahrensituationen befinden.

Es ist dafür Sorge zu tragen, dass von Missbrauch betroffene Kinder und Jugendliche sowie deren Erziehungsberechtigte niederschwellig Informationen und Hilfestellungen erhalten, um insbesondere Verdachtsfällen frühzeitig nachgehen zu können. Verbrechensserien können so eher unterbunden werden. Wir wollen die Nichtanzeige eines geplanten sexuellen Missbrauchs unter Strafe stellen und plädieren daher für eine Aufnahme dieser Straftaten in den Katalog des § 138 StGB, damit geplante Taten abgewendet werden können.

Wir wollen, dass deutsche Internet Service Provider gesetzlich verpflichtet werden, Verdachtsfälle auf Kinder- und Jugendpornographie an eine zentrale Stelle, z. B. beim Bundeskriminalamt, zu melden (Meldepflicht für Diensteanbieter). Deutsche Ermittler bekommen Hinweise auf Kinderpornographie häufig aus den USA. Dort gibt es für Provider bereits eine gesetzliche Pflicht, Verdachtsfälle auf Kinder- und Jugendpornographie zu melden. Die finanziellen Zuweisungen der Länder für die personelle Ausstattung sowie Qualifizierung durch Fortbildung und Supervision der Mitarbeiter in den Jugendämtern und Institutionen müssen zur Prävention wegen der Zunahme von Gewalt und sexuellem Missbrauch von Kindern und Jugendlichen deutlich erhöht werden. Eine reflektierte und besonnene Haltung und Fachlichkeit sind bei den beteiligten Akteuren erforderlich. Für

§ 138
Nichtanzeige geplanter Straftaten

(1) Wer von dem Vorhaben oder der Ausführung

1. *(weggefallen)*
2. eines Hochverrats in den Fällen der §§ 81 bis 83 Abs. 1,
3. eines Landesverrats oder einer Gefährdung der äußeren Sicherheit in den Fällen der §§ 94 bis 96, 97a oder 100,
4. einer Geld- oder Wertpapierfälschung in den Fällen der §§ 146, 151, 152 oder einer Fälschung von Zahlungskarten mit Garantiefunktion in den Fällen des § 152b Abs. 1 bis 3,
5. eines Mordes (§ 211) oder Totschlags (§ 212) oder eines Völkermordes (§ 6 des Völkerstrafgesetzbuches) oder eines Verbrechens gegen die Menschlichkeit (§ 7 des Völkerstrafgesetzbuches) oder eines Kriegsverbrechens (§§ 8, 9, 10, 11 oder 12 des Völkerstrafgesetzbuches) oder eines Verbrechens der Aggression (§ 13 des Völkerstrafgesetzbuches),
6. einer Straftat gegen die persönliche Freiheit in den Fällen des § 232 Absatz 3 Satz 2, des § 232a Absatz 3, 4 oder 5, des § 232b Absatz 3 oder 4, des § 233a Absatz 3 oder 4, jeweils soweit es sich um Verbrechen handelt, der §§ 234, 234a, 239a oder 239b,
7. eines Raubes oder einer räuberischen Erpressung (§§ 249 bis 251 oder 255) oder
8. einer gemeingefährlichen Straftat in den Fällen der §§ 306 bis 306c oder 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 4, des § 309 Abs. 1 bis 5, der §§ 310, 313, 314 oder 315 Abs. 3, des § 315b Abs. 3 oder der §§ 316a oder 316c

zu einer Zeit, zu der die Ausführung oder der Erfolg noch abgewendet werden kann, glaubhaft erfährt und es unterläßt, der Behörde oder dem Bedrohten rechtzeitig Anzeige zu machen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 184 b StGB

Strafgesetzbuch

§ 138
Nichtanzeige geplanter Straftaten

§ 184 b StGB

(2) [1]Ebenso wird bestraft, wer

1. von der Ausführung einer Straftat nach § 89a oder
2. von dem Vorhaben oder der Ausführung einer Straftat nach § 129a, auch in Verbindung mit § 129b Abs. 1 Satz 1 und 2,

zu einer Zeit, zu der die Ausführung noch abgewendet werden kann, glaubhaft erfährt und es unterlässt, der Behörde unverzüglich Anzeige zu erstatten. [2]§ 129b Abs. 1 Satz 3 bis 5 gilt im Fall der Nummer 2 entsprechend.

(3) Wer die Anzeige leichtfertig unterläßt, obwohl er von dem Vorhaben oder der Ausführung der rechtswidrigen Tat glaubhaft erfahren hat, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Strafgesetzbuch

Wäre dies sinnvoll gewesen?

In Schlagzeilen

Je tiefer die Ermittler graben, desto größer wird das Entsetzen: über das, was Kindern auf einem Campingplatz in Lügde widerfuhr – und über das Versagen der Behörden.

Ein Beispiel in Schlagzeilen

- **drei Hauptverdächtige**
- **Mehr als 1.000 Taten**

  mehr als 1.000 einzelne Taten und **41 Opfern**
- **Daten im Umfang von 14 Terabyte**

  13.000 kinderpornografische Dateien

  10 Computer 9 Handys

  40 Festplatten und mehr als 400 weitere Datenträger

  3,3 Millionen sichergestellte Fotos und mehr als 86.000 Videos
- **Wahrscheinlich mehr Opfer**

Phänomen

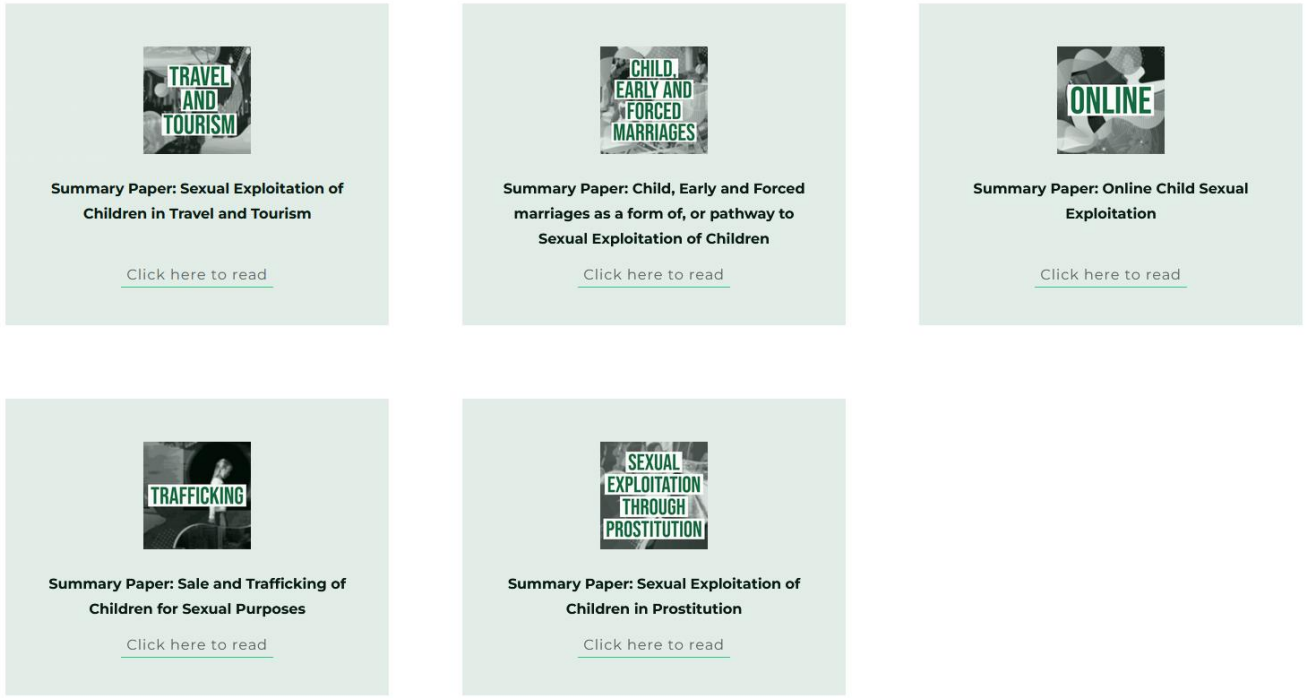
Opfer von sexuellem Kindesmissbrauch leiden unter physischen, psychischen und emotionalen Traumata.

Die **Erkennung** und Löschung von illegalem Online-Material über sexuellen Kindesmissbrauch (CSAM) hilft dabei, die **ständige erneute Viktimisierung** von Kindern zu reduzieren und sogar zu stoppen.

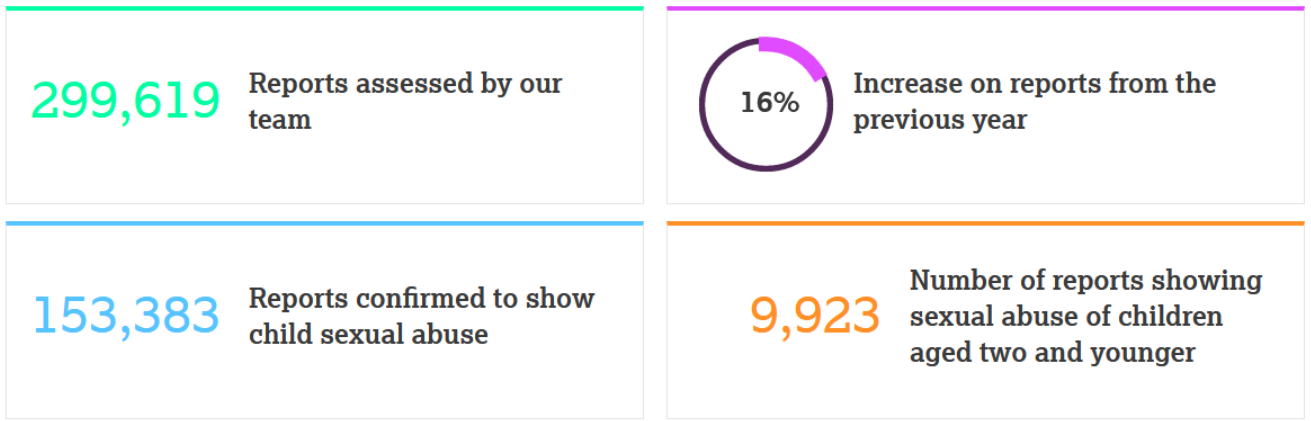
Child Sexual Abuse Material or virtual *child* pornography

Initiativen und Zahlen

https://ecpat.org/search-our-library/



The IWF in 2020



https://www.iwf.org.uk/

https://www.inhope.org/EN?locale=de

IWF

Im Jahr 2020 bestätigte die IWF **68.000 Fälle von selbst erstelltem Bildmaterial**. Dies macht nun **fast die Hälfte (44 %)** des Bildmaterials aus, gegen das die IWF im vergangenen Jahr vorgegangen ist (IWF-Analysten bestätigten insgesamt 153.350 Berichte über Material über sexuellen Kindesmissbrauch).

https://www.iwf.org.uk/about-us/who-we-are/annual-report/

CSAM

Einflussfaktoren:

- aktuellen Forschungsergebnisse
- Technischer Fortschritt
- Herausforderungen CSAM-Erkennung
- Dimensionen der politischen und rechtlichen Rahmenbedingungen,
- der Distributionskanäle
- Erkennungsanwendungen und -implementierungen

Es wurde gezeigt, dass Deep Learning-Techniken andere Erkennungsmethoden für unbekannte CSAM übertreffen.

Mobile Geräte

Mit dem allgemeinen Anstieg der Nutzung mobiler Geräte über die Jahre hinweg, stieg auch der **CSAM-Konsum über mobile Geräte**.

- Tablets und Smartphones 32 % aller mit CSAM verbundenen Suchanfragen

Digitalkameras, Mobiltelefone, Tablets oder Laptops - Produktion von CSAM

- mehr Amateurinhalte produziert

Soziale Medien

- Das Aufkommen sozialer Medien und ihre weit verbreitete Nutzung schaffen neue Plattformen für CSAM.

- **E-Mail**, CSAM hochladen

Wissensgenerierung

Wissensgenerierung (Aufdeckung und Zusammenfassung)

- Bild-Hash-Datenbanken, Foto DNA
- Schlüsselwörter
- Web-Crawler (Einstiegsseiten)
- Erkennung auf Basis von Namen und Metadaten
- visuelle Erkennung

Ergebnisse deuten darauf hin, dass CSAM-Erkennungsanwendungen die besten Ergebnisse liefern, wenn **mehrere Ansätze in Kombination** verwendet werden.

§ 184
Verbreitung pornographischer Inhalte

(1) Wer einen pornographischen Inhalt (§ 11 Absatz 3)

1. einer Person unter achtzehn Jahren anbietet, überläßt oder zugänglich macht,
2. an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, zugänglich macht,
3. im Einzelhandel außerhalb von Geschäftsräumen, in Kiosken oder anderen Verkaufsstellen, die der Kunde nicht zu betreten pflegt, im Versandhandel oder in gewerblichen Leihbüchereien oder Lesezirkeln einem anderen anbietet oder überläßt,

3a. im Wege gewerblicher Vermietung oder vergleichbarer gewerblicher Gewährung des Gebrauchs, ausgenommen in Ladengeschäften, die Personen unter achtzehn Jahren nicht zugänglich sind und von ihnen nicht eingesehen werden können, einem anderen anbietet oder überläßt,

4. im Wege des Versandhandels einzuführen unternimmt,
5. öffentlich an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, oder durch Verbreiten von Schriften außerhalb des Geschäftsverkehrs mit dem einschlägigen Handel anbietet oder bewirbt,
6. an einen anderen gelangen läßt, ohne von diesem hierzu aufgefordert zu sein,
7. in einer öffentlichen Filmvorführung gegen ein Entgelt zeigt, das ganz oder überwiegend für diese Vorführung verlangt wird,
8. herstellt, bezieht, liefert, vorrätig hält oder einzuführen unternimmt, um diesen im Sinne der Nummern 1 bis 7 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, oder

§ 184a
Verbreitung gewalt- oder tierpornographischer Inhalte

[1]Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer einen pornographischen Inhalt (§ 11 Absatz 3), der Gewalttätigkeiten oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand hat,

1. verbreitet oder der Öffentlichkeit zugänglich macht oder
2. herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diesen ein- oder auszuführen, um ihn im Sinne der Nummer 1 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen.

[2]In den Fällen des Satzes 1 Nummer 1 ist der Versuch strafbar.

§ 184b
Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte

(1) [1] Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren wird bestraft, wer

1. einen kinderpornographischen Inhalt verbreitet oder der Öffentlichkeit zugänglich macht; kinderpornographisch ist ein pornographischer Inhalt (§ 11 Absatz 3), wenn er zum Gegenstand hat:

   a) sexuelle Handlungen von, an oder vor einer Person unter vierzehn Jahren (Kind),

   b) die Wiedergabe eines ganz oder teilweise unbekleideten Kindes in aufreizend geschlechtsbetonter Körperhaltung oder

   c) die sexuell aufreizende Wiedergabe der unbekleideten Genitalien oder des unbekleideten Gesäßes eines Kindes,

2. es unternimmt, einer anderen Person einen kinderpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zugänglich zu machen oder den Besitz daran zu verschaffen,

3. einen kinderpornographischen Inhalt, der ein tatsächliches Geschehen wiedergibt, herstellt oder

4. einen kinderpornographischen Inhalt herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diesen ein- oder auszuführen, um ihn im Sinne der Nummer 1 oder der Nummer 2 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, soweit die Tat nicht nach Nummer 3 mit Strafe bedroht ist.

§ 184c
Verbreitung, Erwerb und Besitz jugendpornographischer Inhalte

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer

1. einen jugendpornographischen Inhalt verbreitet oder der Öffentlichkeit zugänglich macht; jugendpornographisch ist ein pornographischer Inhalt (§ 11 Absatz 3), wenn er zum Gegenstand hat:

   a) sexuelle Handlungen von, an oder vor einer vierzehn, aber noch nicht achtzehn Jahre alten Person,

   b) die Wiedergabe einer ganz oder teilweise unbekleideten vierzehn, aber noch nicht achtzehn Jahre alten Person in aufreizend geschlechtsbetonter Körperhaltung oder

   c) die sexuell aufreizende Wiedergabe der unbekleideten Genitalien oder des unbekleideten Gesäßes einer vierzehn, aber noch nicht achtzehn Jahre alten Person,

2. es unternimmt, einer anderen Person einen jugendpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zugänglich zu machen oder den Besitz daran zu verschaffen,

3. einen jugendpornographischen Inhalt, der ein tatsächliches Geschehen wiedergibt, herstellt oder

4. einen jugendpornographischen Inhalt herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diesen ein- oder auszuführen, um ihn im Sinne der Nummer 1 oder 2 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, soweit die Tat nicht nach Nummer 3 mit Strafe bedroht ist.

§ 184h
Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. sexuelle Handlungen
   nur solche, die im Hinblick auf das jeweils geschützte Rechtsgut von einiger Erheblichkeit sind,

2. sexuelle Handlungen vor einer anderen Person
   nur solche, die vor einer anderen Person vorgenommen werden, die den Vorgang wahrnimmt.

Cyber-Mobbing

Cyber-Mobbing, auch Cyber-Bullying genannt ist das absichtliche und über einen längeren Zeitraum anhaltende Beleidigen, Bedrohen, Bloßstellen, Belästigen, Anpöbeln, Tyrannisieren oder Ausgrenzen anderer über digitale Medien. Cyber-Mobbing findet vor allem in Sozialen Netzwerken, Chats, Messengern oder per Handy über SMS, WhatsApp, lästige Anrufe, Handyfotos und -videos statt.

Sexting **"Sexting: es kommt anders als erwartet"**

Sexting ist ursprünglich das Texten, also Schreiben, über sexuelle Themen gewesen, hat sich aber schnell vom Texten zum Senden von Bildern entwickelt. Beim Sexting machen Jugendliche, entweder freiwillig oder durch Mobbing oder Manipulation gezwungen, erotische Fotos des eigenen Körpers und versenden diese über Handys oder Webcams.

Cyber-Grooming

Grooming ist eine spezifische Art der sexuellen Belästigung. Man versteht darunter das sexuell motivierte Anschreiben von Kindern und Jugendlichen durch erwachsene, fremde Personen im Internet.

Definition

Unter Cyberbullying oder Cybermobbing versteht man die Beleidigung, Bedrohung, Bloßstellung oder Belästigung von Personen mithilfe von Kommunikationsmedien, beispielsweise über Smartphones, E-Mails, Websites, Foren, Chats und Communities.

Verschiedene Formen des Mobbing:

- diffamierende Fotos oder Filme
- Lästerei über eine bestimmte Person
- Verbreitung von Unwahrheiten unter falschen Account

Verbreitung in der Öffentlichkeit

Unterschiede Online und Offline

Eingriff rund um die Uhr in das Privatleben

Das Publikum ist unüberschaubar groß; Inhalte verbreiten sich extrem schnell

Bullies können anonym agieren

Betroffenheit des Opfers wird nicht unmittelbar wahrgenommen

Probleme:

- Schnelllebigkeit
- Anonymität & Distanz
- Übermäßiges Mitteilen persönlicher Informationen
- Freunde versus Bekannt

Gesetzeslage

§ 185 Strafgesetzbuch: Beleidigung

§ 186 Strafgesetzbuch: Üble Nachrede

§ 187 Strafgesetzbuch: Verleumdung

§ 238 Strafgesetzbuch: Nachstellung

§ 22 KUG/KunstUrhG: Recht am eigenen Bild

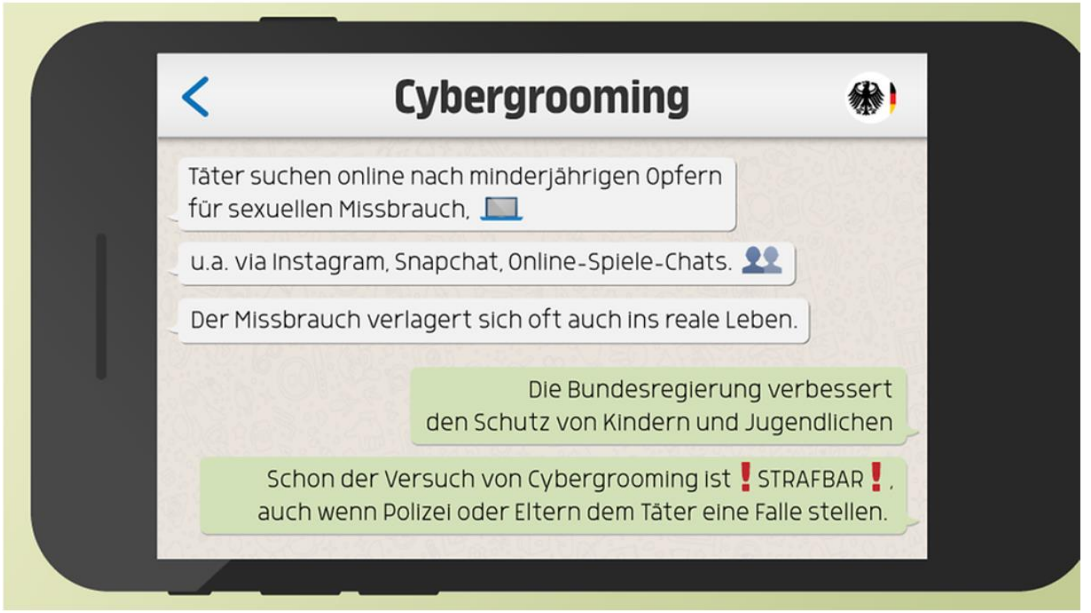
§ 201 Strafgesetzbuch: Verletzung der Vertraulichkeit des Wortes

§ 201a Strafgesetzbuch: Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

§ 240 & § 241 Strafgesetzbuch: Nötigung & Bedrohung

Cybergrooming

Cybergrooming bezeichnet die Anbahnung von sexueller Gewalt gegen Minderjährige im Internet. Das englische Wort „Grooming“ bedeutet „Striegeln“ und steht metaphorisch für das subtile Annähern von Täter:innen an Kinder und Jugendliche.



Cybergrooming

§ 176 Abs. 6 StGB

(6) **Der Versuch ist strafbar**; dies gilt nicht für Taten nach Absatz 4 Nummer 4 und Absatz 5.
Bei Taten nach Absatz 4 Nummer 3 ist der Versuch nur in den Fällen strafbar, in denen eine Vollendung der Tat allein daran scheitert, dass der Täter irrig annimmt, sein Einwirken beziehe sich auf ein Kind.

§ 176 StGB Sexueller Mißbrauch von Kindern - dejure.org

Cybergrooming

Cybergrooming ist gekennzeichnet von bestimmten Täter:innen-**Strategien**, die sich oft ähneln.

Ausnutzung

Unbedarftheit

Vertrauensseligkeit und das

mangelnde Risikobewusstsein von Kindern und Jugendlichen

Oft versuchen die Täter:innen ein **Vertrauens- oder Abhängigkeitsverhältnis** herzustellen, um ihre Opfer manipulieren und kontrollieren zu können.

Kontaktmöglichkeiten

Online-Plattformen (YouTube und Twitch, **soziale Netzwerke** wie TikTok, Instagram und Facebook**)**

Online-Spiele

Gamingplattformen (Fortnite oder Steam**)**

Kommunikationskanäle etwa (Messenger oder Videochat-Dienste)

Drei Arten von Cyber-Grooming

1. Erwachsene TäterInnen versuchen sich dem Kind in Chat-Foren für Kinder oder in sozialen Netzwerken anzunähern.
2. Manchmal geht der erste Kontakt nicht vom Erwachsenen sondern vom Kind aus.
3. **"Loverboys"** nutzen oft soziale Netzwerke, um in Kontakt mit potentiellen Opfern zu kommen. Sozialen Netzwerke bieten die Möglichkeit, zu vielen Mädchen gleichzeitg Kontakt aufzunehmen. "Loverboys" können so sehen, wie sich die Betroffenen präsentieren und an persönliche Informationen aus ihrem Privatleben (Hobbys, FreundInnen) gelangen. In sozialen Netzwerken Vertrauen zu gewinnen, ist einfacher als in der realen Welt. "Loverboys" sprechen den Mädchen Komplimente aus und präsentieren sich als beste Freunde. Sie bitten um Nacktbilder, weil sie doch so hübsch sind.

Cyberstalking

- Ausprägungen von obsessiven Belästigungen im Internet
- Cyberbullying kann theoretisch auch Elemente des Cyberstalkings besitzen und vice versa.

Zehn Jahre Haft für Cyber-Stalker von Amanda Todd

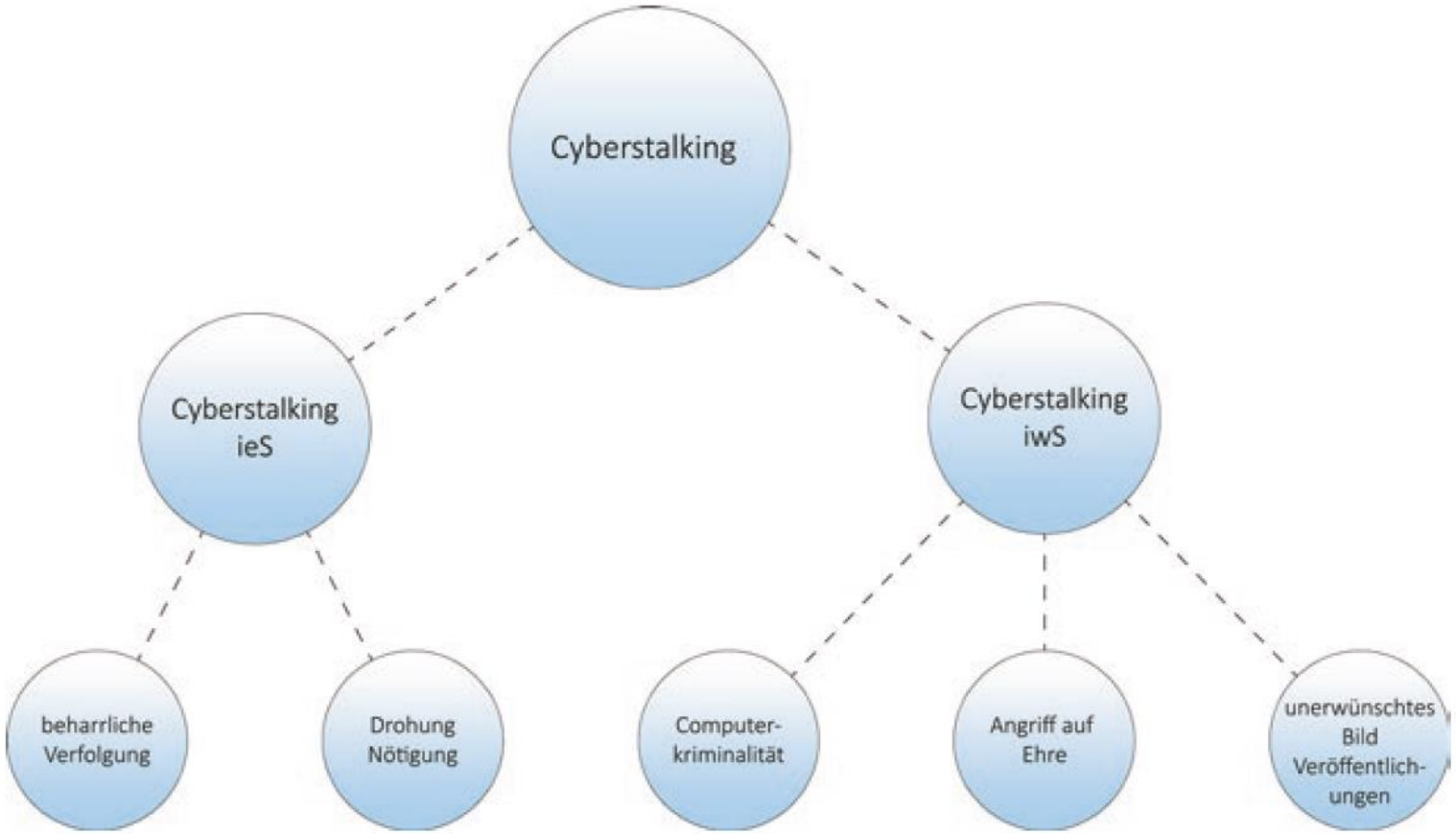
Ein niederländischer Cyber-Stalker ist für die Erpressung und sexuelle Nötigung Dutzender Mädchen zu zehn Jahren und acht Monaten Gefängnis verurteilt worden. Das Strafgericht in Amsterdam sah am Donnerstag die Schuld des 38-Jährigen als erwiesen an.

sda / *16.03.2017, 00:50 Uhr*

Ein kanadisches Opfer des Cyber-Stalkers, die 15-jährige Amanda Todd, nahm sich das Leben. Der Stalker muss nun für zehn Jahre ins Gefängnis. (Archiv) (Bild: sda)

https://tageswoche.ch/allgemein/zehn-jahre-haft-fuer-cyber-stalker-von-amanda-todd/index.html

Systematische Darstellung von Cyberstalking



Definition

Begriff Cyberstalking ist eine Verbindung der Worte ‚Cyber' und ‚Stalking'

Cyberverfolgung

"(1) um private Informationen über die Zielperson zu sammeln, um eine Verfolgung voranzutreiben; und
(2) mit der Zielperson zu kommunizieren (in Echtzeit oder nicht), um implizit oder explizit zu bedrohen oder Angst zu erzeugen."

(Pathe und Mullen 1997)

The impact of stalkers on their victims

Published online by Cambridge University Press: **02 January 2018**

Michele Pathé and Paul E. Mullen

100 Opfer

Abstract

Background

This paper examines the social and psychological impact on victims of stalking.

Method

A group of 100 victims of stalking completed a 50-item questionnaire on their experiences.

Results

The majority of the victims were subjected to multiple forms of harassment including being followed, repeatedly approached and bombarded with letters and telephone calls for periods varying from a month to 20 years. Threats were received by 58 subjects, and 34 were physically or sexually assaulted. All but six victims made major changes in their social and work lives, with 53% changing or ceasing employment and 39% moving home. Increased levels of anxiety were reported by 83%, intrusive recollections and flashbacks by 55%, with nightmares, appetite disturbances and depressed mood also being commonly reported. Suicidal ruminations were acknowledged by 24% of victims. The criteria for a diagnosis of post-traumatic stress disorder were fulfilled in 37% of subjects, with a further 18% having the clinical features but not qualifying for a stressor involving threatened or actual physical harm.

Conclusions

The study indicates the extent of the social and psychological damage sustained by those subjected to persistent stalking, and underlines the inadequacy of the current legal and medical responses to the needs of these victims.

Cyberstalking

Cyberstalking (auch Digital Stalking oder Onlinestalking) bezeichnet **das Nachstellen, Verfolgen und auch Überwachen einer Person mit digitalen Hilfsmitteln**. Dies geschieht insbesondere in Beziehungen, wovon beispielsweise sowohl aktuelle als auch ehemalige Partnerinnen oder Partner betroffen sein können. Hierzu werden nicht nur Informationen des Opfers verwendet, die es in sozialen Netzwerken veröffentlicht, sondern auch sogenannte Stalkerware, also Programme auf dem Smartphone des Opfers, mit denen Informationen gesammelt werden können.

Ähnlich der › Spyware können solche Apps dafür verwendet werden, Chat-Nachrichten, SMS oder den Standort der Person auf den Computer des Täters zu übermitteln. Auch Apps, die eigentlich dazu dienen, das Smartphone im Falle eines Verlusts zu lokalisieren, können zu privaten Spionagezwecken missbraucht werden. Um solche Apps zu installieren, wird in der Regel nur kurz Zugriff auf das zu überwachende Gerät benötigt. Anschließend ist es für das Opfer nicht zu erkennen, dass es ausspioniert wird.

(BSI)

Stalkerware

Straftatbeständewie die §§ 201, 202a ff., 238 StG

§ 238 Nachstellung

Strafgesetzbuch (StGB)
§ 238 Nachstellung

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer einer anderen Person in einer Weise unbefugt nachstellt, die geeignet ist, deren Lebensgestaltung schwerwiegend zu beeinträchtigen, indem er beharrlich

1. die räumliche Nähe dieser Person aufsucht,
2. unter Verwendung von Telekommunikationsmitteln oder sonstigen Mitteln der Kommunikation oder über Dritte Kontakt zu dieser Person herzustellen versucht,
3. unter missbräuchlicher Verwendung von personenbezogenen Daten dieser Person
   a) Bestellungen von Waren oder Dienstleistungen für sie aufgibt oder
   b) Dritte veranlasst, Kontakt mit ihr aufzunehmen, oder
4. diese Person mit der Verletzung von Leben, körperlicher Unversehrtheit, Gesundheit oder Freiheit ihrer selbst, eines ihrer Angehörigen oder einer anderen ihr nahestehenden Person bedroht oder
5. eine andere vergleichbare Handlung vornimmt.

(2) Auf Freiheitsstrafe von drei Monaten bis zu fünf Jahren ist zu erkennen, wenn der Täter das Opfer, einen Angehörigen des Opfers oder eine andere dem Opfer nahe stehende Person durch die Tat in die Gefahr des Todes oder einer schweren Gesundheitsschädigung bringt.
(3) Verursacht der Täter durch die Tat den Tod des Opfers, eines Angehörigen des Opfers oder einer anderen dem Opfer nahe stehenden Person, so ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren.
(4) In den Fällen des Absatzes 1 wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

Andere Arten des Cybermobbings im weiten Sinne wie das **Cyberstalking**, Sextortion, Bildaufnahmen etc. fallen unter die jeweils einschlägigen allgemeinen Delikte im Strafrecht.

Sextortion bezeichnet eine Form der Erpressung, bei welcher der Täter dem Opfer mit der Veröffentlichung von Nacktfotos oder -Videos des Opfers droht, um das Opfer zum Beispiel zu einer Geldzahlung oder zur Vornahme sexueller Handlungen zu zwingen, wobei der Täter die fraglichen Inhalte zuvor mit oder ohne Wissen des Opfers zum Beispiel durch Sexting oder Cybersex mit dem Opfer erlangt hat.

So kommt eine Strafbarkeit wegen:

- Nötigung (§ 240 StGB),
- Bedrohung (§ 241 StGB)
- Erpressung (§ 253 StGB)
- Nachstellung/„Stalking“ (§ 238 StGB),
- Herstellung und Zugänglichmachung von Bildaufnahmen im höchstpersönlichen Lebensbereich (§ 201a StGB)
- Upskirting (§184k StGB)

Die Bestrafung der unterschiedlichen Varianten des Cybermobbings ist nach dem materiellen Strafrecht also in vielen Fällen möglich.

Beharrliche Verfolgung

Ein Problem der Cyberstalking-Opfer – beharrliche Verfolgung nachweißbar

Das Opfer hat also für den Fall einer strafrechtlichen Verfolgung nachzuweisen, dass es beharrlich verfolgt wurde. Dies ist in vielen Fällen relativ schwer. Die Opfer müssen beweisen, dass ihre Lebensführung über einen längeren Zeitraum, in einer bestimmten Häufigkeit unzumutbar beeinträchtigt wurde.

- **Was ist unzumutbar?**
- **Was ist beharrlich?**
- **Was ist räumlichen Nähe?**

Beharrliche Verfolgung

Im klassischen Stalking, wenn z. B. jemandem täglich vor der Wohnungstür aufgelauert wird, kann diese Beharrlichkeit leichter nachgewiesen werden. Wenn man allerdings 70 SMS und 20 E-Mails pro Tag bekommt, **bietet sich als erster Lösungsweg an**, die (Mobil-) Telefonnummer oder E-Mail-Adresse zu wechseln oder den Täter zu blockieren.

Beharrliche Verfolgung

Das Aufsuchen der räumlichen Nähe, ein Merkmal des klassischen Stalkings, spielt im Falle von Cyberstalking eine untergeordnete Rolle. Um das Tatbestandsmerkmal der **Beharrlichkeit** zu erfüllen, können die einzelnen Handlungen auch kumulativ gesetzt werden. Bei der Beurteilung, ob die Lebensführung des Opfers **unzumutbar** beeinträchtigt ist, müssen alle Handlungen in der Gesamtheit geprüft und beurteilt werden.

Die klassische Computerkriminalität

Unter Cyberstalking im weiteren Sinn versteht man in erster Linie die Delikte der klassischen Computerkriminalität, die im rechtlichen Rahmen stehen.
Wenn es zu Delikten der Computerkriminalität
kommt, ist es schwierig auch das Cyberstalking-Verhalten gleich bei der Analyse mit festzustellen.
Es muss immer eine eindeutige Stalking-Absicht vorliegen.

Ein Beispiel dafür wäre, wenn sich der Täter öfter Zugriff in das Computersystem des Opfers verschafft.

Unerwünschte Veröffentlichungen von Bildern

In Zeiten von Networking-Plattformen, wie Facebook, Instagram und Co., präsentieren sich immer mehr Menschen im World Wide Web.
„Selbstdarstellung“

- persönliche Daten
- Bilder

Informationen jeglicher Art über andere Personen

Es spielt dabei keine Rolle, ob das Bild ‚echt‘ oder durch eine Fotomanipulation hergestellt wurde.

Unerwünschte Veröffentlichungen von Bildern

Gefälschte Profile auf Netzwerken (höchstpersönlichen Lebensbereich).

Unter diesen fallen beispielsweise das Sexualleben, der sensible Bereich des Familienlebens, religiöse Ansichten und Krankheiten. Bildaufnahmen (dazu zählen auch Videoaufnahmen) des höchstpersönlichen Lebensbereiches können solche des Opfers selbst, aber beispielsweise auch dessen Wohnräume sein.

Von **‚Happy Slapping‘** spricht man, wenn Prügeleien mit der Handykamera gefilmt und anschließend als Video verbreitet werden.

Dieses Phänomen existiert bereits seit 2005 …

Methoden und Formen

Die Methoden und Formen des Cyberstalkings vervielfältigen und verfeinern sich, wie bei allen Formen der Kriminalität mit der Technologieentwicklung. War es vor rund 20 Jahre noch üblich über SMS gestalkt zu werden, nehmen Stalking-Methoden, wie z. B. das Stalking über Snapchat, Facebook oder WhatsApp, in den letzten Jahren rasant zu.

Analog: wenn der Täter eine E-Mail oder einen handgeschriebenen Brief verschickt

E-Mails oder einer Nachricht: billiger und schneller

- Was ist unzumutbar?
- Was ist beharrlich?
- Was ist räumlichen Nähe?

Methoden und Formen

Cyberstalking eine neue Form des kriminellen Handelns (Entwicklungen der Telekommunikationstechnologien)

Aber

Zwischen 1980 und 1990 existierte Cyberstalking noch nicht, obwohl zu dieser Zeit die Internetnutzung schon stark zunahm.

Vermengung der unterschiedlichsten **Cyberstalking-Varianten**

- Motiv
- nicht nach dem technischen, physischen Angriffsweg definieren.

Variante 1: Offline

Diese Variante des Cyberstalking beschreibt eben jene Delikte, die es auch **offline** schon gab. Beispiel: Der verschmähte Liebhaber möchte seine Freundin zurückbekommen und schreibt ihr täglich mehrere E-Mails.
Früher tat er das durch Briefe oder zahlreiche Anrufe, nun tut er dies online.

Variante 2: Online

Es werden zum Stalking Applikationen verwendet, die es in der Offline-Variante noch nicht gibt.

Beispiel: Bleiben wir bei dem Liebhaber. Er versucht seine Freundin zurück zu erobern, indem er ihr täglich mehr als 50 WhatsApp-Nachrichten schickt.

Variante 3: Mischform

Bei Mischformen werden Online- und Offline-Varianten vermischt.
Beispiel ist wieder der verschmähte Liebhaber: Er ist verletzt und gekränkt, weil sie den Kontakt abgebrochen hat. Er verwendet die klassische SMS und SMS-Online-Plattformen,
um die Freundin wieder zurück zu bekommen.

Es ist schwierig eine klare Trennlinie zwischen den Bereichen zu ziehen.
Am Ende entscheidet das **Motiv des Cyberstalkings**, mit welcher Methode ‚cyber-gestalkt' wird.

zwei Gruppen, :

- ‚Cyberstalking' (ein Täter, mehrere Opfer)
- ‚Stalking-by-Proxy' (über Dritte)

Drei Stufen von Computerbildung bei den Opfern:

- Neulinge (novice)
- Menschen mit mittleren Fähigkeiten
- (intermediate)
- Experten (expert).

Dabei ließ sich erkennen, dass sich Neulinge häufiger bedroht fühlen als Experten. Andersherum erkannten die Experten mehr Attacken auf ihre PCs als Personen mit mittleren EDV-Kenntnissen.

Dies lässt einen Zusammenhang zwischen Computerkompetenzen und Cyberstalking-Verhalten vermuten

Cyberstalking-Täter suchen häufig Verbündete

Durch die Weiterentwicklung der Sozialen Medien hat sich die Opferstruktur in den vergangenen Jahren verschoben. Mittlerweile findet man Cyberstalking-Opfer schon bei **Kindern** bis hin zu Personen, die bereits in **Rente** sind.

Voraussetzungen: eigentlich nur ein Mobiltelefon

Waren 2006 hauptsächlich Erwachsene, geht der Trend aktuell zu Jugendlichen und jungen Erwachsenen.
Die Qualen der Opfer werden oftmals nicht ernst genommen. Fallbeispiele aus der Vergangenheit haben jedoch gezeigt, dass es sogar schon zu Todesfällen aufgrund von Cyberstalking, -mobbing oder -bullying kam.

Täter

Täterprofile Cyberstalking

Art des Cyberstalkings		
Cybercrime-Art	Cyberstalking im weiterten Sinn	Cyberstalking im engeren Sinn
Motive	Intrinsisch: z. B. sich an jemanden rächen wollen, von jmd. bewusst den Ruf schädigen wollen	Intrinsisch: z. B. verflossene Liebe, besessene Verliebtheit, Eifersucht, Nahe suchen, Nichtakzeptanz einer Trennung, Erotomanie, Hass, Aggressionen
	Extrinsisch: z. B. zufällige Gelegenheit, finanzielle Bereicherung, sich einen Vorteil verschaffen	Extrinsisch: Kontrollverlust, Ohnmacht, psych. Krankheit
Beziehungsstatus Opfer-Täter	Ex-Partner, Bekannte, Firmenkollegen, Unbekannte	Ex-Partner, Partner, Verwandte, Bekannte, Freunde, Schulkollegen, Fan
Art des Angriffs	zielgerichtet	zielgerichtet
Tatort	meist Inland	meist Inland

Vielen Dank

Prof. Dr. rer. nat. Dirk Labudde

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Computer- und Biowissenschaften | Fraunhofer Lernlabor

T +49 (0) 3727 58-1469
F +49 (0) 3727 58-21469

labudde@hs-mittweida.de

Haus 8 | Richard Stücklen-Bau | Raum 8-105
Am Schwanenteich 6b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de