Mitschrift der Crypto-Party vom 09.02.19 am Weltethos-Institut, Hintere Grabenstraße 26, 72070 Tübingen Veranstaltung der Crypto-Party Tübingen und dem Weltethos-Institut

"Digitale Gewalt – (Cyber-)Mobbing, Stalking und/oder Box(x)ing"

Begrüßung und Moderation: Dr. Christopher Gohl (Weltethos Institut)

Der Moderator begrüßt die Anwesenden und führt kurz ins Thema ein. Dabei bezeichnet er das Internet als "Treiber der Gesellschaft" und beschreibt, dass im Zuge dessen "neue" Verhaltensformen gefordert sind. Zudem verweist er unter Bezugnahme auf den Titel der Veranstaltung darauf, dass uns das Thema digitaler Gewalt alle angeht! Ziel dieser Veranstaltung ist es neben Aufklärung und Information auch den Opfern und/oder Betroffenen eine Plattform zu geben, um über die gemachten und erlebten Erfahrungen zu berichten und den Dialog zu führen und zu fördern. Im Anschluss an die kurze Einführung, stellt er die drei heutigen Fach-Referent*innen vor:

- Wolfgang Neske (Mitveranstalter der Crypto-Party Tübingen, Experte für IT-Sicherheit / IT-Forensik)
- Andrea Sauter (Geschäftsführerin der Außenstelle Weisser Ring in Reutlingen, Rechtsanwältin)
- Dr. Hanne Detel (Dozentin am Institut f
 ür Medienwissenschaften, Universit
 ät T
 übingen)

1. Impuls: Wolfgang Neske - Crypto-Party Tübingen

Was verbirgt sich hinter einer "Crypto-Party"?

"Crypto-Party" entstand in Australien (ca. 2012); Interessierte und technikaffine Bürger*innen wollten die Nachbarschaft und den Bekannten- und Angehörigenkreis primär über Entwicklungen und Trends im Internet (Geschäftsmodelle, Gesetzgeber, etc.) aufklären und informieren.

Was meint "digitale Gewalt"?

Der Begriff bezeichnet alle Formen von Gewalt, die sich technischer Hilfsmittel oder digitaler Medien bedienen, sowie Gewalt, die im digitalen Raum stattfindet, bspw. im Rahmen von Online-Portalen oder sozialen Plattformen.

- Kurz: *Gewalt + digital* (Mobbing u.a. wird mit technischen Mitteln umgesetzt, ausgeführt, weitergeführt, etc.)

Es gibt viele verschiedene Formen digitaler Gewalt. Zunächst führt der Referent einige Beispiele an (jemand verbreitet Gerüchte und Unwahrheiten über mich, jemand benutzt meine Identität und bestellt in meinem Namen Waren, jemand hat intime oder peinliche Bilder und droht diese online zu stellen, usw.). Er verweist darauf, dass das Phänomen sehr vielfältig ist und in der Öffentlichkeit zahlreiche Begrifflichkeiten kursieren. Juristisch betrachtet ist der Tathergang: eine Attacke auf ein Opfer.

Formen und/oder Begrifflichkeiten von digitaler Gewalt

- o Gerüchte verbreiten
- Nachspionieren (Stalking) (auch durch Späh-Software/Apps)
- o Identitätsdiebstahl oder Identitätsmissbrauch / Identitätsübernahme
- Heimliche Aufnahmen (Bild und/oder Ton) oder Bild- und Videomontagen
- Lokalisierung
- o Exclusion
- Doxxing (Angriff auf und Diebstahl von personenbezogene Daten um Waren zu bestellen und zu kaufen, Anrufe t\u00e4tigen)
- o Hate Speech, Hassreden, Beschimpfung, Bedrohung, Beleidigung, etc.

- Wie häufig passiert das?
 - o "subjektive Einschätzung es nimmt zu!"

Statistiken und Erhebungen

- Zitiert eine Studie (Amnesty International): knapp ¼ der Frauen haben Formen digitaler Gewalt erlebt; davon leidet die Hälfte auch k\u00f6rperlich/psychisch – Ver\u00e4nderungen des Verhaltens;
- Bundesverband der Frauenberatungsstellen und Frauennotrufe / Frauen gegen Gewalt e.V. (BFF): Digitale Gewalt (weitere Info auf der Homepage: https://www.aktiv-gegen-digitale-gewalt.de)
- Kleine Anfrage der Linken: Antwort der Bundesregierung (online); Notfallhotline;

- Kriminalstatistik

 Das Thema digitaler Gewalt taucht nicht auf! Höchstens mal in Form von Stalking oder Beleidigung ("klassische Tatbestände)

- Strafgesetzbuch

Es gibt zwar keinen eigenen "(Cyber-)Mobbing-Paragrafen" oder einen für "Formen digitaler Gewalt", gleichwohl gibt es durchaus Möglichkeiten diese Vorfälle zu ahnden, denn nicht selten greifen Gesetze des Strafrechts:

- o Beleidigung (§185 StGB)
- Üble Nachrede (§186 StGB)
- Verleumdung (§187 StGB)
- Verletzung des höchstpersönlichen Lebensbereich durch Bildaufnahmen (§201a StGB)
- Nachstellung auch Stalking (§238 StGB)
- Nötigung (§240 StGB)
- Bedrohung (§241 StGB)
- Recht am eigenen Bild (§22 KunstUrhG)
- Strafvorschrift (§33 KunstUrhG)

https://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/was-sagt-das-gesetz/

Tatbestände bestehen, aber müssen aktiv angezeigt werden (=Antragsdelikte);

Ulrike Lembke "Kollektive Rechtsmobilisierung gegen digitale Gewalt" (2017): Sie untersuchte das Phänomen mit dem Ergebnis, dass es zur Verharmlosung kommt und zur Unterschätzung der strafrechtlichen Relevanz;

"Doch diese Straftatbestände werden bislang nicht zur Bekämpfung digitaler Gewalt mobilisiert. Ein Grund dürfte sein, dass digitale Gewalt verharmlost und ihre strafrechtliche Relevanz nicht erkannt wird: "nur Worte". Zudem wird oft bestritten, dass die Tatbestandsvoraussetzungen der jeweiligen Norm vorliegen."

- Was fehlt uns?
 - o Untersuchungen über Formen und Ausmaß digitaler Gewalt (und deren Formen)
 - Wissen über Art und Weise digitaler Gewalt und dem Umgang damit
 - o Mangelndes Bewusstsein bei Polizei und Staatsanwalt;
 - Anpassung von Rechtsnormen?!
 - Fehlende IT-Forensiker*innen, die Vorfälle analysieren, Schadsoftware und andere Fehlerquellen erkennen und Beweise sichern können;
 - o Mehr Geld und Qualität bezüglich Infos, Beratung und Fort- und Weiterbildung;
 - o Informierte Akteure: Politik; Wirtschaft, Zivilgesellschaft;

Überlegungen und Anmerkungen (5 Min. Murmeln)

Braucht es mehr Handlungsmöglichkeiten (für Bürger*innen, Eltern, aber auch Professionelle und Opfer) sich zu wehren (Alltagsnah) oder braucht es mehr Wissen und Informationen über bereits bestehende Handlungsmöglichkeiten? Vermutlich beides. Präventive Maßnahmen sind an Schulen, in Betrieben und Ausbildungsstätten anzubieten.

Polizeiempfehlung: Melden Sie das Kind von Netzwerken ab; Posten Sie keine Nacktbilder*innen; da können wir nichts machen; Empfehlungen wie diese sind wenig hilfreich!

2. Impuls von Andrea Sauter – Weisser Ring (Leiterin einer Außenstelle in RT, Rechtsanwältin)

Was ist bzw. was tut "Weisser Ring"?

Zu den zentralen Aufgaben gehören: Betreuung von Opfern von Gewalt (allgemein; vereinzelt auch Cybermobbing), Begleitung zur Polizei; zur Therapie, etc. / Opferhilfe / Prävention / Öffentlichkeitsarbeit – Öffentliches Eintreten;

Gemeinnütziger Verein zur Unterstützung von Kriminalitätsopfern und zur Verhütung von Straftaten (Bundesgeschäftsstelle in Mainz / über 400 Außenstellen, eine davon befindet sich in Reutlingen)

Zahlen und Fakten:

5,76 Millionen Straftaten wurden 2017 in Deutschland verübt

Alle drei Minuten bricht jemand in ein Haus ein – Beratung und Betreuung, da Sicherheitsgefühl verletzt ist bzw. geht verloren;

Ehrenamtliche Profis im Einsatz (Deutschlandweit)

- Justiz und staatliche Stellen nicht gut vorbereitet;

"Das Opfer hat fast immer lebenslänglich."

Die unterschiedlichen Formen digitaler Gewalt sind ebenfalls zunehmend ein Thema beim "Weissen Ring", auch wenn die Erfahrungswerte noch nicht sehr hoch sind. Interessante Unterstützer*innen aus Politik und Film;

Buchempfehlung: Cem Karakaya & Tina Groll (2018): Die Cyber-Profis – Lassen Sie Ihre Identität nicht unbeaufsichtigt. Zwei Experten für Internetkriminalität decken auf, Ariston Verlag, 256 Seiten

3. Impuls von **Dr. Hanne Detel** – Institut für Medienwissenschaft an der Universität Tübingen

Digitale Gewalt – Über den Kontrollverlust im Netz – Ansätze der Prävention und Reaktion (PPP)

(Lehrstuhl: Prof. Dr. Pörksen) / Dialog mit anderen Akteur*innen;

Einstieg ins Thema: 2009/10 Skandale im Netz

Die Referentin hat ebenfalls persönliche Erfahrung gemacht und festgestellt, wie schnell es gehen kann, dass man mit digitaler Gewalt konfrontiert ist. Gründe sieht Sie zum einen darin, dass wir in der Öffentlichkeit (durch Social Media und Suchmaschinen) präsenter sind und somit eine größere Angriffsfläche bieten. Zum anderen kommt man über Recherche im Netz leicht an Infos. Das Internet bietet viele Möglichkeiten und es ist schön – dass wir so schnell und einfach viele Infos bekommen, aber es gibt eben auch die "dunkele Seite" des Internets;

Bild: Pranger-Situation aus dem 18. Jh. vergleichbar mit einem Shitstorm von heute?!

Phänomene digitaler Gewalt: Diffamierung, Scamming, Grooming; Internet-Shaming, Nötigung, Rufschädigung, Bedrohung, Datenklau, Bloßstellung, ... vieles wurde bereits benannt;

Begriffsklärung: Was meint Cybermobbing – und –bullying?

"Unter Cyber-Mobbing (Synonym zu Cyber-Bullying) versteht man das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mithilfe von Internet- und Mobiltelefondiensten über einen längeren Zeitraum hinweg."

Anmerkung: Je nach Inhalt kann ein einmaliges Hochladen bereits gravierende Auswirkungen haben, sodass es nicht zwangsläufig über einen längeren Zeitraum gehen muss

Cyberstalking (Nachstellen und nachspionieren von Personen).

Auszug aus der JIM-Studie 2017 zu dem Thema

Im Bekanntenkreis wurde schon mal jemand per Handy/im Internet fertig gemacht ...

JIM-Studie – Eine Untersuchung des Medienpädagogischen Forschungsverbundes Südwest (mpfs) – Online sind alle Studien seit 1998 abrufbar

Vom Mobbing zum Cybermobbing – 8 Thesen

- 1. (vermeintliche) Anonymität bzw. Pseudonymität des Täters
- 2. physische Unsichtbarkeit
- 3. Angriffe rund um die Uhr möglich
- 4. kein Rückzugsort (vor den Beleidigung)
- 5. Eingriff in die Privat- oder Intimsphäre
- 6. Enthemmung durch Gruppendynamik (Enthemmungseffekt) und vermeintliche Regellosigkeit;
- 7. rasante Verbreitung der diffamierenden Inhalte in kurzer Zeit an ein großes Publikum
- 8. Dauerhaftigkeit der digitalen Inhalte

-> Folge: VERLUST DER KONTROLLE

Schwer zu löschen, denn es kann immer wieder hochgeladen werden ...

In ihren wissenschaftlichen Untersuchungen hat sich die Referentin v.a. mit Online-Skandalen von Prominenten beschäftigt; z.B. Dog-Shit-Girl – Hund kackt in die U-Bahn! Die Hundehalterin wird aufgefordert den Kot zu entfernen. Sie weigert sich. Ein Fahrgast zückt sein Handy und nimmt die Szene auf. Das Bild verbreitet sich rasend schnell in diversen Social Media Plattformen;

Wichtiger Hinweis: Jede*r kann Opfer und Täter*in werden; Laut wissenschaftlichen Erkenntnissen unterschätzen viele Täter*innen die Folgen der Veröffentlichung und die Verbreitung des Inhalts; denn "das wollten die Leute nicht"; (gewollt/ungewollt)

Das digitale Panoptikum (Quelle: Bentham, J. (1791): Panoptikum Leben wir in so einer Zeit?! Jede*r beobachtet jede*n ... Ist uns das allen klar?! Sind wir Publikum oder Insassen?!

Vom Umgang mit dem Kontrollverlust

- Kategorischer Imperativ des digitalen Zeitalters "Handele stets so, dass Dir die öffentlichen Effekte deines Handels langfristig vertretbar erscheinen. Aber rechne damit, dass dies nichts nützt." Oder auch: Sei dir stets über die möglichen Folgen deines Handelns bewusst – wohlwissend, dass es nicht ausreichen wird …"

	Individuum	Gesellschaft
Prävention	 Sparsam mit Daten umgehen Privatsphäre-Einstellungen anpassen Freundschaftsanfragen prüfen Sichere Passwörter und regelmäßiger Wechsel 	- Medienerziehung - Medienmündigkeit
Reaktion	- Beweise sichern - Vergehen, Nutzer oder gefälschte Profile melden - Distanz zum Angreifer (Blockieren, Adresse ändern, etc.) - Gespräche suchen, falls Täter bekannt ist - Ggf. Anzeige erstatten - Beratungsangebot nutzen - Reputationsmanagement (d.h. sich professionelle Hilfe im Netz suchen, Löschung der Daten)	 Digitale Empathie (Schaden wir jemanden mit dem Post) Gelassenheit Mithilfe im Kampf gegen die Täter*innen Counter Speech (dagegenReden), Juuuport
	-	-

Diskussion im Plenum

Offene Fragen und/oder Ergänzungen

- Ein Opfer von Dox(x)ing berichtet über (frustrierende) Erfahrungen mit Polizei und Staatsanwaltschaft;: "Ich ging zur Polizei und habe Strafanzeige gestellt. Die Person hat mich angeschaut und – so mein Eindruck – der/die wusste anfangs nicht, was ich eigentlich von ihm/ihr wollte. Damals dachte ich – der kennt sich halt nicht aus; aber was soll es."
 Das Strafverfahren wurde inzwischen eingestellt. Grund: Die Person ist nicht auffindbar!
- Was muss da konkret passieren?
 Ein TN ist der Meinung, dass es v.a. Zeit braucht und zieht einen Vergleich zu
 Krankheitsbildern, die auch lange Zeit nicht anerkannt wurden;
 Vereinzelt wird darauf verwiesen, dass es mehr Transfer und eine stärkere
 Übersetzungsleistung braucht, sodass auch Formen digitaler Gewalt als Straftatbestand
 anerkannt und konsequenter verfolgt werden.
- Hinweis der Veranstalter Auch die Polizei wurde zu der heutigen Veranstaltung eingeladen, allerdings wurde von einer aktiven Teilnahme abgesehen.
- Geschäftsmodelle von Facebook und Google (Bundeskartellamt wird aktiv, Bundesregierung nicht!) Eine Forderung, dass die Politik aktiv werden muss, wird kritisch kommentiert. Wie soll die Politik (Bundesregierung) da Einfluss nehmen? Das sind international und global agierende Konzerne ... Wie wirkungsvoll sind nationale oder auch europäische Regulierungen?

4. Impuls von Wolfgang Neske

Impression – eigene Recherche (politische, soziale, technische Infos/Ebenen) Gibt es eigentlich ein gemeinsames Grundverständnis? Oder hat jeder/jede was für sich ... Was ist mit der Netiquette? Digitale Grundrechte (EU) - Digitale Ethik

Nächste Woche werden technische Aspekte beleuchtet, um präventiv tätig zu werden. Dabei geht es u.a. darum, Beweise zu sichern (Screenshots – Beweiskräftig?! Was meint beweiskräftig? Facebook späht viel aus, kann das vielleicht auch hilfreich sein? Wenn jemand betroffen ist, spricht viel dafür, dass man "neu" anfängt – digitaler Neustart / Reset-Taste. Ist das möglich und wenn ja, wie? Reputationsmanagement?!

Wir sitzen nicht nur zu Hause an unseren digitalen Endgeräten, sondern tragen unseren "Gerätezoo" meistens mit uns herum und sind ständig online. Wie gehen wir damit um? Wie wollen wir vielleicht künftig damit umgehen? Wie sieht es in der Firma aus? E-Mail, Soziale Medien, etc. Wie gehen wir dort damit um? Was tue ich und was nicht und wie gehe ich damit um, wenn ich gehackt und/oder angegriffen werde?

Ein zeitliches Format von 2 bis 3 Stunden reicht da fast nicht aus! Zumal die Themen nicht nur besprochen werden sollen, sondern es soll auch ums Handeln und Aktiv-werden gehen. Wie kann ich mich besser schützen?

Weiß jede*r von ihnen, dass das Handy/Smartphone bei Bildaufnahmen die Lokalisation meist automatisch mitträgt und speichert? Das kann man/frau Ausschalten, aber wenn das nicht aktiv gemacht wird, ist die Information dauerhaft enthalten! Beim I-Phone werden Bilder sogar gleich nach Datum, Ort und Zeit sortiert und auf einer Landkarte markiert.

"Die Crypto-Party gibt es seit vielen Jahren, d.h. wir fangen nicht bei 0 an – aber wir haben auch noch viel vor uns".

Veranstaltungshinweis

Crypto-Party Samstag, 09.03.2019 (15:00 bis 18:00 Uhr am Weltethos Institut) Bitte Geräte mitbringen!

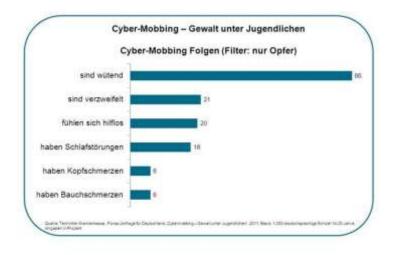
Nachtrag von Christiane Bollig:

Beim Cyber-Mobbing oder –Bullying handelt es sich um kein völlig neues Phänomen, jedoch unterscheidet es sich in einigen Punkten vom "einfachen" oder "klassischen" Mobbing:

- Cybermobbing ist weder zeitlich noch räumlich begrenzt bzw. eingeschränkt.
- Das Publikum ist unüberschaubar groß. Der Verbreitungsgehalt im Netz ist enorm und nicht bzw. nur schwer kontrollierbar (Schneeball-Effekt).
- Täter*innen können leichter unerkannt bzw. anonym bleiben.
- Cybermobbing kann jeden/jede treffen (Kinder, Jugendliche, Mitschüler/innen, Gleichaltrige, Lehrer/innen, Fremde, etc.).

Erschwerend hinzukommt, dass hochgeladene Inhalte und Bilder, Videos aus dem Internet nur schwer zu entfernen sind, da diese, wenn sie nur einmal kopiert und heruntergeladen wurden, immer wieder neu eingestellt werden können. Dies führt nicht selten zu einem Kontrollverlust über Daten und Informationen → besonders hohes Belastungspotenzial!

Eine Studie der TK (2011) zeigt, welche Folgen Cyber-Mobbing bei den Betroffenen auslösen (können). Zudem wissen viele nicht an wen sie sich wenden können.



Es gibt weder ein konkretes Täter- noch ein Opferprofil. Durch vermeintliche Anonymität sinkt die Hemmschwelle ("es ist so einfach!") - *Online-Enthemmungseffekt*

Ursachen/Motive sind vielfältig: kleine Nichtigkeiten, unerwiderte Liebe, Neid, Hass, Rache, verletzte Ehre, sexuelle Orientierung, politische Einstellung, etc.

Hinweis auf Angebote des Demokratiezentraum Baden-Württemberg:

Demokratiezentrum BW (https://demokratiezentrum-bw.de/) – Projekte: Da.gegen.Rede (Umgang mit Hassreden und Gerüchten im Netz) https://demokratiezentrum-bw.de/angebote/da-gegen-rede/ https://demokratiezentrum-bw.de/) – Projekte: Da.gegen.Rede (Umgang mit Hassreden und Gerüchten im Netz)

Respekt – eine Meldestelle für Hass im Internet

https://demokratiezentrum-bw.de/angebote/respect-die-meldestelle-fuer-hetze-im-netz/

Zum Nachlesen und Informieren:

Belkacem, Iméne (2012): Cyber-Mobbing: Der virtuelle Raum als Schauplatz für Mobbing unter Kindern und Jugendlichen: Problemlagen und Handlungsmöglichkeiten (Verlag: Diplomica)

Fawzi, Nayla (2009): Cybermobbing. Ursachen und Auswirkungen von Mobbing im Internet (Verlag: Nomos)

Grimm, Petra/Rhein, Stefanie/Clausen-Muradian, Elisabeth (2008): Gewalt im Web 2.0: Der Umgang Jugendlicher mit gewalthaltigen Inhalten und Cyber-Mobbing sowie die rechtliche Einordnung der Problematik (Verlag: Vistas)

Pieschl, Stephanie/Porsch, Torsten (2012): Schluss mit Cybermobbing. Das Trainings- und Präventionsprogramm "Surf-Fair". Mit Film und Material (Beltz-Verlag)

Riebel, Julia/Zentrum für empirische pädagogische Forschung (Hrsg.) (2008): Spotten, Schimpfen, Schlagen ... Gewalt unter Schülern – Bullying & Cybermobbing

Schäfer, Mechthild/Herpell, Gabriela (2011): Du Opfer! Der Mobbing-Report.

Scheithauer/Hayer/Petermann: Bullying unter Schülern – Erscheinungsformen, Risikobedingungen und Interventionskonzepte

Materialien und Broschüren:

Aktion Jugendschutz Landesarbeitsstelle Baden-Württemberg (Hrsg.): ajs-Kompaktwissen (2012): Cybermobbing (URL: www.ajs-bw.de)

Aktion Jugendschutz Landesarbeitsstelle Baden-Württemberg (Hrsg.) (2012): ajs-Informationen. Analysen. Materialien. Arbeitshilfe zum Jugendschutz: Cybermobbing (Fachzeitschrift der Aktion Jugendschutz. Nr. 2/48 Jg.)

Aktion Jugendschutz Baden-Württemberg (Hrsg.) (2017): **Schriftenreihe Medienkompetenz.** *Medien: Macht-Gewalt-Kultur? Herausforderungen für Medienpädagogik und politische Bildung*. Stuttgart

Arbeitsgemeinschaft Kinder- und Jugendschutz (AJS) Landesstelle Nordrhein-Westfalen e.V. (Hrsg.) (2012): Cybermobbing. Informationen für Eltern und Fachkräfte (DREI-W-VERLAG GmbH)

Arbeitsgemeinschaft Kinder- und Jugendschutz (AJS) Landesstelle Nordrhein-Westfalen e.V. (Hrsg.) (2007): Mobbing unter Kindern und Jugendlichen. Informationen für Schulen, Jugendhilfe und Eltern. (DREI-W-VERLAG GmbH)

Klicksafe (Hrsg.) (2012): Was tun gegen Cyber-Mobbing? Zusatzmodul zu Knowhow für junge User.

Unterstützung, Beratung und Informationen (Empfehlenswerte Links):

Für Eltern und Interessierte

http://www.jugendschutz.net/ (Infos zu Cybermobbing, Rechtsextremismus und Islamismus im Internet, etc.)
www.netzdurchblick.de

<u>www.klicksafe.de</u> (Unter Themen: Cybermobbing. Dort gibt es Broschüren, Info-Materialien, Spots und vieles mehr) u.a. https://www.klicksafe.de/themen/rechtsfragen-im-netz/irights/cyber-mobbing/

http://zartbitter.de/gegen_sexuellen_missbrauch/Aktuell/100_index.php

www.internet-beschwerdestelle

https://www.buendnis-gegen-cybermobbing.de/

http://www.schueler-gegen-mobbing.de (Hilfe für Schüler, Eltern und Lehrer)

Für Kinder und Jugendliche

https://www.netzdurchblick.de/ - Der Internetratgeber für Jugendliche – Gaming, sicheres Surfen, etc.

https://www.handysektor.de/startseite/

https://mobbing-schluss-damit.de/cybermobbing

<u>https://mobil.seitenstark.de/</u> Internetseite für Kinder

Kostenlose, anonyme Beratungs- und Informationsplattformen:

www.juuuport.de www.youth-life-line.de https://www.jugendnotmail.de/ www.bke-beratung.de

Nummer gegen Kummer (0800 – 111 03 22 oder 11 61 11) www.nummergegenkummer.de