

# Patriarchale Gewalt im digitalen Raum

AG Link & Kritische Jurist\*innen Leipzig  
09.10.2023

# Geschlechtsspezifische digitale Gewalt

geschlechtsspezifischer Gewalt, die durch technische Hilfsmittel ausgeübt wird oder im digitalen Raum stattfindet (bff 2019)

# Formen

- Doxing
- Identitätsdiebstahl /-missbrauch
- (Cyber-)Stalking
- Diffamierung
- Bedrohung
- Non-Consensual Pornography (“Revenge-Porn”)
- Belästigung (auch cyber harassment)
- Cyber-Grooming
- Deepfakes
- Kontrolle durch technische Geräte
- Zugangsverweigerung
- Psychoterror (Gaslighting)

# Aspekte des Digitalen

- Schnelles Weiterleiten & Kopieren
- Anonymität
- Standortunabhängigkeit
- Fehlendes Verständnis für Ernsthaftigkeit
- Herausfordernd für Beratungsstellen

# Auswirkungen

- Verunsicherung, Scham, Ohnmacht, Angst
- Stören von Beziehungen zu Freund\*innen und Familie
- Rückzug aus Onlineleben
- Psychische Krankheiten: Depression, Angststörung, Schlafstörung, ...

# Wer ist betroffen?

- Geschlechtsspezifische Gewalt: Betroffene sind meist Frauen, Ausübende meist Männer
- 18% der Frauen von Stalking betroffen, Ausübende zu 80% Männer
- Jüngere Menschen häufiger von digitaler Gewalt betroffen
- Datenlage schlecht

# Technische Perspektive

# Allgemeines

- Überblick über eigene digitale & technische Nutzung
- Datensicherheit + Datensparsamkeit
- up-to-date bleiben
- Medienkompetenz & digitale Selbstbestimmung stärken (individuelle Ebene)
- öffentliche Debatte verfolgen & sich einmischen (gesellschafts-politische Ebene)



## Checkliste zur digitalen Trennung

**HINWEIS!** Sie können gerne im Vorfeld unsere Beratung aufsuchen, besonders wenn:

- Sie befürchten, dass sich durch die „digitale Trennung“ Gewalt d. Partner\*in verschärft.
- Sie befürchten, dass digitale Gewalt bereits stattgefunden hat und sie diese nachweisen möchten.

Alle Schritte auch für die Geräte und Accounts der Kinder anwenden!

### Zu Beginn

- Bestandsaufnahme aller Accounts und Geräte anfertigen

Beispiel

Name Gerät/Account	Gemeinsam genutzt?	Hatte Partner*in (möglichen) Zugriff?	Sensibel?	Sicheres Passwort?
Smartphone	nein	ja	ja	nein
E-Mail	nein	nein	ja	nein
...				

### Dringend

- Geräte, die gemeinsam genutzt wurden/ durch Partner\*in eingerichtet wurden/ ein (möglicher) Zugriff für Partner\*in bestand: auf Werkeinstellungen zurückstellen

- Smartphone
- Laptop/PC/Tablet
- W-LAN-Router
- Smart-Geräte (besonders: Smart-Watch, Haustür!)
- \_\_\_\_\_

- Updates (Apps & Betriebssystem) durchführen

- Bestandsaufnahme aller Accounts und Geräte anfertigen

Beispiel

Name Gerät/Account	Gemeinsam genutzt?	Hatte Partner*in (möglichen) Zugriff?	Sensibel?	Sicheres Passwort?
Smartphone	nein	ja	ja	nein
E-Mail	nein	nein	ja	nein
...				

# Wo lauern Gefahren?

- Browser, Suchverläufe, etc.
- Unsichere Passwörter
- Datenleaks/ Hacks
- Social Media
- Cloud & Datenspeicher
- Smarte Gadgets & Kameras
- Stalking Apps & Stalker Ware



# Browser

- Browserverlauf & gespeicherte Informationen verraten viel
- Phishing (besonders E-Mails)
- Accounts ausloggen (Amazon, Online Banking, etc.)
- Regelmäßig Browserdaten löschen

## History

- Remember browsing and download history
- Remember search and form history
- Clear history when LibreWolf closes

Clear History...

Settings...



## History

- Browsing & download history
- Active logins
- Form & search history
- Cookies
- Cache

## Data

- Site settings
- Offline website data

Cancel

Clear Now

# Passwörter

- Sichere Passwörter:
  - Min. 12 Zeichen
  - "echte" Wörter vermeiden bei kürzeren Passwörtern („Tisch123“)
  - Sonderzeichen (Ä, ß, %, ...)
  - PINs vermeiden
- Einmalig verwenden
- Passwörter ändern (z.B. nach Trennung)
- Passwort Reset Optionen sichern (E-Mail Zugang, Handy Zugang)
- Nicht weitergeben & nicht aufschreiben!



# Passwörter

- Schwache Passwörter ermöglichen oft eindringen in Accounts
- Kann zur Veröffentlichung von Daten führen

Entity	Year	Records	Organization type	Method	Sources
Bangladesh Government website data breach	2023	50,000,000+	government	data leak due to security vulnerabilities	[46]
Duolingo	2023	2,676,696	educational services	hacked	[10][123]
Evide data breach	2023	1,000	computer services for charities	ransomware hacked	[141][142] [143][144][145]
Manipulated Caiman	2023	40,000,000	financial	hacked	[247][248]
NTT Docomo	2023	5,960,000	telecoms	hacked	[285]
Philippine law enforcement agencies (Philippine National Police, National Bureau of Investigation, Bureau of Internal Revenue)	2023	1,279,437	government	poor security	[294]
Tesla	2023	75,000	transport	inside job	[353]
Tic Hosting Solutions (known as Torchbyte)	2023	unknown	hosting provider	hacked	[356]
T-Mobile	2023	37,000,000	telecom	hacked	[363]

## DuoLingo (2.6 Million Entries) Scrape

by House - Tuesday January 24, 2023 at 02:18 AM

 House



1 hour ago (This post was last modified: 1 hour ago by House.)

#1

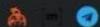
I am selling 2.6 million DuoLingo account entries that were scraped from an exposed API.

Starting price is \$1,500 USD, but the price can be negotiated.

### The data contains the following fields:

Email, joinedClassroomIds, Streak, Motivation, acquisitionSurveyReason, shouldForceConnectPhoneNumber, Picture, learningLanguage, hasFacebookId, shakeToReportEnabled, shakeToReportEnabled, liveOpsFeatures, canUseModerationTools, id, betaStatus, hasGoogleId, privacySettings, fromLanguage, hasRecentActivity15, achievements, observedClassroomIds, username, bio, profileCountry, globalAmbassadorStatus, currentCourseId, hasPhoneNumber, creationDate, hasPlus, name, roles, classroomLeaderboardsEnabled, emailVerified, courses, totalXp

Below is a sample of 1,000 accounts for you to look through. If you're interested in buying it, please contact me on one of the platforms linked below this post.



Posts: 46  
Threads: 7  
Joined: Jul 2022  
Reputation: 657

# Passwörter

- Schwache Passwörter ermöglichen oft eindringen in Accounts
- Kann zur Veröffentlichung von Daten führen
- Tools um nach Datenleaks & Hacks zu suchen:
  - Identity Leaker Check (<https://sec.hpi.de/ilc/>)
  - Firefox Monitor (<https://monitor.firefox.com/>)
  - Have I been powned? (<https://haveibeenpwned.com/>)

# We found **mmeheykeroth@web.de** exposed in **2** data breaches.

Sign in to get clear steps on how to resolve these breaches, view all breaches, and get continuous monitoring for any new known breaches.

[Sign in to resolve breaches](#)



## MyFitnessPal

Breach Added:  
**February 21, 2019**

Exposed Data:  
**Email addresses, IP addresses, Passwords, Usernames**

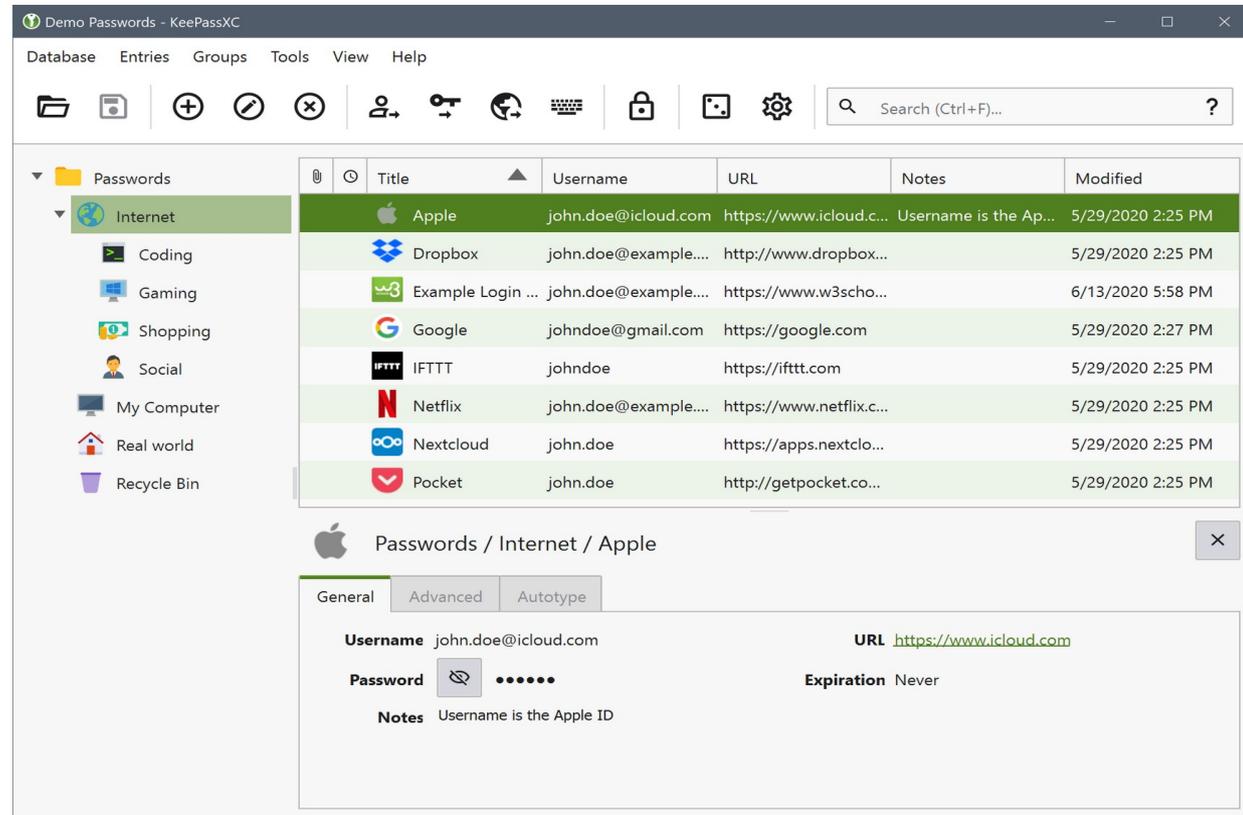
## Heroes of Newerth

Breach Added:  
**January 24, 2016**

Exposed Data:  
**Email addresses, Passwords, Usernames**

# Passwörter

- Passwort Manager verwenden (Empfehlung: **KeepassXC**)
- 2-Faktor-Authentifizierung nutzen



# Social Media

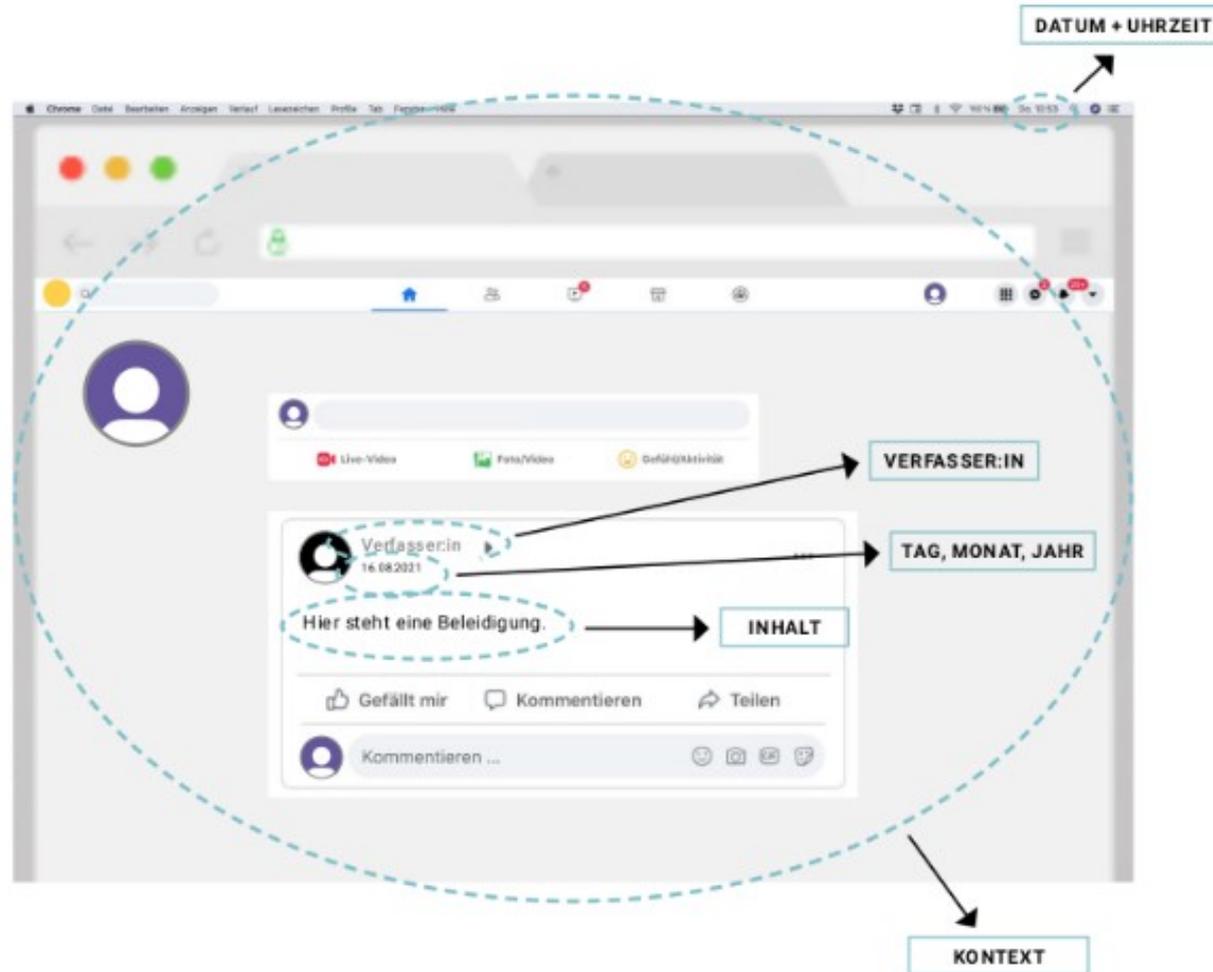
- Welche Daten sollen von mir öffentlich sein? Was kann gegen mich verwendet werden? Wer kann das sehen?
- Privatsphäre Einstellungen überprüfen (privates Profil, Sichtbarkeit nur für Freunde, ...)
- Plattform kontaktieren, Personen blockieren, Chats melden (kann auch von Freund\*innen übernommen werden)
- Stalking Tagebuch & rechtssichere Screenshots
- Betrug & Phishing aufpassen
- Fallspezifisch → Beratungs-/ Hilfsangebote nutzen
  - Dickpics: Online Tool für Erstellung einer Anzeige (<https://dickstinction.com/>)



# Rechtssichere Screenshots

- Auf Screenshot sichtbar:
  - URL
  - Datum & Uhrzeit
  - Verfasser der Nachricht (z.B. bei Twitter)
  - Kontext muss ersichtlich sein (an wen richtet sich Nachricht/ Kommentar)
  - Auch Screenshot des Profil des Täters
  - Keine eigenen Informationen preisgeben (offene Tabs, Lesezeichen, etc.)
- Evtl. weitere Informationen von Nutzen → hängt aber von Plattform ab (YouTube, Twitter, Instagram, ...)
  - Rechtssichere Screenshots als Beweismittel bei Gewalt im Netz. Eine Kurzanleitung für Betroffene und Ratsuchende (<https://verband-brg.de/rechtssichere-screenshots/>)

# Rechtssichere Screenshots



# Rechtssichere Screenshots

- z.B. Browser (Chrome) Plugin: *Atomshot*
- Dokumentiert Datum + URL mit Bild

This screenshot was taken on 2023-05-29, 15:27:34 (atomic time PTB)  
URL: <https://twitter.com/Dagobert95>

Onkel Dagobert  
84.023 Tweets

WUTERGANQ DES FUS\$BALLS

Onkel Dagobert  
@Dagobert95

Tiefkühl-Kroketten und Fortuna Düsseldorf. Niemand mag Gewinner.

Düsseldorf, Deutschland Seit Mai 2011 bei Twitter

2.391 Folge ich 20.073 Follower

Twitter durchsuchen

**Neu bei Twitter?**  
Registriere dich jetzt, um deine eigene personalisierte Timeline zu erhalten!

Mit Google anmelden

Mit Apple registrieren

Account erstellen

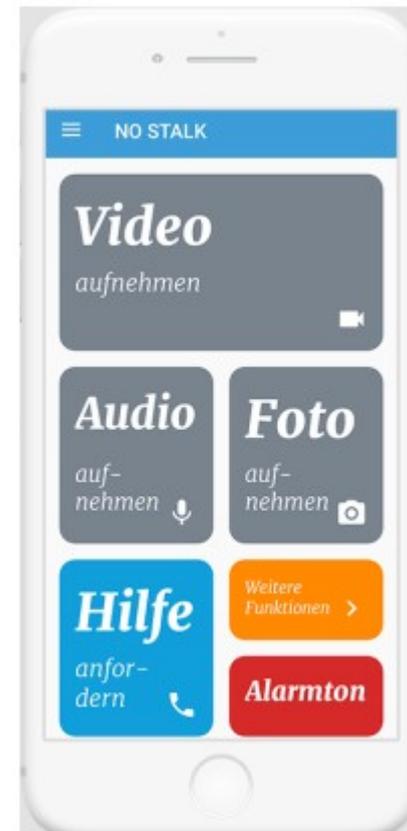
Indem du dich registrierst, stimmst du den [Allgemeinen Geschäftsbedingungen](#) und [Datenschutzrichtlinien](#) sowie der [Nutzung von Cookies](#) zu.

varzgelb sta  
:nwalder Mi  
enlogo in E



# Stalking Tagebuch

- App: *No-Stalk*
- erleichtert Dokumentation von Stalking Vorfällen
- Verschlüsselter Upload von Fotos, Video & Audio
- Dokumentiert: Wo, Wer, Wann, Was (bei Upload)
- Materialien können über Website gesammelt & chronologisch runtergeladen werden
- Website (<https://nostalk.de/>)



# Einschub: Sensible Bilder verschicken

- es gibt keine Garantie auf Sicherheit → überlege genau was & warum du etwas machst
- Nutze nur Ende-zu-Ende Messenger (z.B. Signal)
- Kein Gesicht/ Tattoos/ auffälliger Hintergrund
- GPS deaktivieren
- Cloud-Synchronisierung deaktivieren
- Verändere Bild o. füge Wasserzeichen mit Namen der Person ein
  - erleichtert Identifikation falls Bild veröffentlicht wird
  - Hemmt Person evtl. vor Weiterleitung

# Cloud & Datenspeicher

- Wer hat Zugang zu meinen Daten/ Cloud?
- Cloud Einstellungen überprüfen (geteilte Ordner, automatische Synchronisierung, ...)
- Sichere Passwörter + 2-Faktor Authentifizierung
- Ungenutzte/ alte Dateien anderweitig ablegen
- Zugang sichern durch Verschlüsselung



# Cloud & Datenspeicher

- *Unsere Empfehlung*
- Verschlüsselungs-Programm:
  - für eigenen Rechner/ Festplatten/ USB-Sticks:
    - **VeraCrypt**: verschlüsselt Festplatte oder “Daten-Safe”
  - Für Cloud-Speicher:
    - **Cryptomator**: Daten auf eigenem Rechner verschlüsseln, dann Synchronisierung der Daten in Cloud



**CRYPTOMATOR**

# Das Internet der Dinge

## Die Auswirkungen »smarter« Geräte auf häusliche Gewalt

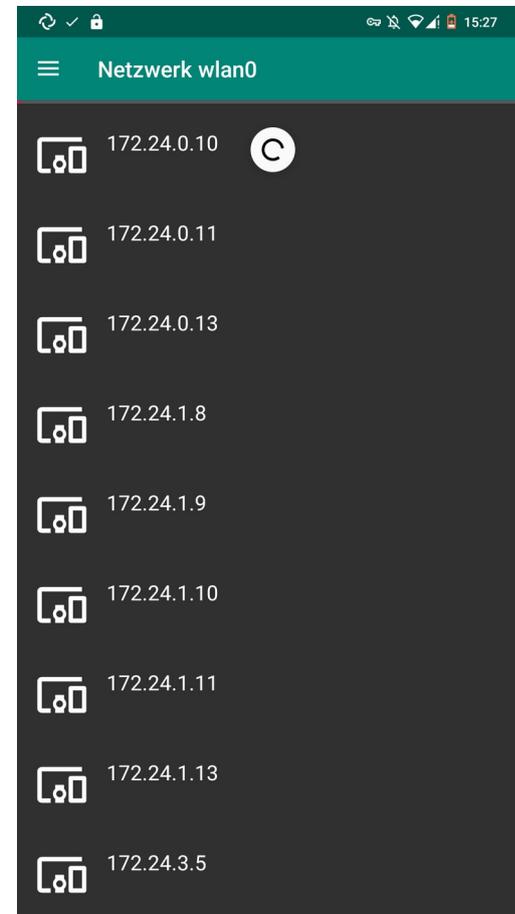
---

*Leonie Maria Tanczer*

Aus:  
Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung: Formen und Interventionsstrategien  
(<https://www.frauen-gegen-gewalt.de>)

# Smart Home Geräte

- Inventur! Welche Geräte? Was können die? (Stecker, Lampen, Thermostate, Thermometer, Kameras, Türschloss, Waschmaschine, ...)
- Wer hat Geräte eingerichtet?
- Gibt es Geräte, von denen ich nichts weiß?
  - 1) Scanne lokale Geräte (z.B. Android – “Ning”, iOS – “Vernet”)
  - 2) Nutze Handy-Kamera, um Kameras zu finden ([mehr Tipps](#))



# AirTag Stalking

- AirTags erlauben Ortung in Echtzeit
- Neuere iOS Versionen warnen automatisch (ab iOS 14.5)
- Weniger Chancen für Android
- AirTag Hacking als neue Gefahr

**Immer mehr Stalking-Fälle mit Bluetooth-Trackern wie Apple AirTags**

Ravensburger Polizeipräsident warnt vor Dunkelfeld bei Cyberstalking



# Stalking Apps



**Track Employees Check Work Phone Online Spy Free**  
Daily Tools  
PEGI 3  
★★★★☆ 73

This app is compatible with your device.

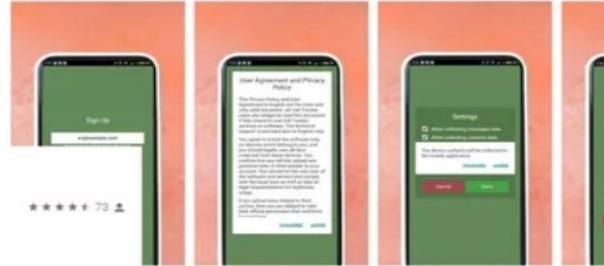
Add to Wishlist [Install](#)



**Spy Kids Tracker**  
Wido Personalization  
PEGI 3  
★★★★☆ 236

This app is compatible with your device.

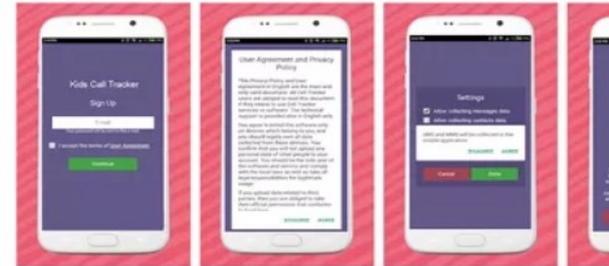
Add to Wishlist [Install](#)



**Employee Work Spy**  
Piter Cline Tools  
PEGI 3  
★★★★☆ 1,263

This app is compatible with your device.

Add to Wishlist [Install](#)



**Phone Cell Tracker**  
StaHar Tools  
PEGI 3  
★★★★☆ 73

This app is compatible with your device.

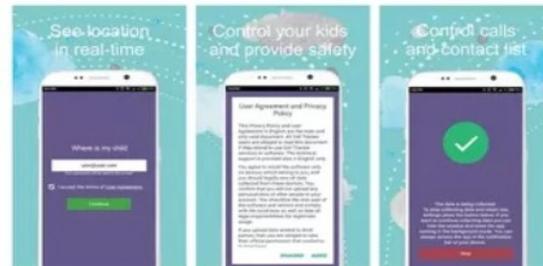
Add to Wishlist



**Mobile Tracking**  
AntWat Tools  
PEGI 3  
★★★★☆ 892

This app is compatible with your device.

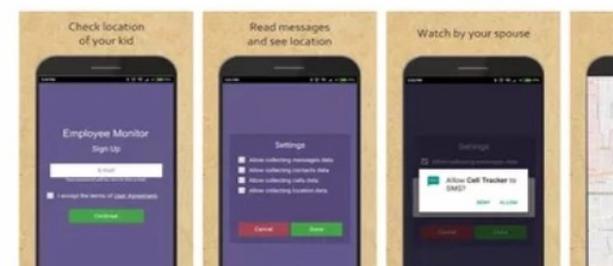
Add to Wishlist [Install](#)



**SMS Tracker**  
TheHar Tools  
PEGI 3  
★★★★☆ 2,865

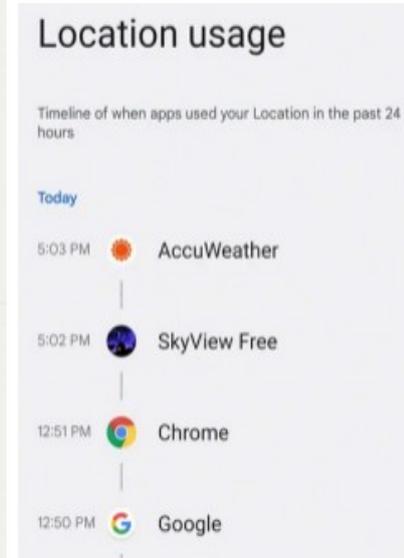
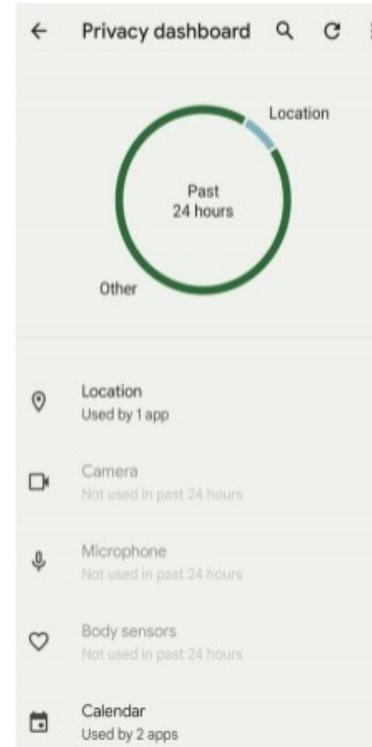
This app is compatible with your device.

Add to Wishlist [Install](#)



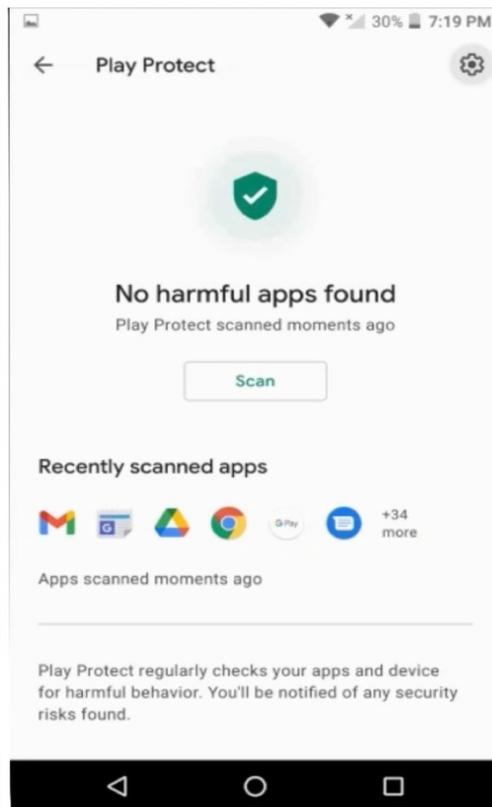
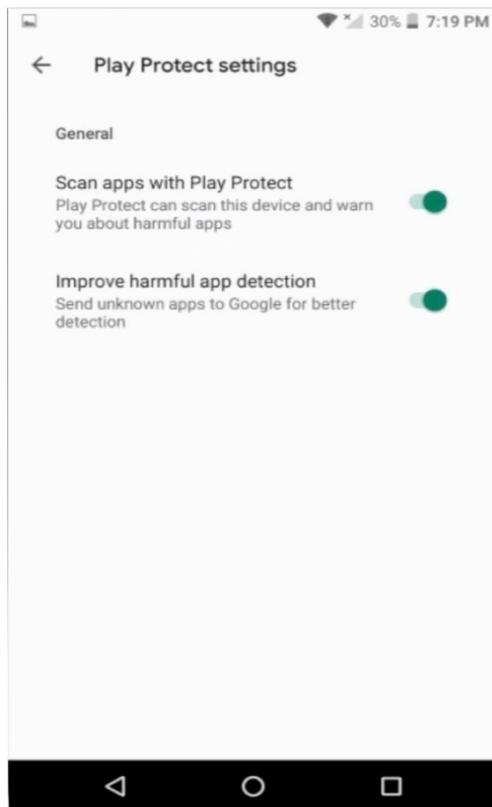
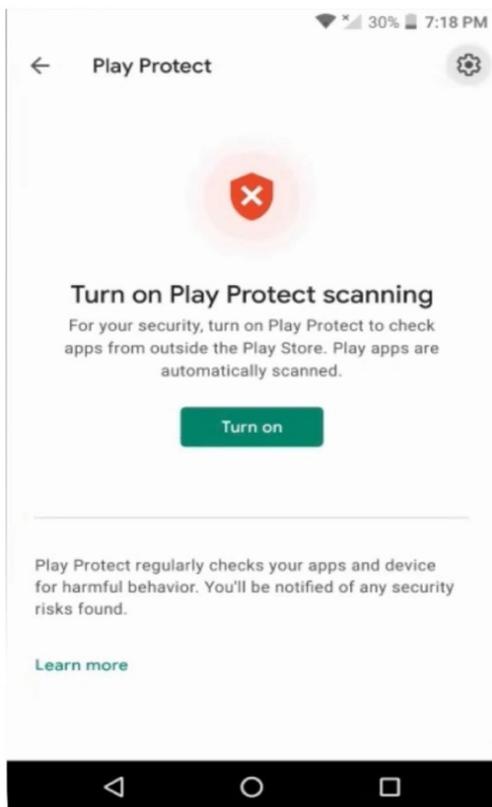
# Stalking Apps

- Gibt viele Stalking/ Family Apps
- Überwachen/ Kontrollieren andere Apps & Handy
- Android 12 & iOS 15: **Privacy Dashboard**
- Im Zweifel Handy zurücksetzen & Passwort ändern



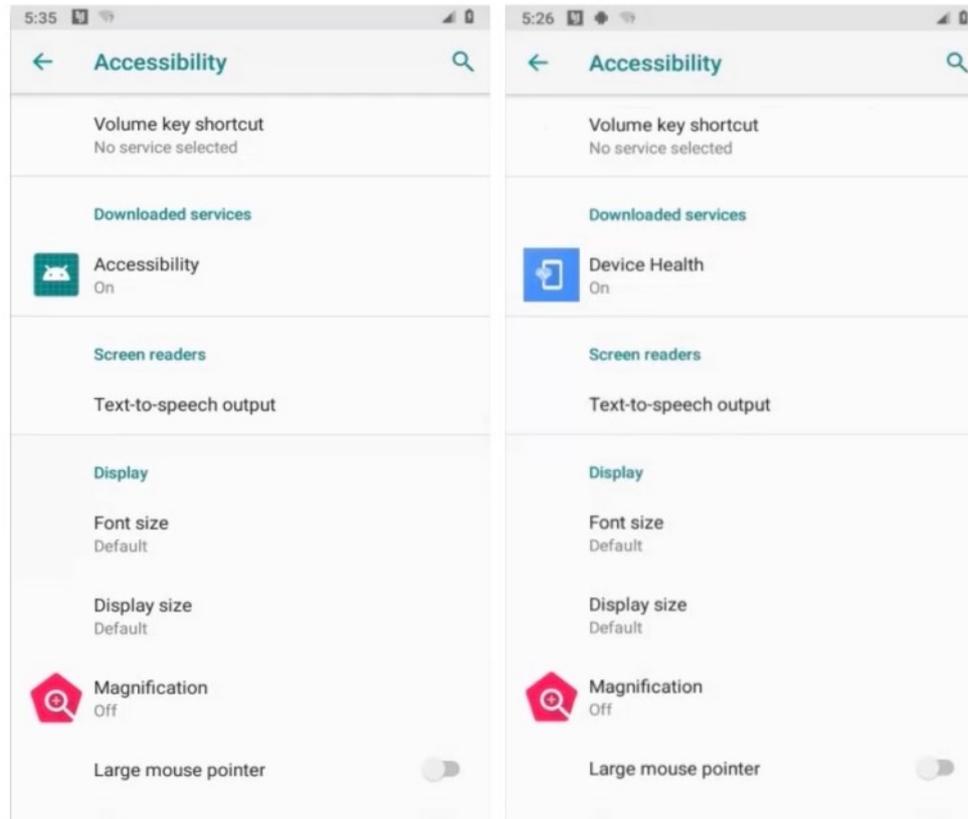
# Stalking Apps erkennen

## 1) Google Play Protect aktivieren



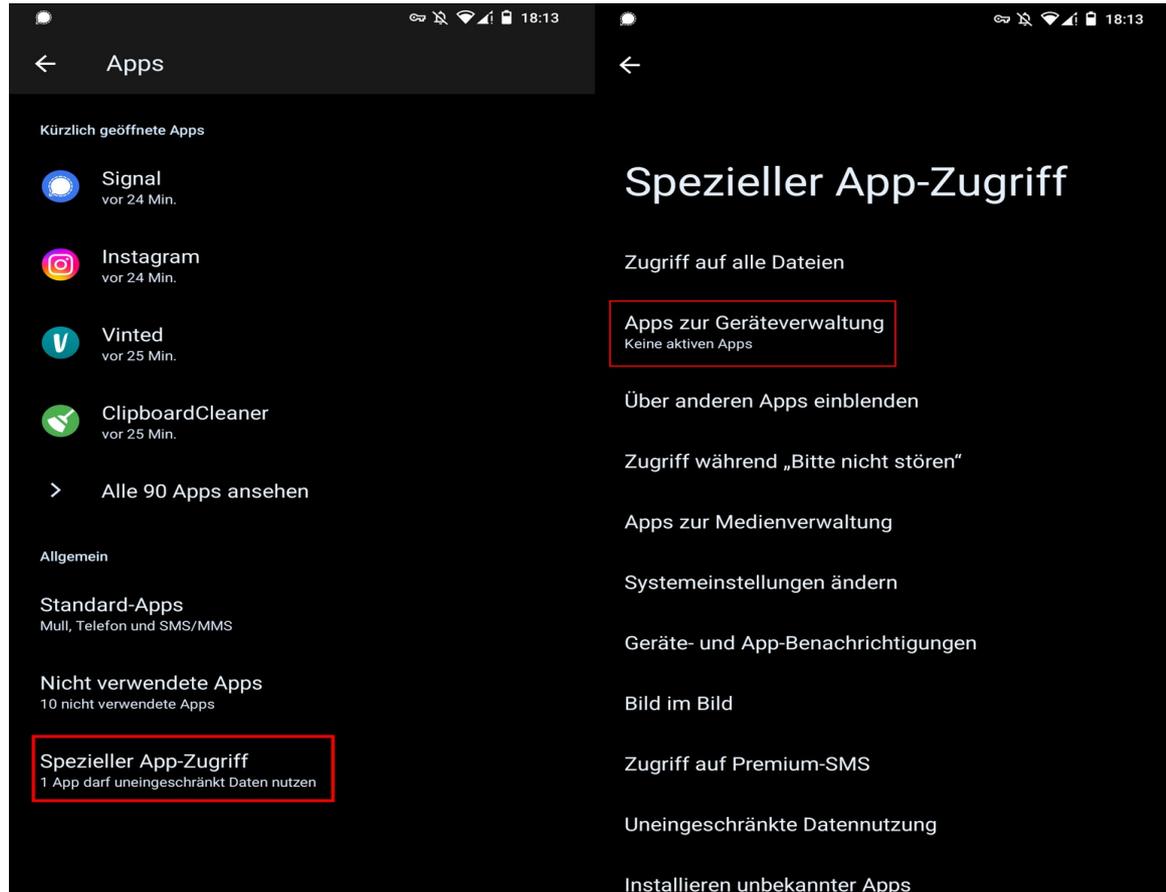
# Stalking Apps

## 2) Bedienungshilfen Einstellungen überprüfen



# Stalking Apps

## 3 ) Admin Apps & Apps mit speziellen Berechtigungen finden



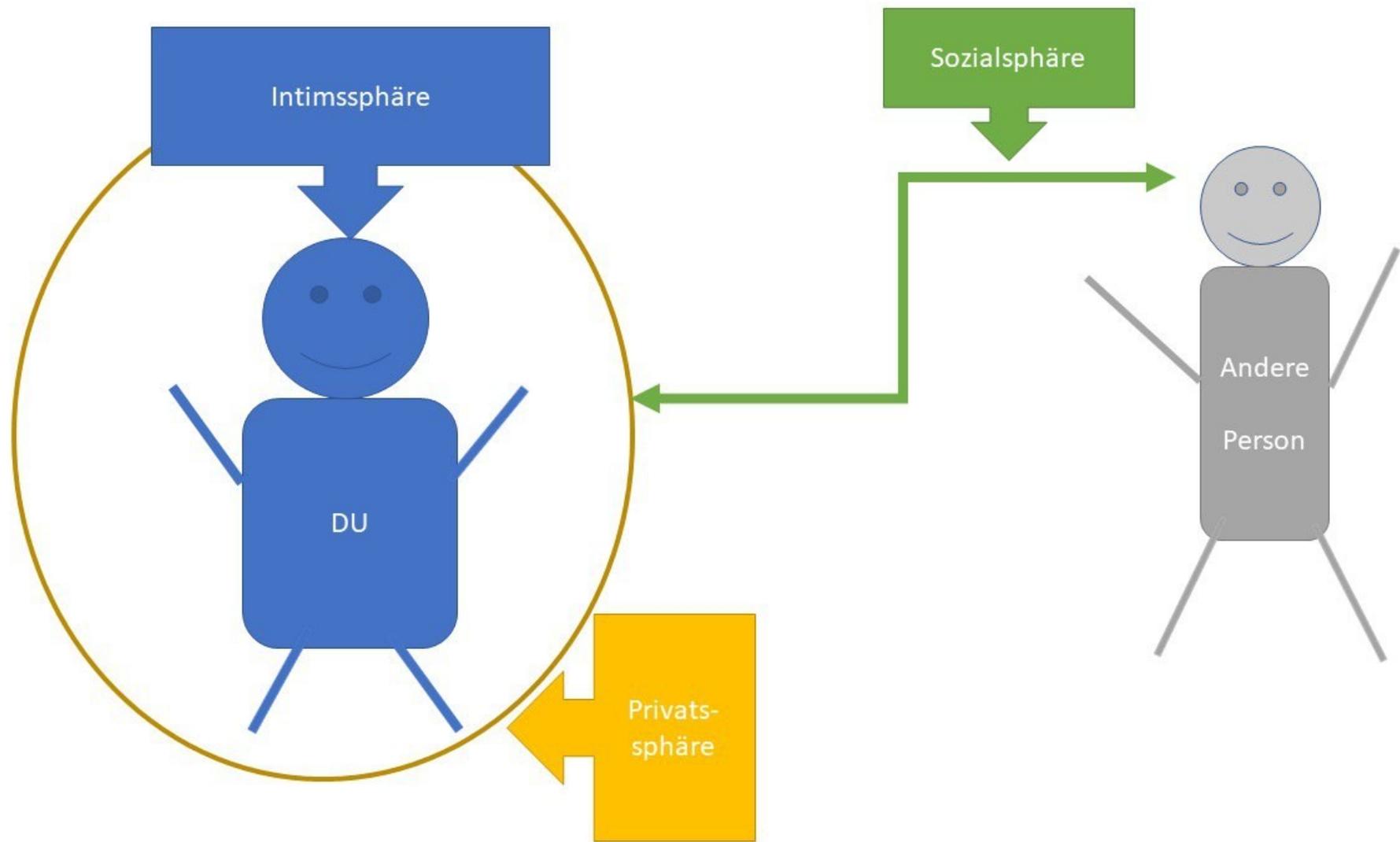
# Rechtliche Einordnung

# Vorab:

- **Wertung “rechtlich relevant” ≠ automatisch richtig!**
- Rechtlicher Weg kann für Betroffene schwer sein, ist nicht für alle der richtige Weg/ der gewünschte
- Hilfe von Strafverfolgungsbehörden sowie Gerichten manchmal leider letzter Weg für Betroffene

# Grundlagen

- Allgemeines Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG jeder Person



# Grundlagen

- Allgemeines Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG jeder Person
  - Recht auf informationelle Selbstbestimmung, Recht am gesprochenen Wort
- Recht am eigenen Bild aus KUG (Kunsturhebergesetz)

# “Rechtlich Relevant”

- Verletzung des Allgemeinen Persönlichkeitsrechtes
- Verletzung des Kunsturhebergesetzes (nicht konsensuales Verbreiten von Fotos)  
- § 33 KUG

**Recht: §§ 22 KUG**

- **Verletzung § 33 KUG**

**Bildnisse** dürfen **nur mit Einwilligung** des Abgebildeten **verbreitet** oder **öffentlich** zur Schau gestellt werden. (...)

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird **bestraft, wer entgegen den §§ 22, 23** ein Bildnis verbreitet oder öffentlich zur Schau stellt.

(2) Die Tat wird **nur auf Antrag verfolgt**.

# “Rechtlich Relevant”

- Strafbare Handlungen aus dem Strafgesetzbuch

(nicht abschließende Liste):

→ Gefährdendes Verbreiten personenbezogener Daten - § 126 a StGB

→ Ausspähen, Abfangen von Daten, Verbreitung, Vorbereitung dieses Handelns - §§ 202a, 202b, 202c, 202d StGB

→ Nötigung, Bedrohung, Beleidigung, Verleumdung - §§ 240, 241, 185, 186, 187 StGB

→ Unaufgefordertes Versenden pornographischer Inhalte - § 184 Nr. 6 StGB

→ Stalking - § 238 StGB

# Rechtliche Handlungsoptionen

	Außergerichtlich	Gerichtlich
Gegen den*die Täter*in	Abmahnung,  Strafbewehrte Unterlassungserklärung	Strafrechtlich Zivilrechtlich Gewaltschutz

# Rechtliche Handlungsoptionen

	Außergerichtlich	Gerichtlich
<b>Gegen den*die Täter*in</b>	Abmahnung,  Strafbewehrte Unterlassungserklärung	Strafrechtlich Zivilrechtlich Gewaltschutz
<b>Gegen Plattformanbieter*innen</b>	Beschwerde mit Ziel der Inhaltsentfernung	Zivilrechtlich

# Rechtliche Handlungsoptionen

<b>Zivilrechtlich Bürger*in gegenüber Bürger*in</b>	
Klage auf Schadensersatz, Unterlassen, (Folgen-)Beseitigung	
Einstweilige Sicherungsverfügung, Gewaltschutz	

# Rechtliche Handlungsoptionen

<b>Zivilrechtlich Bürger*in gegenüber Bürger*in</b>	<b>Strafrechtlich Staat gegenüber Bürger*in</b>
Klage auf Schadensersatz, Unterlassen, (Folgen-)Beseitigung	Anzeige, Anstoß der Strafverfolgung
Einstweilige Verfügungen, Gewaltschutz	Nebenklage

## Außergerichtlich

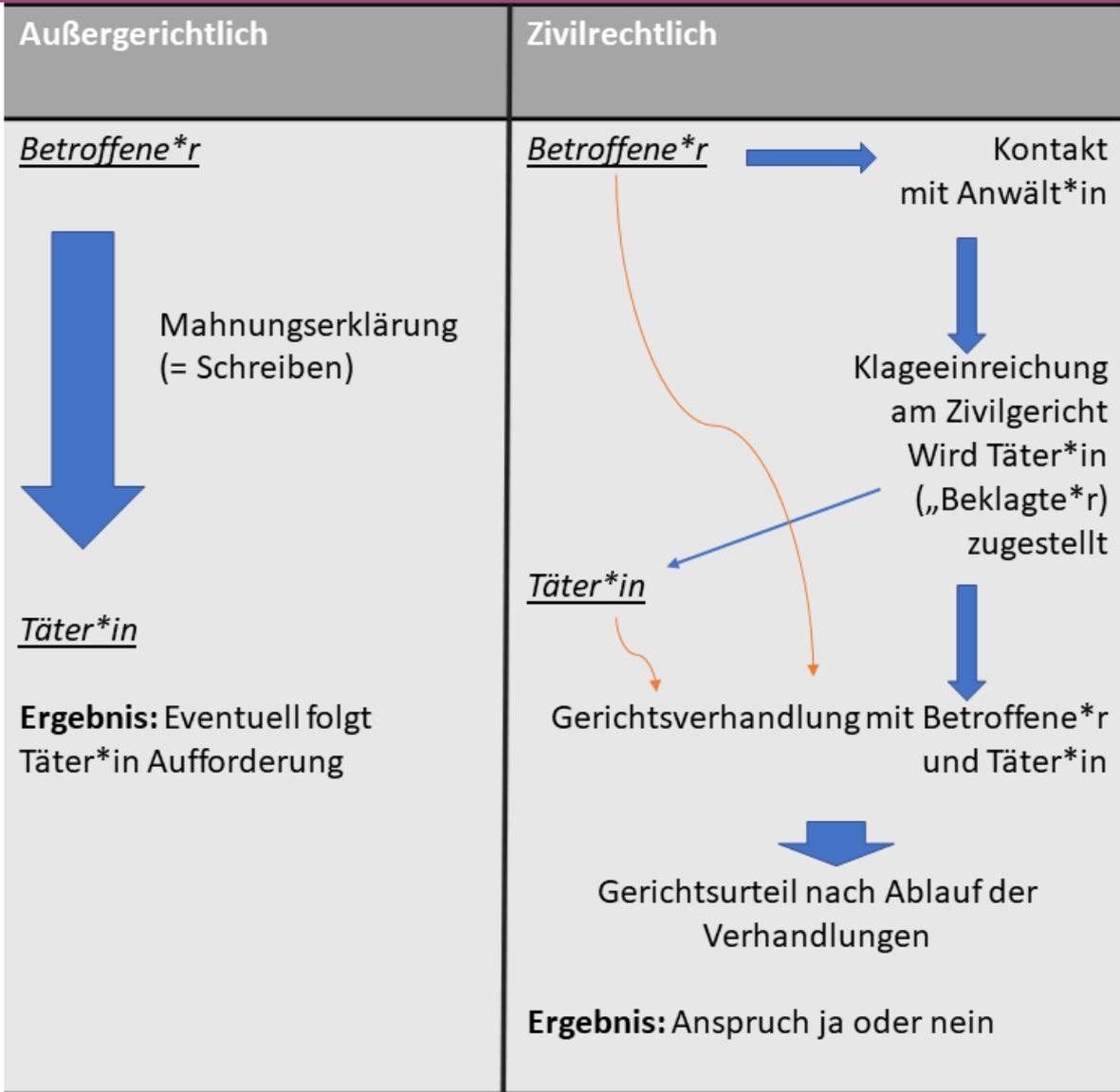
Betroffene\*r

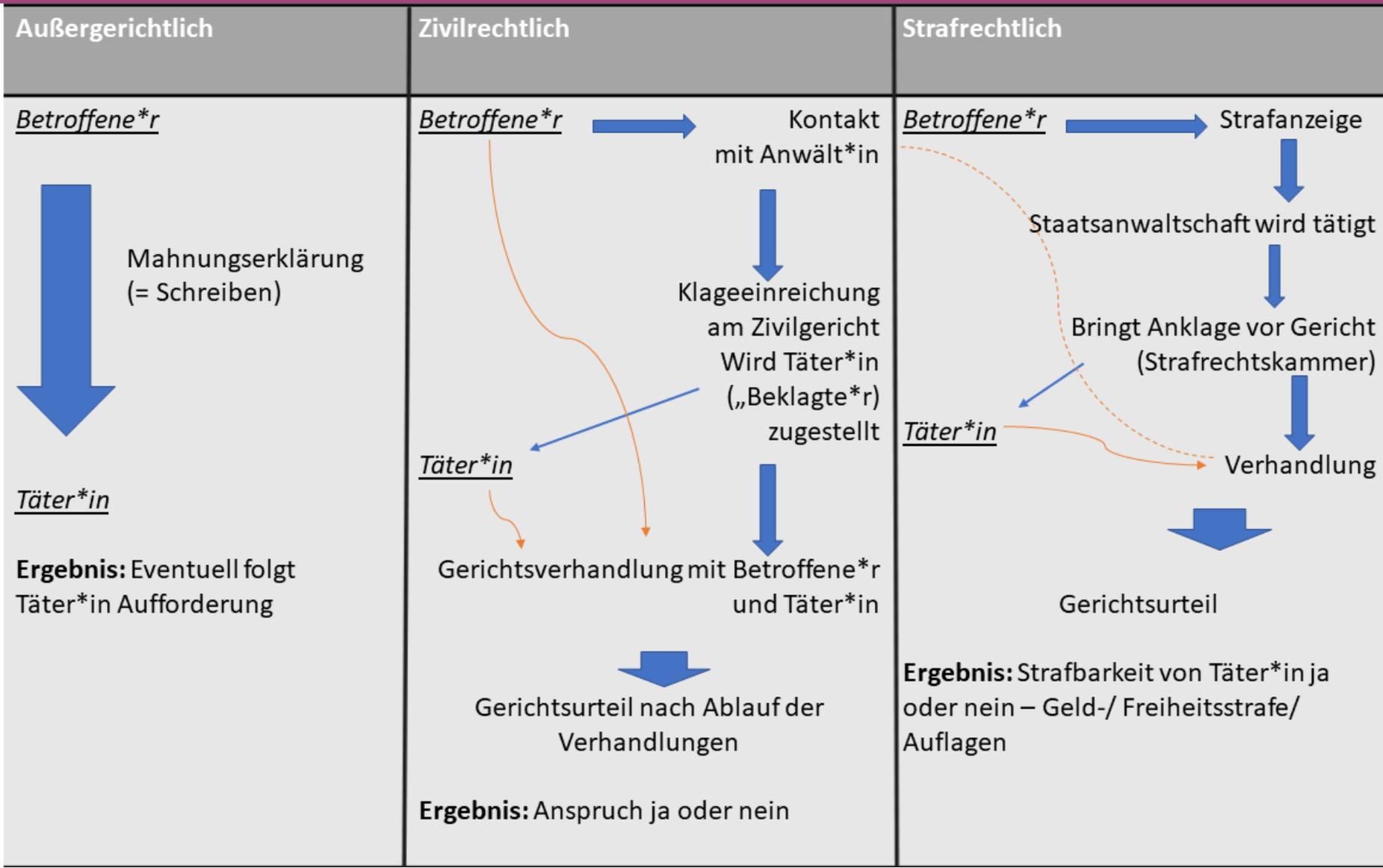


Mahnungserklärung  
(= Schreiben)

Täter\*in

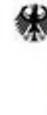
**Ergebnis:** Eventuell folgt  
Täter\*in Aufforderung





# Gewaltschutzverfahren

- „häusliche Gewalt“ = jegliche Gewalttaten, die bei in einem Haushalt lebenden Menschen vorkommen
- GewSchG § 1 Abs. 1 S. 3  
“Das **Gericht kann** insbesondere **anordnen**, dass der Täter es unterlässt,  
  
4. Verbindung zur verletzten Person, **auch unter Verwendung von Fernkommunikationsmitteln**, aufzunehmen”
- Auf Antrag am Familiengericht
- Maßnahmen maximal auf 6 Monate befristet



Bundesministerium  
für Familie, Senioren, Frauen  
und Jugend

Bundesministerium  
der Justiz und  
für Verbraucherschutz

## Mehr Schutz bei häuslicher Gewalt

Information zum Gewaltschutzgesetz

# Beispiel: Spionagesoftware

	Außergerichtlich	Zivilrechtlich	Strafrechtlich
Gegen Täter*in	Mahnung, nicht mehr Daten abzufangen; Unterlassungserklärung vorlegen	Anspruch Software zu deinstallieren, Daten zu löschen, Schadensersatz wie Schmerzensgeld (Sicherungsverfügung: ggf Geräte, auf denen Daten sind, sichern)	Strafbar = Ausspähen, Abfangen von Daten sowie die Verbreitung nach §§ 202a, 202b, 202d StGB
Gegen Plattformbetreiber*in	Gepostete Inhalte melden	Schadensersatz, wenn Prüfpflichten nicht nachgegangen	

# Beispiel: “Dickpics”/ Cyber Harassment

	Außergerichtlich	Zivilrechtlich	Strafrechtlich
<b>Gegen Täter*in</b>	Mahnung, Strafbewehrte Unterlassungs- erklärung	Unterlassen (Person muss Verhalten stoppen), Folgebeseitigung (Löschen von Kommentaren/Bildern), Schmerzensgeld	Beleidigung nach § 185 StGB Strafbar nach § 184 Nr. 6 StGB ( <a href="https://dickstinction.com/">https:// dickstinction.com/</a> )
<b>Gegen Plattform- betreiber*in</b>	Inhalt melden → Löschpflichten	Schadensersatz bei Verletzung der Prüfpflicht	

# Zivilrechtlicher vs. strafrechtlicher Prozess

- Bürger\*in klagt gegen Bürger\*in
- Verfahrensgestaltung selbst in der Hand
- **Probleme:**
  - Last Beweise selbst zu erbringen
  - nicht abschätzbare Verfahrensdauer
  - ggf selbst zu tragende Kosten
  - lange Verfahren
- Staat (Vertreten durch Staatsanwaltschaft) klagt gg. Bürger\*in
- Amtsermittlungsgrundsatz (Staatsanwaltschaft erbringt Beweise)
- **Probleme:**
  - Verfahrensgestaltung nicht in der Hand der Betroffenen → nur Möglichkeit der Nebenklage
  - Kontakt mit Polizei und Staatsanwaltschaft
  - oft Beweisschwierigkeiten
  - oft belastender Verfahrensablauf

# Prozessführung

- Beweissicherung
  - rechtssicher → siehe [hateaid.org](https://hateaid.org):
  - ggf URL speichern
  - Die NO STALK App des WEISSEN RINGS
- Zeug\*innen
  - zur Unterstützung
  - + Hilfe bei Erstellung von Beweisen
- Rechtliche und psychosoziale Beratung
- Prozesskostenhilfe

## Die NO STALK App

Die Stalking Tagebuch-App des WEISSEN RINGS

Dokumentieren Sie einfach alle Stalking-Vorfälle per Foto-, Video- sowie Sprachaufnahmen chronologisch und lückenlos mit Ihrem Smartphone (Betriebssystem: mindestens iOS 11 oder Android 4.4). Ihre Aufnahmen zählen bei der Polizei bzw. vor dem zuständigen Gericht als vollwertige Beweise! Die NO STALK App des WEISSEN RINGS unterstützt Sie dabei, aktiv und selbstbestimmt gegen Stalking vorzugehen.



**NO STALK App –  
Ab sofort in Ihren APP Stores verfügbar!**



# Betroffenen-/Opferrechte im Strafverfahren

- Möglichkeit der psychosozialen Prozessbegleitung
- Möglichkeit der Anwesenheit einer Vertrauensperson
- Adressdatenschutz
- Aufzeichnung von Vernehmungen
- Position der Nebenklage

# Ausblick:



Rechtsstaat kompakt

Themen

Ministerium

Presse

Service



Drucken

Seite teilen

## Eckpunkte für ein Gesetz gegen digitale Gewalt

### Gesetzgebungsverfahren

Entwurf

Letzte Aktualisierung

14. Juni 2023

Erscheinungsjahr

25. April 2023

Immer wieder werden Menschen im Netz massiv beleidigt und verleumdet oder im schlimmsten Fall wird dort ihr Leben bedroht. Für viele Betroffene ist es wichtig, dass solche Inhalte schnell gelöscht und die weitere Verbreitung verhindert werden.

Derzeit haben Betroffene aber oft nur unzureichende Möglichkeiten, ihre Rechte selbst durchzusetzen. Häufig scheitert die Durchsetzung ihrer Rechte bereits daran, dass es nicht gelingt, zügig und mit vertretbarem Aufwand Auskunft über die Identität des Verfassers bzw. der Verfasserin rechtswidriger Inhalte zu erlangen. Auch fehlt es an einem effektiven Instrument, um gegen den ständigen Missbrauch eines Nutzerkontos für Angriffe gegen eine andere Person vorzugehen.

Um künftig die private Rechtsdurchsetzung zu stärken, plant das Bundesministerium der Justiz ([BMJ](#)) ein Gesetz gegen digitale Gewalt vorzulegen. Zur Vorbereitung dieses Gesetzentwurfs hat das [BMJ](#) ein Eckpunktepapier erstellt.

^ [Details verbergen](#)

# Wo bleibt:

- Die Lösung auf kollektiver statt individueller Ebene
- Die Sensibilisierung für das Thema  
(und alle weiteren Formen digitaler Gewalt)
- Die Hilfe für Betroffene ausbauen
- Der Abbau von Hürden/ die Zugänglichkeit der Gerichte
- Stärkung von Schutzräumen



# Forderungen

- Öffentlichkeit herstellen
- Sensibilisierung: Digitale Gewalt im Nahfeld anerkennen & mitdenken
  - Behörden (Polizei, BSI)
  - Justiz
  - Plattformbetreiber\*innen
    - Apple & Google
    - Social Media Konzerne
- Forschung und Monitoring
  - Ausmaß abschätzen
  - besseres Verständnis
- Expertise & Ressourcen von Beratungsstellen auf- & ausbauen
- Kompetenzstellen für digitale Gewalt
- Spy-Apps verbieten

# Betroffene unterstützen

- vorsortieren von Nachrichten & Kommentaren
- Beweissicherung und Dokumentation
- Öffentlich solidarisieren (Counterspeech)
- Technische Hilfe
- gemeinsam Beratungsangebote (be-)suchen

# Hilfsangebote



FRAUEN GEGEN GEWALT E.V.

Transformative Gerechtigkeit & Kollektive  
Verantwortungsübernahme 10.10. 17 Uhr

Coding Art 11.10. 17 Uhr

Hands-On digitale Selbstverteidigung 12.10. 15 Uhr

FLINTA Workhop:  
Gender based digital violence 12.10. 17 Uhr

Wie studiere ich kritisch Jura? 12.10. 17 Uhr

Offenes Plenum AG Link 18.10. 19 Uhr

Offenes Plenum KJL 25.10. 19 Uhr

Folien, Anlaufstellen &  
weiterführendes Material:  
[ag-link.xyz/events](https://ag-link.xyz/events)

AG Link  
web: [ag-link.xyz](https://ag-link.xyz)  
instagram: [@ag.link\\_le](https://www.instagram.com/ag.link_le)  
mastodon: [link@systemli.social](mailto:link@systemli.social)  
email: [ag-link@riseup.net](mailto:ag-link@riseup.net)

KJL  
web: [kjlleipzig.noblogs.org](https://kjlleipzig.noblogs.org)  
instagram: [@akj.leipzig](https://www.instagram.com/akj.leipzig)  
email: [kjl@riseup.net](mailto:kjl@riseup.net)

