

Deepfakes erkennen, richtig reagieren, Betroffenen helfen

Stand: Oktober 2026

Hinweis: Die Rechtslage zu Deepfakes ändert sich gerade (Gesetzentwürfe, EU-Regeln). Bitte vor Veröffentlichung prüfen. Der Text ist keine Rechtsberatung.

1. FAQ: Wie erkenne ich Deepfakes?

Was ist ein Deepfake?

Ein mit KI erzeugtes oder manipuliertes Bild, Video oder Audio, das echt wirkt, aber Dinge zeigt oder sagt, die so nie passiert sind. Dazu zählen Face-Swaps, komplett generierte Personen und Stimmklone.

Woran erkenne ich Fälschungen im Bild und Video?

- Ränder von Gesicht, Haaren und Ohren flackern oder verschwimmen, besonders bei Kopfbewegungen.
- Zähne, Zunge, Brillen, Schmuck und Hände sehen unscharf oder unlogisch aus.
- Licht und Schatten passen nicht zur Umgebung. Die Hautstruktur wirkt zu glatt.
- Blinzeln, Mimik und Lippenbewegung stimmen nicht ganz mit dem Gesagten überein.
- Hintergrund, Text und Logos im Bild sind verzerrt.

Und bei Audio?

Auffällig sind eine monotone oder merkwürdig betonte Sprache, fehlende Atemgeräusche, ein „sauberer“ Hintergrund ohne Raumklang und seltsame Pausen. Bei Anrufen von angeblichen Verwandten oder Vorgesetzten gilt: auflegen und über eine bekannte Nummer zurückrufen. Eine Rückfrage mit einem vorher vereinbarten Codewort hilft ebenfalls.

Reicht der Blick auf Fehler?

Nein. Die Technik wird besser, und das Fehlen von Fehlern beweist keine Echtheit. Prüfe deshalb immer auch den Kontext.

Welche Kontext-Checks helfen?

- **Quelle:** Wer hat es zuerst veröffentlicht? Gibt es ein Original, einen vollständigen Clip oder eine Berichterstattung seriöser Medien?
- **Rückwärtssuche:** Google Lens, TinEye oder Bing Visual Search zeigen, ob ein Bild schon früher in anderem Zusammenhang auftauchte.

- **Plausibilität:** Passt die Aussage zur Person? Soll das Material vor allem Wut, Angst oder Empörung auslösen? Das ist ein Warnsignal.
- **Faktenchecks:** Prüfe, ob dpa-Faktencheck, Correctiv, Tagesschau-Faktenfinder oder BR24 #Faktenfuchs den Fall schon behandelt haben.
- **Herkunftsnachweise:** Manche Kameras und KI-Dienste hinterlegen Metadaten oder „Content Credentials“ (C2PA). Sie sind ein Hinweis, aber kein Beweis, denn sie fehlen oft oder werden beim Hochladen entfernt.

Helfen automatische Erkennungstools?

Nur bedingt. Sie liefern Wahrscheinlichkeiten, keine Gewissheit, und irren sich in beide Richtungen. Als Ergänzung sind sie brauchbar (z. B. das Browser-Plugin InVID-WeVerify), ein Urteil allein darauf zu stützen ist es nicht.

2. Ich glaube, einen Deepfake erkannt zu haben: Was tun?

1. **Nicht teilen, auch nicht „zur Warnung“.** Jede Weiterverbreitung vergrößert den Schaden.
2. **Quelle und Original suchen** (siehe Checks oben). Im Zweifel erst einmal abwarten.
3. **Beitrag melden.** Alle großen Plattformen haben Meldewege für manipulierte Inhalte und Identitätsmissbrauch. Nach dem Digital Services Act müssen sie Meldungen prüfen.
4. **Betroffene informieren.** Das gilt für Personen, die im Material zu sehen oder zu hören sind. Schicke ihnen den Link, aber nicht die Datei selbst.
5. **Bei Wahl- oder Politikbezug** die Redaktion oder einen Faktencheck-Dienst informieren, mit Link und Fundstelle.
6. **Bei sexualisierten Inhalten, besonders wenn Minderjährige betroffen sein könnten:** nicht weiterleiten, nicht herunterladen und keine Screenshots anfertigen, denn schon Besitz und Weitergabe können strafbar sein. Melde den Fund bei der Plattform, der Internet-Beschwerdestelle (internet-beschwerdestelle.de) oder der Polizei.
7. **Bei Betrugsversuchen** (z. B. Stimmklon, gefälschte Videoanrufe) Polizei und gegebenenfalls die eigene Bank informieren.

3. Ich bin selbst Opfer eines Deepfakes: Was tun?

Gemeinsame Sofortschritte (bei allen Fällen)

- **Beweise sichern:** Screenshots mit sichtbarer URL, Datum und Uhrzeit, Nutzernamen des Verbreiters und Kommentare. Notiere, wer es dir gezeigt hat. Bei Minderjährigen oder

sexualisiertem Material mit Minderjährigen: nicht selbst sichern, sondern sofort die Polizei einschalten.

- **Plattform melden** und Löschung verlangen. Nenne dabei ausdrücklich, dass es sich um eine Fälschung und eine Verletzung deiner Persönlichkeitsrechte handelt.
- **Nicht allein auseinandersetzen.** Antworte nicht auf Provokationen, sondern hole dir Unterstützung (siehe Liste unten).
- **Fristen beachten:** Für Antragsdelikte wie üble Nachrede und Beleidigung gilt nach unserem Kenntnisstand eine Strafantragsfrist von drei Monaten ab Kenntnis der Tat und des Täters.

A) Üble Nachrede / Verleumdung

Gemeint ist ein Deepfake, der dir etwas Ehrenrühriges in den Mund legt oder unterstellt (z. B. rassistische Äußerungen, strafbares Verhalten).

- **Strafrecht:** Üble Nachrede (§ 186 StGB), Verleumdung (§ 187 StGB, wenn der Täter wissentlich lügt) und Beleidigung (§ 185 StGB) kommen in Betracht. Für Personen des politischen Lebens sieht § 188 StGB zusätzliche Regeln vor.
- **Anzeige:** Bei der Polizei oder über die Online-Wache Niedersachsen, mit den gesicherten Beweisen.
- **Zivilrecht:** Anwaltliche Abmahnung auf Unterlassung (Persönlichkeitsrecht, §§ 823, 1004 BGB). Bei schweren Verletzungen kann zusätzlich Geldentschädigung in Betracht kommen.
- **Medien:** Berichten Medien auf Grundlage des Fakes, können Gegendarstellung, Richtigstellung oder Widerruf infrage kommen.
- **Öffentlichkeit:** Eine kurze, sachliche Richtigstellung auf den eigenen Kanälen kann sinnvoll sein. Beziehe dabei wenn möglich Belege für die Fälschung ein, ohne das Material zu verlinken.

B) Falsche Tatsachenbehauptungen

Gemeint sind Fakes, die dir erfundene Aussagen, Handlungen oder Aufrufe zuschreiben, ohne unbedingt ehrenrührig zu sein (z. B. Falschzitat, gefälschter Spendenaufruf, vorgetäuschte Videobotschaft).

- **Rechtlicher Rahmen:** Bewusst oder erwiesen unwahre Tatsachenbehauptungen genießen nach ständiger Rechtsprechung keinen Schutz der Meinungsfreiheit. Du kannst Unterlassung, Berichtigung und Löschung verlangen.

- **Strafrecht:** Je nach Fall kommen Fälschung beweiserheblicher Daten (§ 269 StGB), Betrug (§ 263 StGB, etwa bei gefälschten Aufrufen oder Stimmklon-Anrufen) oder Identitätsmissbrauch in Betracht.
- **Wirtschaftlicher Schaden:** Dokumentiere ihn (entgangene Aufträge, Kündigungen, Folgekosten). Er ist für Schadensersatzansprüche wichtig.
- **Betrug im Umfeld:** Wenn Dritte betroffen sind (Familie, Kunden, Spender), warne sie direkt.

C) Sexualisierte Gewalt (sexualisierte Deepfakes)

Gemeint sind Fakes, die dich in sexuellen Situationen zeigen, etwa durch Face-Swaps auf pornografisches Material oder „Nudify“-Apps. Das ist bildbasierte sexualisierte Gewalt. Die Schuld liegt allein bei den Tätern.

1. **Du musst nichts alleine entscheiden.** Eine Beratungsstelle hilft dir, in deinem Tempo vorzugehen. Das gilt auch, wenn du noch nicht anzeigen willst.
2. **Verbreitung stoppen:** Melde den Inhalt bei Plattformen und Hostern. Bei Suchmaschinen kannst du die Entfernung aus den Ergebnissen beantragen (es gibt eigene Formulare für nicht einvernehmliche intime Bilder). Mit **StopNCII.org** können Betroffene Bilder „hashen“ lassen, ohne sie hochzuladen, damit teilnehmende Plattformen sie blockieren. Minderjährige können **Take It Down** (takeitdown.ncmec.org) nutzen.
3. **Beweise sichern:** Ein Screenshot mit URL, Datum und Account ist für die Anzeige wichtig. Lass dich dabei von einer Beratungsstelle unterstützen oder bitte eine Vertrauensperson. Bei Minderjährigen: Nichts selbst speichern, sondern direkt die Polizei einschalten.
4. **Anzeige:** Dafür kommen je nach Einzelfall u. a. § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs), § 185 StGB, das Recht am eigenen Bild (§§ 22, 33 KUG) und bei Minderjährigen die Vorschriften zu Kinder- und Jugendpornografie (§§ 184b, 184c StGB) in Betracht. Ob rein synthetische Deepfakes bereits vollständig erfasst sind, ist umstritten. Ein eigener Straftatbestand (§ 201b StGB) wurde vorgeschlagen, bitte den aktuellen Stand prüfen. Fachberatungsstellen und Opferanwälte kennen die aktuelle Lage.
5. **Prozessbegleitung und Nebenklage:** Betroffene können sich anwaltlich vertreten lassen und bei bestimmten Delikten Prozessbegleitung bekommen. Die Beratungsstellen vermitteln das.
6. **Umfeld informieren:** Wenn Schule, Arbeitgeber oder Verein betroffen sind, kannst du gezielt informieren und Schutzmaßnahmen verlangen.
7. **Psychische Entlastung:** Scham, Angst und Kontrollverlust sind normale Reaktionen. Du darfst dir Unterstützung holen, auch wenn es „nur ein Fake“ ist.

Anlaufstellen bei sexualisierter Gewalt durch Deepfakes (Region Hannover)

Notfall: Polizei 110.

Fachberatung in Hannover

- **Frauennotruf Hannover** (Frauen und Mädchen ab ca. 16 Jahren): Goethestraße 23 (Eingang Leibnizufer), 30169 Hannover, Telefon 0511 332112, info@frauennotruf-hannover.de. Die Beratung umfasst auch digitale Gewalt, sexuelle Belästigung und Stalking.
- **Violetta** (Mädchen und junge Frauen, die von sexuellem Missbrauch betroffen sind): Wöhlerstraße 42, 30163 Hannover, Telefon 0511 855554.
- **Frauenberatung Hannover** (Gewalt und krisenhafte Lebenssituationen): Marienstraße 61, 30171 Hannover, Telefon 0511 323233.
- **FMGZ, Frauen- und MädchenGesundheitsZentrum**: Escherstraße 10, 30159 Hannover, Telefon 0511 3004546.
- **Anstoß** (Jungen und männliche Jugendliche): spezialisierte Fachberatungsstelle in Hannover, Telefon 0511 123 589 11, auch Onlineberatung.
- **Männerbüro Hannover** (Männer über 27): Beratung bei sexualisierter Gewalt, Telefon 0511 123 589 0, Termine nach telefonischer Vereinbarung.

In der Region Hannover (außerhalb der Stadt)

- **AWO-Frauenberatung Barsinghausen**: Marktstraße 33, 30890 Barsinghausen, Telefon 05105 6613550.
- **AWO-Frauenberatung Lehrte** (zuständig auch für Burgdorf, Sehnde, Uetze): Goethestraße 8, 31275 Lehrte, Telefon 05132 823434.
- **valeo** (Region Hannover): Telefon 0511 616-22160, valeo@region-hannover.de. Bitte vor Veröffentlichung kurz klären, wie das Angebot beschrieben werden soll.
- Weitere Stellen listet die Region Hannover in ihrer Übersicht „Beratung und Unterstützung gegen häusliche und sexualisierte Gewalt“ auf hannover.de.

Bundesweit (telefonisch und online, auch aus der Region nutzbar)

- **Hilfetelefon „Gewalt gegen Frauen“**: 116 016, rund um die Uhr, anonym, mehrsprachig.
- **Hilfetelefon Sexueller Missbrauch**: 0800 22 55 530.

- **Nummer gegen Kummer** (Kinder und Jugendliche): 116 111.
- **Weißer Ring** (Opfertelefon): 116 006.
- **HateAid** (Beratung bei digitaler Gewalt, Unterstützung bei Anzeigen und Prozesskosten):
hateaid.org.
- **Internet-Beschwerdestelle**: internet-beschwerdestelle.de.

Inhalte und rechtliche Voraussetzungen können sich ändern.