820/A(E)
vom 23.04.2026 (XXVIII. GP)

ENTSCHLIESSUNGSANTRAG

der Abgeordneten Meri Disoski, Süleyman Zorba, Freundinnen und Freunde

betreffend Missbrauchs-Deepfakes bekämpfen - Gesetzeslücken rasch und effektiv schließen

BEGRÜNDUNG

Es dauert wenige Minuten und kostet nur ein paar Euro bis man(n) ohne besondere technische Vorkenntnisse mit generativen KI-Modellen Deepfake-Videos und -Bilder erstellen kann. Der Kreativität werden hierbei kaum mehr Grenzen gesetzt – krimineller Energie und Missbrauch leider ebenso wenig. So zeigt sich, dass in den vergangenen Wochen und Monaten eine Flut von sexualisierten Gewaltdarstellungen über User:innen hereingebrochen ist: Frauen, die erschossen werden, Frauen, die gegen Wände geschlagen werden, Teenager, die stranguliert werden – alles kommentiert mit Millionen Lach-Emojis einer offenbar völlig verrohten und empathiefreien Community. Befeuert wird das über „soziale" Netzwerke – so hat Google zuerst einen Youtube Kanal namens „WomanShotAI" ungehindert groß werden lassen, bevor er dann doch endlich gesperrt wurde.[1]

Missbräuchliche Deepfakes, die natürliche Personen kompromittieren, in pornografischen Kontext setzen oder ihnen geschlechtsspezifische, sexualisierte Gewalt antun, werden zu einem zunehmenden Problem. In einem im Jahr 2023 erstellten Report von Security Hero wurden 95.820 Deepfake-Videos untersucht.[2] 98% dieser Videos waren Deepfake-Pornos. In diesen pornografischen Deepfakes waren 99 % der Opfer weiblich. Zuletzt hat der Missbrauchsfall der deutschen Moderatorin und Schauspielerin Collien Fernandes auf erschütternde Weise neuerlich vor Augen geführt, wie notwendig ein politisch und gesetzlich schärferes Vorgehen gegen Deepfakes und sexualisierte digitale Gewalt ist. Ihr Ex-Mann wird beschuldigt, Fake-Profile in sozialen Netzwerken erstellt und darüber unter anderem gefälschte pornografische Bildaufnahmen unter Fernandes Namen an zahlreiche Männer verschickt zu haben.[3]

Es ist unumgänglich, rasche Reformschritte gegen Gewalt an Frauen im digitalen Raum zu setzen – schon jetzt hinken Gesetze den gefühlt täglichen technischen Neuerungen hinterher. Das heißt Betroffene haben einerseits zu wenig Möglichkeiten,

---

[1] https://www.derstandard.at/story/3000000295389/traenen-der-angst-wie-ki-videos-zum-ventil-fuer-gewaltfantasien-werden

[2] https://www.securityhero.io/state-of-deepfakes/#key-findings; https://www.euronews.com/next/2023/10/20/generative-ai-fueling-spread-of-deepfake-pornography-across-the-internet; https://www.derstandard.at/story/3000000295714/nutzer-verbreiten-ki-generierte-videos-in-denen-frauen-stranguliert-werden

[3] https://orf.at/stories/3424689/

sich wirksam vor Gewalt zu schützen, und andererseits kaum juristische Handhabe, nachdem sie Gewalt erfahren mussten. Im Jahr 2025 hat Video- und Bild-KI einen massiven Sprung gemacht – nahezu im Monatsrhythmus gab es aufsehenerregende Neuerungen. Mittlerweile ist die KI-Videoproduktion massentauglich — auch ohne Kamera, Beleuchtung oder Schnittkenntnisse. Aus einer simplen Texteingabe entstehen auf Knopfdruck realistische Videos mit Dialog, Musik, Soundeffekten und exakten Lippenbewegungen. Ein Foto reicht, um ein KI-Video von einer Person zu generieren, ohne dass diese jemals dabei mitgewirkt oder ihre Zustimmung gegeben hätte.

Angesichts dieser rasanten technischen Entwicklung ist es dringend notwendig, auch das rechtliche Instrumentarium zum Schutz vor missbräuchlicher Verwendung von Bild- und Video-KI umfangreich und wirksam nachzuschärfen. Unter Grüner Regierungsbeteiligung wurde hierzu bereits im Jahr 2022 der Aktionsplan Deepfake[4] ausgearbeitet. Seitdem hat die technische Entwicklung aber einen enormen Sprung getan und es offenbaren sich neue erhebliche Angriffsszenarien und Missbrauchspotenziale. Darum besteht bei der Regulierung von Deepfakes zum Schutz von Betroffenen umgehender Handlungsbedarf. Auch die EU-Richtlinie 2024/1385 *zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt* verpflichtet Österreich, Formen digitaler Gewalt – darunter ausdrücklich nicht-einvernehmliche sexualisierte Deepfakes – sowie die Androhung solcher gezielt unter Strafe zu stellen[5].

Rechtliches Instrumentarium nachschärfen

Aktuell haben Opfer von missbräuchlichen Deepfake-Videos eine Reihe zivilrechtlicher Ansprüche – angefangen bei der DSGVO über das Recht am Bild des § 78 UrhG bis hin zu medienrechtlichen Ansprüchen. Für die Durchsetzung dieser Ansprüche sind jedoch teure zivilrechtliche Verfahren erforderlich, bei denen Opfer mit Gerichts- und Anwaltskosten in Vorlage gehen müssen. Die Deepfake-Urheber und -Betrüger ausfindig zu machen, bleibt dabei – zu Unrecht – ebenfalls den Opfern überlassen. Damit wird eine Rechtsdurchsetzung massiv erschwert, in den meisten Fällen gar verunmöglicht. Denn wer sich derartige zivilrechtliche Schritte nicht leisten kann, bleibt auf der Strecke.

Problematisch ist insbesondere auch, dass sowohl das Recht am Bild gem. § 78 UrhG als auch medienrechtliche Ansprüche immer auf eine Veröffentlichung der Deepfakes abstellen. Lediglich die DSGVO untersagt schon die Verwendung von personenbezogenen Daten (also von Fotos oder Videos) für die Erstellung von Deepfakes.

Gerade auch im Bereich des Strafrechts ergibt sich im Hinblick auf nicht-konsensuale Deepfake-Pornos eine gefährliche Lücke. Der Cybermobbing-Straftatbestand des §107c StGB stellt für eine Strafbarkeit darauf ab, dass strafbare Handlungen für eine größere Zahl von Menschen wahrnehmbar sind, und das für eine längere Zeit. Selbst

[4] https://www.bmi.gv.at/bmi_documents/2779.pdf
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401385

wenn derartige Deepfakes nicht veröffentlicht werden, bleibt das Videomaterial aber in KI-Anwendungen gespeichert und fließt noch dazu in das weitere KI-Training ein. Im Gegensatz zum Cybermobbing-Straftatbestand des § 107c StGB stellt § 207a StGB bereits die Erstellung von bildlichem sexual-bezogenem Kindesmissbrauchsmaterial und bildlichen sexualbezogenen Darstellungen minderjähriger Personen unter Strafe. Somit ist auch schon die Erstellung von Kindesmissbrauchs-Deepfakes strafbar. Bei volljährigen Opfern entfällt dieser Schutz vor Erstellung missbräuchlicher Deepfake-Pornos oder KI-generierter Gewaltdarstellungen. Nicht sachgerecht ist insbesondere, dass bei missbräuchlichen Deepfake-Pornos Strafbarkeit erst bei längerer Wahrnehmbarkeit eintritt. Derartige Deepfakes haben virales Potenzial und können somit binnen weniger Minuten Opfer massiv treffen. Hier wäre es notwendig nachzuschärfen.

Eine Strafbarkeit nach dem Pornographiegesetz für die Erstellung missbräuchlicher Deep-Fake-Pornografie setzt Gewinnabsicht voraus; die Verbreitung derartiger Darstellungen ist nur bei wissentlichem Zugänglichmachen für einen größeren Kreis von Personen unter 16 Jahren strafbar. Auch damit wird Opfern von Deepfake- Pornos somit nicht unbedingt geholfen.

Auch die Möglichkeit des Privatbeteiligtenanschlusses im Strafverfahren bzw. ein beschleunigtes Mandatsverfahren gem. § 549 ZPO bleibt im Zusammenhang mit Deep Fakes auf bestimmte Sachverhalte beschränkt, die in der Regel bereits eine Übermittlung bzw. Veröffentlichung erfordern.

Mitverantwortlichkeit von KI-Anbietern und Online-Plattformen

Dringender Handlungsbedarf besteht weiters bei der Klärung der Mitverantwortlichkeit von KI-Anbietern, deren Software die Erstellung missbräuchlicher Deepfake-Darstellungen erst ermöglicht. KI-Anbieter müssen verpflichtet werden, in dieser hochsensiblen Software Safeguards, also technische Sicherheitsmaßnahmen, vorzusehen, die eine Erstellung missbräuchlicher und gewaltsamer Deepfakes von reellen Personen wirksam unterbindet. Tun sie das nicht, und das, obwohl ihnen das massive Missbrauchspotenzial bewusst ist, müssen KI-Anbieter für die Handlungen ihrer User:innen künftig endlich vollends mitverantwortlich sein – und zwar sowohl in zivilrechtlicher als auch in strafrechtlicher Hinsicht. Denn KI-Anbieter nehmen den Schaden, den Opfer missbräuchlicher Deepfakes erleiden, derzeit oft billigend in Kauf.

Aktuell sorgen mit KI erstellte Gewaltvideos, in denen (fiktive) jugendliche Mädchen stranguliert werden, für Schlagzeilen. Berichten zufolge wurden diese Videos massenhaft über die Online-Plattform X verbreitet. Es ist davon auszugehen, dass es sich hier um Verhetzung iSd § 283 StGB handelt. Trotz Meldung der Accounts an X wurde die Entfernung abgelehnt. Auch über TikTok fanden diese Gewaltvideos massive Verbreitung.[6] Einmal mehr zeigt dieser Fall, dass Social Media Plattformen

[6] https://www.derstandard.at/story/3000000295714/nutzer-verbreiten-ki-generierte-videos-in-denen-frauen-stranguliert-werden

konsequent zur Mitverantwortung gezogen werden müssen: Grundsätzlich müssten Plattformen schon von vornherein sicherstellen, dass missbräuchliches Deepfake-Material gar nicht hochgeladen werden kann. Werden erst Meldungen an die Plattform erforderlich, ist die Rechtsverletzung tatsächlich schon passiert.

Die Untätigkeit von Plattformen bei der – insbesondere auch proaktiven! – Bekämpfung derartigen Gewaltmaterials muss haftungsbegründend sein. Mit der Zunahme von missbräuchlichen Deepfakes wird das Problem untätiger Online-Plattformen eine noch größere Dimension erlangen – und damit zu einer Bedrohung für noch mehr Frauen und Mädchen werden.

Ein wachsendes Problem ist hier auch die sogenannte „Sextorsion", bei der Betrüger unter falschen Voraussetzungen sexualisierte Bilder von Nutzer:innen, oft von Teenagern, erlangen und diese dann erpressen. Hier gilt es, Opfer zu unterstützen – juristisch, vor allem aber auch psychologisch. Opfern muss die Wahrnehmung ihrer Rechte erleichtert werden.

Es besteht somit dringender politischer Handlungsbedarf auf vielen Ebenen:

- Die strafrechtlichen Möglichkeiten, sich gegen sexualisierte Missbrauchs-Deepfakes zur Wehr zu setzen, müssen effektiv nachgeschärft werden.
- Hierbei ist Sorge zu tragen, dass eine rechtliche Verschärfung nicht erst ab Zeitpunkt der Veröffentlichung, sondern auch bei Erstellung derartiger Inhalte eintritt.
- Die Mitverantwortung von Anbietern von KI-Programmen sowie von Online-Plattformen, über die derartige missbräuchliche Inhalte erstellt und/oder verbreitet werden, und die keine hinreichenden Sicherheitsschranken setzen, um diesen Missbrauch proaktiv zu verhindern und den Missbrauch somit in Kauf nehmen, ist zu schärfen.
- Opferhilfe, psychosoziale und juristische Prozessbegleitung sind auszubauen.
- Exekutivbeamt:innen, Staatsanwält:innen und Richter:innen sind im Hinblick auf die neuen Herausforderungen, die missbräuchliche Deepfakes und Online-Gewalt stellen, zu schulen.
- Die bundesweite Etablierung sogenannter Cyberambulanzen ist einzuleiten, um die gerichtsfeste Sicherung digitaler Beweismittel sowie ausführliche fallspezifische Beratungen für Gewaltbetroffene gewährleisten zu können.
- Awareness-Kampagnen müssen vor allem Jugendliche aufklären, welche Gefahren mit dem Online-Stellen von eigenen Fotos verbunden sind.
- Die in der KI-Verordnung 2024/1689 von der EU gesetzlich zwingend vorgesehene KI-Behörde ist unverzüglich in Österreich einzurichten.

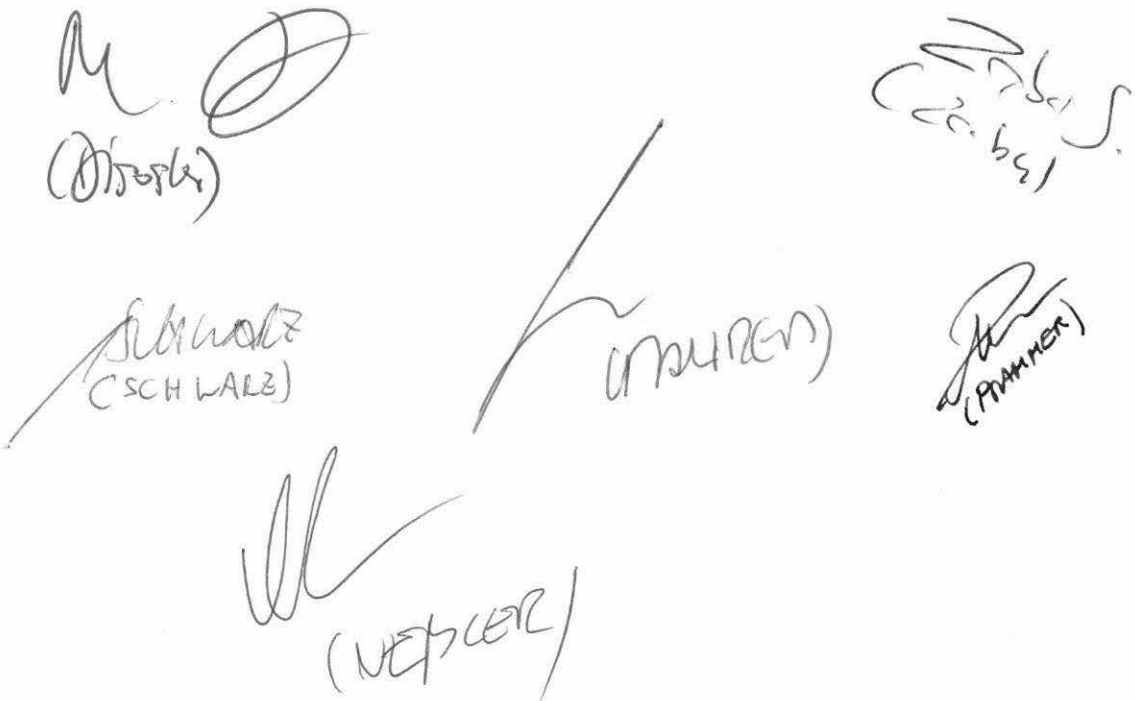
Die unterfertigenden Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

„Die Bundesregierung, insbesondere die Bundesministerin für Frauen, Wissenschaft und Forschung und die Bundesministerin für Justiz, wird ersucht, dem Nationalrat umgehend ein Maßnahmenpaket zur Bekämpfung missbräuchlicher Deepfakes zuzuleiten. Dieses Maßnahmenpaket muss einerseits rechtliche Instrumentarien nachschärfen und die Anspruchswahrnehmung erleichtern, andererseits Schulungen, Awareness-Kampagnen, zusätzliche Möglichkeiten im Bereich von Opferhilfe und Prozessbegleitung sowie die verpflichtende Einrichtung der nationalen KI-Behörde und zusätzlicher Cyberambulanzen vorsehen."

In formeller Hinsicht wird die Zuweisung an den Gleichbehandlungsausschuss vorgeschlagen.



	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-04-23T20:03:33+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	