ENTSCHLIESSUNGSANTRAG

der Abgeordneten Meri Disoski, Süleyman Zorba, Freundinnen und Freunde

betreffend Schluss mit Warten: JETZT vor Deepfakes schützen!

eingebracht im Zuge der Debatte zum Bericht des Gleichbehandlungsausschusses über den Antrag 796/A(E) der Abgeordneten Sabine Schatz, Mag. Dr. Juliane Bogner-Strauß, Henrike Brandstötter, Kolleginnen und Kollegen betreffend Schaffung rechtlicher Konsequenzen bei missbräuchlicher Verwendung von Deepfakes (507d.B.) (TOP 11)

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. Missbräuchliche Deepfakes, die natürliche Personen kompromittieren, in pornografischen Kontext setzen oder ihnen geschlechtsspezifische, sexualisierte Gewalt antun, sind als Problem in der Mitte unserer Gesellschaft angekommen.

Doch sind es vor allem Frauen und Mädchen, die Opfer von Missbrauchs-Deepfakes werden: Security Hero hat 2023 95.820 Deepfake-Videos untersucht.[1] 98% dieser Videos waren Deepfake-Pornos. In diesen pornografischen Deepfakes waren wiederum 99 % der Betroffenen weiblich. Spätestens nach dem Mitte März 2026 bekannt gewordenen Missbrauchsfall der deutschen Moderatorin und Schauspielerin Collien Fernandes[2] muss allen bewusst sein, wie dringend notwendig ein politisch und gesetzlich schärferes Vorgehen gegen Deepfakes und sexualisierte digitale Gewalt ist.

Es ist zwingend notwendig, unverzüglich und rasch Reformschritte gegen Gewalt an Frauen im digitalen Raum zu setzen – schon jetzt hinken Gesetze den gefühlt täglichen technischen Neuerungen hinterher. Von Deepfakes betroffene Frauen können schlicht und einfach nicht darauf warten, dass diese Bundesregierung zunächst die strafrechtliche Rechtslage evaluiert, um erst zu einem unbestimmten

[1] 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

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

Zeitpunkt in der Zukunft – wenn überhaupt – „gegebenenfalls gesetzliche Änderungen auszusprechen“[3].

Betroffene haben aktuell einerseits zu wenig Möglichkeiten, sich wirksam vor Gewalt zu schützen, und andererseits kaum juristische Handhabe, nachdem sie Gewalt erfahren mussten. Ein Foto reicht, um ein KI-Video von einer Person zu generieren, ohne dass diese jemals dabei mitgewirkt oder ihre Zustimmung gegeben hätte. Ist ein solches Deepfake-Video erst einmal veröffentlicht und verbreitet, stehen die Geschädigten allein auf weiter Flur im Kampf, dieses wieder von diversen Online-Plattformen zu entfernen. Angesichts dieser rasanten technischen Entwicklung ist es also 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 ernstzunehmende Missbrauchspotenziale. Darum besteht bei der Regulierung von Deepfakes zum Schutz von Betroffenen umgehender Handlungsbedarf. Das hat die EU zuletzt auch im Digital Omnibus zu KI[5] aufgegriffen und wird KI-Systeme ohne effektive Sicherheitsmaßnahmen gegen eine Generierung nicht-konsensualer sexualisierter Bild- oder Videoinhalte künftig verbieten (Novelle zu Art 5 KI-Verordnung). Das ist freilich nur ein Teil der notwendigen Maßnahmen. So gilt es auch auf individueller Ebene das rechtliche Instrumentarium gegen die Nutzung grundsätzlich zulässiger KI für die Erstellung missbräuchlicher Deepakes zu schärfen. Dementsprechend verpflichtet die EU-Richtlinie 2024/1385 *zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt* Österreich, Formen digitaler Gewalt – darunter ausdrücklich nicht-einvernehmliche sexualisierte Deepfakes (sowie die Androhung solcher) – gezielt unter Strafe zu stellen[6]. Diese Bundesregierung muss jetzt endlich aus ihrem Ankündigungsmodus und ihrer Tatenlosigkeit herauskommen und effektive Schutzmaßnahmen vor digitaler Gewalt auf die versprochene „Fast Lane“[7] bringen.

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

---

[3] https://www.parlament.gv.at/dokument/XXVIII/A/796/fname_1750412.pdf
[4] https://www.bmi.gv.at/bmi_documents/2779.pdf
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9247_2026_INIT
[6] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401385
[7] Regierung will missbräuchliche Deepfakes verbieten und digitale Gewalt strenger bestrafen - Inland - derStandard.at › Inland

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. Problematisch ist auch, dass sowohl das Recht am Bild gem. § 78 UrhG als auch medienrechtliche Ansprüche immer auf eine Veröffentlichung der Deepfakes abstellen.

Gerade auch im Bereich des Strafrechts ergibt sich im Hinblick auf nicht-einvernehmliche sexualisierte Deepfakes 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 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 bildlichen sexualbezogenen Darstellungen minderjähriger Personen unter Strafe. Somit ist auch schon die Erstellung von Kindesmissbrauchs-Deepfakes strafbar. Bei volljährigen Opfern entfällt jedoch dieser Schutz vor Erstellung. Nicht sachgerecht ist insbesondere, dass bei missbräuchlichen Deepfake-Pornos Strafbarkeit erst bei längerer Wahrnehmbarkeit an eine größere Zahl von Menschen eintritt. Hier muss juristisch dringend nachgeschärft werden.

Eine Strafbarkeit nach dem Pornographiegesetz für die Erstellung missbräuchlicher Deep-Fake-Pornografie setzt wiederum Gewinnabsicht voraus; die Verbreitung derartiger Darstellungen ist nur bei wissentlichem Zugänglichmachen für einen größeren Kreis von Personen unter 16 Jahren strafbar. Auch damit ist Opfern von Deepfake-Pornos unzureichend geholfen. Ebenso bleibt die Möglichkeit des Privatbeteiligtenanschlusses im Strafverfahren bzw. ein beschleunigtes Mandatsverfahren gem. § 549 ZPO 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

Auch die zivil- und strafrechtliche Mitverantwortlichkeit von KI-Anbietern, deren Software die Erstellung missbräuchlicher Deepfakes erst ermöglicht, muss verschärft werden. Der Digital-Omnibus zu KI sieht künftig ein Verbot von Nudifier Apps vor. Das ist ein wichtiger regulatorischer Schritt, der aber von einer Mitverantwortlichkeit für missbräuchliche Deepfakes begleitet werden muss: KI-Anbieter müssen verpflichtet werden, Safeguards, also funktionierende technische Sicherheitsmaßnahmen, vorzusehen, die eine Erstellung missbräuchlicher und gewaltsamer Deepfakes von reellen Personen wirksam unterbinden. Tun sie das nicht, müssen KI-Anbieter für die Handlungen ihrer User:innen künftig endlich vollends mitverantwortlich sein – sowohl zivilrechtlich als auch strafrechtlich.

Wesentlich ist es, auch Plattformen, über die Deepfakes verbreitet werden, in die Pflicht zu nehmen: Grundsätzlich sollen Plattformen schon von vornherein sicherstellen müssen, dass missbräuchliches Deepfake-Material gar nicht hochgeladen und verbreitet werden kann. Werden erst Meldungen an die Plattform erforderlich, ist die Rechtsverletzung tatsächlich schon passiert. Insbesondere die Untätigkeit von Plattformen bei der 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.

Gewaltbetroffene müssen zudem bei sogenannter Sextorsion, bei der Betrüger unter falschen Voraussetzungen sexualisierte Bilder von Nutzer:innen erlangen und diese dann erpressen, besser unterstützt werden – juristisch wie psychologisch.

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. Der KI-Omnibus sieht in der geänderten Fassung des Art 77 KI-Verordnung die Zusammenarbeit von Grundrechtsbehörden und nationalen Marktüberwachungsbehörden ausdrücklich vor. So eine Zusammenarbeit ist faktisch unmöglich, wenn Österreich weiterhin die nationalen Behörden gem. Art 77 KI-Verordnung nicht benennt.

Die unterfertigenden Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

„Die Bundesregierung, insbesondere der Bundeskanzler, die Bundesministerin für Frauen, Wissenschaft und Forschung und die Bundesministerin für Justiz, wird aufgefordert, umgehend ein Maßnahmenpaket zur Bekämpfung missbräuchlicher Deepfakes mit den in der Begründung beschriebenen Inhalten vorzulegen und die zuständigen nationalen Behörden gem. Art 70 KI-Verordnung einzurichten."