578/A(E)
vom 19.11.2025 (XXVIII. GP)

ENTSCHLIESSUNGSANTRAG

der Abgeordneten Süleyman Zorba, Freundinnen und Freunde

betreffend entschlossenes Vorgehen gegen böswillige, betrügerische und irreführende Deepfakes - Mitverantwortung von Plattformen

BEGRÜNDUNG

Wenn Armin Assinger in einem Video erzählt, wie er mit einem geheimen Investment-Trick über 2 Millionen Euro verdient hat[1], wenn Magnus Brunner auf einer gefälschten Bundesschatz-Seite dazu auffordert, persönliche Daten und Kontoinformationen einzugeben[2] oder wenn Gerhard Karner in einem Videochat um Spenden für Lösegeldzahlungen im Zusammenhang mit Geiselnahmen bittet[3], dann sind das alles böswillige Deepfakes.

Deepfake-Phishing-Betrug, bei dem KI-generierte Stimmen und Videos zum Einsatz kommen, wird immer schwieriger zu erkennen und zeigt massive Zuwachszahlen von prognostizierten 900% pro Jahr.[4] Davon betroffen sind nicht nur natürliche Personen, auch Unternehmen können so diskreditiert oder Opfer von Deepfake-Betrug werden. Im Jahr 2024 waren 49 % der Unternehmen von Audio- und Video-Deepfakes betroffen.[5] Das European Parliamentary Research Service führt in einem Briefing vom Juli 2025 aus, dass im Jahr 2024 die Verwendung von generativen KI-basierten Deepfakes um 118 % zugenommen hat.[6] Das war 2024.

Video- und Bild-KI hat in den vergangenen Wochen und Monaten eine extrem schnelle technische Entwicklung durchgemacht – KI-generierte Inhalte sind jetzt kaum mehr von echten Bildern und Videos zu unterscheiden. Damit hat sich das Gefährdungspotenzial von irreführenden, täuschenden und betrügerischen Deepfakes vervielfacht.

Während die Rechtsdurchsetzung im Zusammenhang mit derartigen Deepfakes oft daran scheitert, dass deren Urheber nicht ausfindig gemacht werden können, spielt

---

[1] https://www.konsumentenfragen.at/konsumentenfragen/Digitalisierung/Digitalisierung/Deepfake-Videos-fuehren-zu-Investitionsbetrug.html#
[2] https://www.bmf.gv.at/presse/pressemeldungen/2024/juni/phishing-deep-fake-video.html
[3] https://help.orf.at/stories/3231801/
[4] https://keepnetlabs.com/blog/deepfake-statistics-and-trends
[5] https://trustpair.com/blog/fraud-report-2025-press-release/#:%7E:text=In%202024%2C%20the%20use%20of,amplify%20payment%20fraud%20this%20year.
[6] https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI%282025%29775855_EN.pdf

die Verbreitung über Social Media eine enorme Rolle und führt zu einem erheblichen Schädigungspotenzial.

Erst vor kurzem hat ein Bericht aufgedeckt, dass Meta pro Jahr wissentlich rund 15 Millionen Scam-Werbungen, also betrügerische Werbungen, an User:innen ausspielt und damit offenbar allein im Jahr 2024 16 Milliarden Dollar umgesetzt hat. Das sind 10% des gesamten Jahresumsatzes.[7] Angesichts dieser Umsätze wird somit offenbar auch Betrug billigend in Kauf genommen: Trotz Kenntnis über diese Sachverhalte hat Meta Investitionen in automatisierte Scam-Detection unterlassen.

Einmal mehr zeigt sich somit, dass Social Media Plattformen zur Mitverantwortung gezogen werden müssen. Grundsätzlich müssten Plattformen schon von vornherein sicherstellen, dass betrügerisches Deepfake-Material nicht hochgeladen werden kann (Art 34, 35 Digital Services Act). Tatsächlich wird aber offenkundig aus monetären Interessen Betrug gerade nicht verhindert und somit die Schädigung von User:innen, Unternehmen und Opfern, deren Konterfei für die Generierung derartigen Deepfake-Betrugs herangezogen werden, bewusst in Kauf genommen. Dieses Verhalten von Plattformen muss haftungsbegründend sein und mit abschreckenden Strafen geahndet werden.

Neben betrügerischen Aktivitäten sind Deepfakes insbesondere auch geeignet, politisch Stimmung zu machen, Wahlen zu beeinflussen und Politiker:innen gefälschte Inhalte zu unterstellen. Vollständig gefälschte Reden sind schon heute Realität, wie etwa Videos von Donald Trump oder Barack Obama zeigen. Damit stellen Deepfakes ein erhebliches innenpolitisches Risiko dar.

Das hat auch die österreichische Bundesregierung erkannt und im Regierungsprogramm an verschiedenen Stellen folgende Maßnahmen angekündigt:

- *Die verstärkte Bekämpfung von Desinformation und des missbräuchlichen Einsatzes von KI im digitalen Raum wird weiter forciert. Insbesondere wird der Kampf gegen Deepfakes intensiviert, um die Integrität demokratischer Prozesse zu schützen.*
- *Desinformationen, Deepfakes und andere Aktivitäten, die die Grundprinzipien unserer Demokratie gefährden, müssen genauso konsequent bekämpft und reguliert werden.*
- *Es braucht insbesondere eine Verstärkung der Verantwortung bei Moderations- und Löschungsverpflichtungen. Wer digitale Räume bereitstellt, trägt auch die Pflicht, sie sicher zu halten.*

Bislang sind diesen Ankündigungen aus dem Regierungsprogramm noch keine faktischen Aktivitäten gefolgt. Gerade angesichts der rasanten Entwicklung von

[7] https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

Deepfake-Technologie und der daraus resultierenden Schäden ist hier weiteres Zuwarten nicht hinzunehmen.

Die unterfertigenden Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

„Die Bundesregierung wird ersucht, dem Nationalrat ein Maßnahmenpaket für die Bekämpfung böswilliger Deepfakes vorzulegen, das insbesondere auch verschärfte Regelungen für Online-Diensteanbieter enthält, die ihren Verpflichtungen zur Detektion, Moderation, Kennzeichnung und Löschung von böswilligen Deepfakes nicht nachkommen."

In formeller Hinsicht wird die Zuweisung an den Ausschuss für Wissenschaft, Forschung und Digitalisierung vorgeschlagen.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-11-19T19:36:08+01:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	