

## **ENTSCHLISSUNGSANTRAG**

Gemäß § 26 GOG-NR

der Abgeordneten Mag Philipp Schrangl, Hermann Brückl  
und weiterer Abgeordneter  
betreffend Identitätsdiebstahl sowie auch Deepfakes als eigene Straftatbestände

Kriminelle nutzen gestohlene Daten im Netz für allerlei Einkäufe und Verträge auf Kosten ihrer Opfer.

### **Die Formen von Identitätsmissbrauch**

Die Marktwächterteams in den zuständigen Schwerpunkt-Verbraucherzentralen haben in ihren Segmenten zahlreiche Beispiele für den Missbrauch von Verbraucherdaten gefunden:

- In etlichen Fällen nutzen Unbefugte die Daten von Verbrauchern, um beispielsweise **Hörbücher oder Software** einzukaufen. Die erworbenen Hörbücher oder Lizenzschlüssel für Software können dann von Kriminellen weiterverkauft werden.
- Auch **kostenpflichtige Streaming-Dienste** werden vielfach in fremden Namen gebucht, wie die Fälle im Frühwarnnetzwerk zeigen.
- In anderen Fällen nutzen Unbekannte die Daten von Verbrauchern, um Abos für teure **Online-Dating-Portale oder Premium-Mail-Konten** abzuschließen.
- Ebenso liegen Fälle von **Abbuchungen über die Handyrechnung** vor, weil Verbraucher erst ihre Handynummer an einen angeblichen Facebook-Freund weitergegeben haben, dann eine PIN auf ihr Handy erhielten, mit der sie unwissentlich eine Zahlung freigaben und diese ebenfalls ihrem angeblichen Facebook-Freund mitteilten.
- Eine Vielzahl an Fällen bezieht sich auch auf **Einkäufe bei Onlinehändlern**, die im Namen der ahnungslosen Verbraucher vorgenommen werden.
- In einigen Fällen berichten Verbraucher, dass Dritte beispielsweise ihre **Payback-Punkte eingelöst oder ihre Kundenkonten auf Marktplätzen vermutlich gehackt** und über ihr Profil eingekauft haben.
- Unerwartete Vertragsabschlüsse für **Mobilfunkverträge** zählen ebenfalls zum Identitätsdiebstahl. Verbraucher erfuhren von dem Betrug durch Willkommensschreiben als auch Zahlungsaufforderungen der Firmen.

Persönliche Daten können unter anderem über Phishing-E-Mails oder Firmen-Datenlecks in die Hände von Kriminellen gelangen. Für Betroffene bleibt häufig unklar, wie die Täter an ihre digitalen Identitäten gelangt sind und in welchem Umfang diese nun genutzt oder weitergegeben werden.<sup>1</sup>

---

<sup>1</sup> <https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750>

## Deep-Fakes

„Der Begriff „**Deepfake**“ setzt sich aus den englischen Begriffen „deep learning“ und „fake“ zusammen. „**Deep learning**“ bezeichnet dabei **Methoden des maschinellen Lernens** – also den Einsatz von **Künstlicher Intelligenz** – und „fake“ lässt sich mit **Fälschung, Imitation oder Schwindel** übersetzen. Somit vermittelt bereits die Wortbedeutung einen guten Eindruck, was Deepfakes sind.

Denn hierbei handelt es sich um die **Fälschung oder Veränderung von medialen Inhalten mithilfe von Künstlicher Intelligenz**. Dabei wird eine Software regelrecht darauf trainiert, die **charakteristischen Merkmale** einer Person mithilfe von **vorhandenen Bild- oder Tonmaterial** zu erkennen und diese dann in ein bereits vorhandenes Video zu **übertragen**.

Damit das **Endergebnis** auch möglichst realistisch erscheint, benötigt die Software möglichst **viele Daten**. Aus diesem Grund werden für Deepfakes vor allem **Prominenten oder Politikern** genutzt, denn von diesen gibt im Internet **viel Material**. Darüber hinaus beanspruchen aufwändige Bearbeitungen eine **hohe Rechenleistung** und sind verhältnismäßig **zeitaufwändig**. Allerdings entwickelt sich die Technologie immer weiter und mittlerweile gibt es auch schon **kostenlose Apps**, mit denen selbst **Laien** innerhalb von kürzester Zeit **Deepfakes erzeugen** können. Abhängig von den verwendeten **Inhalten** und der **Art der Veränderung** lassen sich vor allem folgende **Formen von Deepfakes** unterscheiden:

- Face Swapping
- Voice Swapping
- Body Puppetry

Beim **Face Swapping** (dt. Gesichtertausch) handelt es sich um die bekannteste Form der Deepfakes. Dabei werden **Gesichter** in Videos durch die Gesichter anderer Personen **ersetzt**. Dadurch lässt sich zum Beispiel simulieren, dass ein **anderer Schauspieler** die Hauptrolle in einem Film übernommen hätte oder bereits **verstorbene Personen** mithilfe von altem Filmmaterial zumindest **auf der Leinwand wieder zum Leben erwachen**. Allerdings wird diese Methode auch dazu verwendet, um die Gesichter von Schauspielerinnen in **Pornofilme** einzubauen.

Mit der richtigen Deepfake-Software ist es darüber hinaus auch möglich, die **Stimme** einer Person zu **rekonstruieren**. Durch das **Voice Swapping** (dt. Stimmentausch) lassen sich Politikern irgendwelche **Worte in den Mund legen**. Aber auch in der Wirtschaft kann diese Technik ein Problem werden. Denn unter Umständen können **Betrüger** Audioaufnahmen mit der Stimme von führenden Angestellten erzeugen und dadurch **telefonisch die Überweisung von Geldbeträgen anordnen**. Es ist außerdem möglich, einzelne **Bewegungen** oder sogar **komplette Bewegungsabläufe** bei einem Video auf eine andere Person übertragen. Diese Form des Deepfakes wird als **Body Puppetry** (dt. „Körper-Marionettentheater“) bezeichnet.<sup>2</sup>

Die Erstellung von Deepfakes ist juristisch nicht ganz unproblematisch. Allerdings fehlt es bislang an konkreten Vorschriften oder auch Urteilen, die sich explizit mit dieser Technik beschäftigen.

---

<sup>2</sup> <https://www.anwalt.org/deepfakes/>

Die unterfertigten Abgeordneten stellen daher folgenden

**ENTSCHLIESSUNGSANTRAG:**

Der Nationalrat wolle beschließen:

„Die Bundesregierung, insbesondere die Bundesministerin für Justiz und der Bundesminister für Inneres, wird ersucht, dem Nationalrat eine Regierungsvorlage, die eigene Strafbestimmungen für „Identitätsdiebstahl“ sowie auch „Deepfakes“ und begleitend dazu einen personellen sowie technischen Ausbau der Cyber-Spezialisten bei Polizei und Justiz zum Inhalt hat, zuzuleiten.“

In formeller Hinsicht wird die Zuweisung an den Justizausschuss vorgeschlagen.

Alois Kraus  
(ALLOIS KRAUS)

  
CARLSBAVER

  
(SCHRAG)

  
(BRÜCK)

  
(CHVORN)

