

---

**365/A(E) XXVII. GP**

---

**Eingebracht am 27.02.2020**

**Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.**

## **ENTSCHLIESSUNGSANTRAG**

### **der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen betreffend Entwicklung einer Strategie zur Thematik und Risiken von Deepfakes**

Bei Deepfake-Technologien handelt es sich um eine Kombination von Deep Learning Algorithmen mit Audio- bzw. Videobearbeitungssoftware. Damit wird es zunehmend einfacher, täuschend echte Video- und Audio-Dateien von Menschen zu erstellen und ihnen Aussagen in den Mund zu legen oder sie bei Handlungen zu zeigen, die diese nie getätigt haben. Derzeit konzentrieren sich diese Fälschungen noch auf Personen der Öffentlichkeit, von denen ausreichend Bild- und Tonmaterial vorhanden ist. Aufgrund der allgegenwärtigen Verwendung von Smartphones in Verbindung mit der Speicherung von Foto- und Audiodateien in angreifbaren Clouds bzw. in den Sozialen Medien steigt jedoch auch das Risiko für Privatpersonen, Opfer von Deepfakes zu werden.

Fortschritte im Bereich des Deep Learnings ermöglichen bereits heute ein hohes Niveau an Qualität und Glaubwürdigkeit. Mimik, Gestik und Stimme wirken zunehmend realer. Deepfakes können von Laien mittlerweile oft nicht mehr von echten Video- und Audiodateien unterschieden werden. Gefälschte Bilder, Videos und Tonaufnahmen werden so zu Fake News, die um die Welt gehen können. Aufgrund rasanter Fortschritte im Bereich von Künstlicher Intelligenz ist davon auszugehen, dass Deepfakes in naher Zukunft noch an Qualität gewinnen werden. In Kombination mit der mittlerweile recht einfachen Verfügbarkeit solcher Technologien, etwa über Apps, nehmen auch die Verbreitungsmöglichkeiten zu.

Deepfakes von Schlüsselpersonen in der Politik oder in der Wirtschaft bergen ein erhebliches innenpolitisches Risiko. Im Falle von Unternehmen besteht die Gefahr gezielter Marktmanipulation durch den Einsatz von gefälschtem Video- und Bildmaterial, das unwahre Aussagen von führenden Mitarbeiter\_innen von Unternehmen zeigt. Gefälschte Audio- und Videoaufnahmen bergen außerdem politische Risiken, etwa wenn sie politische Schlüsselfiguren zeigen und sich rasend schnell über das Internet und Soziale Medien verbreiten. Vollständig gefälschte Reden von Politiker\_innen sind bereits Realität, wie etwa Videos von Donald Trump oder Barack Obama zeigen. Auf lange Sicht könnte durch Deepfakes ein signifikanter Vertrauensverlust in politische und mediale Institutionen entstehen. Zusätzlich können Pri-

**Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.**

vatpersonen durch diese Technologie sehr leicht Opfer von Rufschädigung, Erpressung oder Identitätsdiebstahl werden.

Seitens der Politik besteht hier also unzweifelhaft Handlungsbedarf, um der Verbreitung und den Auswirkungen von Deepfakes frühzeitig entgegenzutreten zu können. Der Begriff wird jedoch, wie auch schon 2017, nicht explizit im Regierungsprogramm 2020-24 erwähnt. Dieser Umstand lässt vermuten, dass die Gefahr der Verbreitung von Deepfakes für Bürger\_innen, Politik und Unternehmen noch unterschätzt wird und daher nicht im Fokus der aktuellen Bundesregierung steht.

Die unterfertigenden Abgeordneten stellen daher folgenden

## ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

"Die Bundesregierung, insbesondere der Bundesminister für Inneres, wird aufgefordert, dem Nationalrat ein Konzept zum Umgang mit Deepfakes und einer Strategie zur Bekämpfung von politischen, gesellschaftlichen und wirtschaftlichen Risiken durch Deepfakes vorzulegen. Darin soll das Ziel verfolgt werden, frühzeitig Maßnahmen zur Eindämmung von Risiken zu finden."

*In formeller Hinsicht wird die Zuweisung an den Ausschuss für innere Angelegenheiten vorgeschlagen.*