Deutscher Bundestag **Drucksache 19/27848**

19. Wahlperiode 24.03.2021

Antrag

der Abgeordneten Joana Cotar, Dr. Michael Espendiller, Uwe Schulz, Waldemar Herdt, Jörn König, Tobias Matthias Peterka, Dr. Dirk Spaniel, René Springer, Petr Bystron, Peter Felser, Armin-Paulus Hampel, Mariana Iris Harder-Kühnel, Jens Maier, Dr. Birgit Malsack-Winkemann, Christoph Neumann, Ulrich Oehme, Jürgen Pohl und der Fraktion der AfD

Förderung der automatischen Erkennung KI-manipulierter Fotos und Videos

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

In der Fotografie werden Bilder häufig nachträglich bearbeitet, aus ästhetischen, kommerziellen oder politischen Gründen. Seit den 1990er Jahren geschieht dies durch Software, deren Bearbeitung digitaler Fotos keine sichtbaren Spuren mehr hinterlässt. Dies ist mittlerweile auch beim bewegten Bild möglich. Sogenannte Deep Fakes, manipulierte Videodateien, deren Bearbeitung mit bloßem Auge nicht mehr zu erkennen ist, setzen eine lange Tradition fort. Durch den Einsatz Künstlicher Intelligenz (KI) wächst die Präzision der Manipulation, während der zeitliche wie technische Aufwand und der Preis sinken. Die dafür benötigten Programme sind auf dem freien Markt erhältlich (Enquete-Kommission Künstliche Intelligenz, Gesamtbericht, Drucksache 19/23700).

Das wenige Jahre alte Werkzeug des Deep Fake auf der Basis des Maschinellen Lernens wird zum Beispiel im Filmgeschäft eingesetzt, um Trailer zu produzieren, Filmmusik zu komponieren oder um verstorbenen Schauspielern einen Gastauftritt zu verschaffen. Auch die Gamingbranche profitiert von der Kreation potenziell grenzenloser, realistisch wirkender Bildwelten mithilfe eines Algorithmus (Marc Bovenschulte: Deepfakes – Manipulation von Filmsequenzen, Themenkurzprofil Nr. 25, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Mai 2019). Des Weiteren werden Deep Fakes im künstlerischen oder komödiantischen Kontext verwendet.

Die Erstellung und Nutzung von Deep Fakes kann aber auch erhebliche Schädigungen nach sich ziehen. Ein Großteil der erzeugten Deep Fakes entfällt bisher auf das Genre der Pornographie, wo das Antlitz von Prominenten als auch von Privatpersonen täuschend echt in einzelne Szenen montiert wird, meist in rufschädigender oder erpresserischer Absicht. Eine Studie identifizierte rund 14 000 gefälschte Videos, die online zu sehen waren (Henry Ajder et al.: The State of Deepfakes. Landscape, threats, and impact, September 2019).

Daneben besteht für Personen des öffentlichen Lebens die Gefahr, Opfer eines Deep Fake zu werden. Diese können im schlimmsten Fall Teil einer Kampagne sein, um Wahlen zu beeinflussen und das Ansehen demokratischer Institutionen zu untergraben. Um dieser Gefahr zu begegnen, hat die amerikanische Defence Advanced Research Projects Agency (DARPA) im Vorfeld der jüngsten US-Präsidentschaftswahlen 70 Mio. US-Dollar an Forschungsmitteln bereitgestellt, um Abwehrstrategien gegen Deep

Fakes zu entwickeln; dabei geht es primär um Lösungen, Fälschungen automatisch zu erkennen (Norbert Lossau: Deep Fake: Gefahren, Herausforderungen und Lösungswege, in: Analysen & Argumente, Konrad-Adenauer-Stiftung, Februar 2020).

Deep Fakes haben das Potenzial, das Vertrauen in den Journalismus, in Social Media und in die gesellschaftliche Debatte zu verletzen, wenn bei potenziell jedem Foto und jedem Film der Verdacht im Raum steht, die Aufnahme könnte gefälscht, verfremdet oder konstelliert worden sein (https://ninaschick.org/deepfakes). Darunter können die Demokratie und die öffentliche Sicherheit leiden, für die Verlässlichkeit eine unabdingbare Ressource darstellt. Daher ist es von vorrangigem Interesse, Deep Fakes sicher, rasch und kostengünstig als solche identifizieren zu können. Experten gehen von einer Verdopplung der online gestellten Deep Fakes alle sechs Monate aus (https://sensity.ai/deepfake-threat-intelligence-a-statistics-snapshot-from-june-2020/).

Der gegenwärtige Ansatz der Medienforensik untersucht das statistische Paket aller Spuren über Maschinelles Lernen auf Unregelmäßigkeiten (Enquete-Kommission Künstliche Intelligenz, PG 6, Drucksache 006). Der Erfolg der Verifizierung eines Videos als authentisch hängt wesentlich davon, ob RAW-Bilder vorliegen, ob die Aufnahmekamera zugänglich ist, ob die Metadaten vollständig sind, wie oft ein Video editiert wurde. Stark komprimierte Bilder erschweren einen Prüferfolg immens.

Für die Medienforensik wird es mit der technologischen Weiterentwicklung der Software zur permanenten Herausforderung, echte von computergenerierten Videos zu unterscheiden. Zurzeit ist von einem Wettlauf zwischen Verfahren zur Produktion von Deep Fakes und solchen zu ihrer Identifizierung die Rede (Norbert Lossau 2020, a. a. O.). Kommt dann noch die Zirkulation über soziale Netzwerke hinzu, sind manipulierte Videos nach aktuellem Forschungsstand schwer zu entlarven. Für eine manuelle Analyse ist das Volumen schlicht zu groß; vollautomatisierte Verfahren stoßen an semantische Grenzen, wenn sie etwa ironische oder satirische Darstellungen nicht als solche erkennen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

– das Wissen über die dynamische Erstellung und die Detektion von Deep Fakes in Deutschland deutlich auszubauen, um der signifikanten Verbreitung von Deep Fakes auf der Basis von KI angemessen begegnen zu können;
– medienforensische Fähigkeiten entlang der oben genannte Desiderate in Behörden, Unternehmen und Hochschulen wie auch außeruniversitärer Forschungseinrichtungen (stellvertretend das Fraunhofer Institut für Digitale Medientechnologie IDMT) auszubauen, um auch in diesem Bereich eine digitale Souveränität Deutschlands zu gewährleisten;
– das Wissen über Fertigung, Wirkung, Verbreitung und Identifizierung von Deep Fakes für eine systematische Aufklärung der Bevölkerung über das technisch Praktikable zu nutzen;
– Kooperationen unterschiedlichster Institutionen rechtlich, organisatorisch, finanziell und technisch zu unterstützen, um die bestehenden Kompetenzen zur Verifizierung/Falsifizierung von Medien zu bündeln und so die Prüfpraxis erheblich schlagkräftiger und schneller machen und die Glaubwürdigkeit der Prüfergebnisse zu erhöhen;
– den entsprechenden Wissenstransfer mit hinreichenden Mitteln auszustatten, um mit der technologischen Entwicklung Schritt halten zu können.

Berlin, den 17. Februar 2021

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

Begründung

Das Anfertigen eines Deep Fake ist nicht per se illegal, entscheidend sind Motivation und Kontext seiner Verbreitung. Die interdisziplinäre Forschung muss in die Lage versetzt werden, zwischen den unterschiedlichen Aspekten des technisch Machbaren und des jeweiligen Verwendungszusammenhangs differenzieren zu können. Dafür muss sie aber in der Lage sein, Deep Fakes als solche zu erkennen.

Große Internet-Konzerne rufen Programmierer regelmäßig zu Wettbewerben zur Detektion und Identifikation von Deep Fakes auf (etwa unter www.kaggle.com/c/deepfake-detection-challenge). Mit diesem dergestalt erworbenen Wissen können sie gegen mutmaßliche Deep Fakes auf ihren eigenen Plattformen vorgehen. Dessen ungeachtet erscheint es als unabdingbar, dass auch die unabhängige Forschung jenseits kommerzieller Interessen den jeweils aktuellen Stand der Deep-Fakes-Fabrikation abbilden kann.

Die Bundesregierung attestiert, dass Entwicklung und Forschung zum Thema Deep Fakes noch am Anfang stehen (Antwort der Bundesregierung auf eine Kleine Anfrage zur „Beschäftigung der Bundesregierung mit Deepfakes“, Drucksache 19/15657). Allerdings zieht sie aus diesem Befund nicht den Schluss, dass die Forschung zum Thema gerade angesichts des weiter oben genannten Missbrauchspotenzials im politischen Kontext zu fördern wäre. Diese Lücke schließt der vorliegende Antrag.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333