Deutscher Bundestag **Drucksache 19/15210**

19. Wahlperiode 14.11.2019

Kleine Anfrage

der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, Renata Alt, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Dr. Marco Buschmann, Britta Katharina Dassler, Hartmut Ebbing, Dr. Marcus Faber, Daniel Föst, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Reinhard Houben, Olaf in der Beek, Gyde Jensen, Dr. Marcel Klinge, Daniela Kluckert, Konstantin Kuhle, Alexander Graf Lambsdorff, Ulrich Lechte, Michael Georg Link, Roman Müller-Böhm, Hagen Reinhold, Bernd Reuther, Dr. Wieland Schinnenburg, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Katja Suding, Linda Teuteberg, Michael Theurer, Stephan Thomae, Dr. Florian Toncar, Gerald Ullrich, Nicole Westig und der Fraktion der FDP

Beschäftigung der Bundesregierung mit Deepfakes

Der Begriff „Deepfake“ bezeichnet täuschend echt wirkende Bild-, Audio- oder auch Videomanipulationen, die zumeist mit Hilfe künstlicher Intelligenz hergestellt wurden. Hierfür werden neuronale Netzwerke entsprechend programmiert und trainiert, sodass die Bilder bzw. Videos weitgehend autonom erzeugt werden können. So wurde beispielsweise bereits das Gesicht Dr. Angela Merkels durch das von Donald Trump ersetzt (www.tagesschau.de/faktenfinder/hintergrund/deep-fakes-101.html) oder ein Video erstellt, in dem Mark Zuckerberg von der Macht schwärmt, die ihm die gestohlenen Daten von Milliarden von Menschen verleihen (www.welt.de/wirtschaft/webwelt/video195189665/Deepfake-Video-Mark-Zuckerberg-schwaermt-von-Weltherrschaft-verblueffend-echt.html). Auch wenn sich zu Beginn viele Fälschungen noch bei genauerem Hinsehen mit bloßem Auge erkennen ließen, werden die Manipulationen zunehmend besser und sind vor allem beim schnellen Erfassen beispielsweise über Social Media auf dem Handybildschirm kaum als Fälschung zu erkennen.

„Im Oktober 2019 hat der US-Bundesstaat Kalifornien das Verbreiten von „materially deceptive audio or visual media“ in Bezug auf politische Kandidaten für den Zeitraum von 60 Tagen vor einer Wahl verboten (Assembly Bill No. 730 „Elections: deceptive audio or visual media.“). Das Gesetz nimmt für „materially deceptive audio or visual media“ in SEC. 4 subdivision (e) eine Definition vor. (Quelle: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730)“

Die missbräuchliche Nutzung von Deepfakes ist aus Sicht der Fragesteller zurzeit hauptsächlich in drei Feldern zu beobachten bzw. zu befürchten. Zum einen bieten Deepfakes neue und bessere Möglichkeiten für Desinformation. So können beispielsweise falsche Statements bzw. Fotos oder Videos von Personen oder Unglücksfällen nach Ansicht der Fragesteller im schlimmsten Fall Einfluss auf politische Prozesse nehmen. Ein weiterer Bereich ist die Nutzung von Deepfakes für pornographische Inhalte. Publik wurde dieses Thema kürzlich

durch den Erfolg der App „DeepNude“, die aus Fotos einer bekleideten Person ein Nackt-Foto ebenjener Person generierte. Das Programm wurde binnen kürzester Zeit 100.000fach heruntergeladen, sodass schließlich die Entwickler selbst die App vom Markt nahmen. Sie begründeten dies damit, dass bei einer solchen Masse an Nutzern trotz der getroffenen Sicherheitsvorkehrungen (wie z. B. Wasserzeichen auf den Bildern) ein Missbrauch der Anwendung nicht auszuschließen sei und sie auf diesem Wege kein Geld verdienen wollen (https://twitter.com/deepnudeapp/status/1144307316231200768). Anzumerken ist jedoch, dass dies lediglich mit weiblichen Körpern funktionierte (www.heise.de/tr/artikel/Deepfakes-Die-nackte-Gefahr-4458332.html). Darüber hinaus werden immer bessere Videos pornographischen Inhalts erstellt, in denen die Gesichter der Akteure mit Hilfe künstlicher Intelligenz ausgetauscht werden. Zurzeit sind hiervon hauptsächlich prominente Künstlerinnen betroffen, jedoch sind vermehrt auch Privatpersonen das Ziel der Manipulationen. Bereits jetzt gibt es die Möglichkeit, gegen Bitcoins einen Deepfake-Porno mit einer beliebigen Person zu erwerben (www.wired.com/story/most-deepfakes-porn-multiplying-fast/). Voraussetzung ist lediglich genügend Bildmaterial, was zum Teil bereits durch die Links zu Social-Media-Profilen gegeben ist. Solche Videoclips können nach Ansicht der Fragesteller als Grundlage für beispielsweise Erpressungen, Verleumdungen oder weiteres strafrechtlich relevantes Verhalten dienen. Bisher ist zu beobachten, dass von dieser Problematik hauptsächlich Frauen betroffen sind. Eine weitere Gefahr von Deepfakes ist der Bereich der Identifizierung bzw. Authentifizierung. Biometrische Merkmale wie die Stimme, die Iris oder das Gesicht lassen sich mit immer weniger Aufwand bei zeitgleich immer besserer Qualität unter Zuhilfenahme künstlicher Intelligenz fälschen. Vor allem im Hinblick auf das Video-Ident-Verfahren eröffnet sich hier die Gefahr eines weitreichenden Identitätsdiebstahls (vgl. www.computerwoche.de/a/so-manipulieren-hacker-audio-und-videodaten,3545745).

Zusammenfassend lässt sich sagen, dass Deepfakes nach Ansicht der Fragesteller das Potential haben, die Sicherheit momentan angewendeter Methoden zur Authentifizierung im Rechtsverkehr zu untergraben, das Vertrauen der Bevölkerung in den öffentlichen Diskurs zu beschädigen sowie gerade bei pornographischen Inhalten nicht nur massiv die Persönlichkeitsrechte Betroffener zu verletzen, sondern auch tiefgreifende persönliche Schäden zu verursachen. Jedoch gibt es auch aktive Bestrebungen und Forschungen zur Erkennung von manipulierten Bild-, Ton- oder Videoaufnahmen. So hat Facebook zusammen mit einigen Partnern wie Microsoft oder Amazon die „Deepfake Detection Challenge“, kurz: DFDC (https://deepfakedetectionchallenge.ai/), ins Leben gerufen, welche im Dezember 2019 starten wird und die Forschung im Bereich der automatisierten Erkennung von Deepfakes vorantreiben soll.

Es kann jedoch auch durchaus positive Einsatzmöglichkeiten von Deepfakes geben. Im kulturellen Bereich hat beispielsweise die Zeitung „The Times“ zusammen mit Rothco einen ersten Schritt mit dem Projekt „JFK Unsilenced“ gemacht, indem sie die Rede, die John F. Kennedy am Tag seiner Ermordung in Dallas hätte halten sollen, mit Hilfe von künstlicher Intelligenz und einem Deepfake in seiner Stimme vertont hat (https://rothco.ie/work/jfk-unsilenced/). Ebenso ist ein Einsatz im medizinischen Bereich denkbar. Deepfakes können zum Beispiel Menschen helfen, die aufgrund von Behinderungen oder chronischen Erkrankungen ihre Stimme verlieren, eine authentische Stimme zur Kommunikation zu erhalten oder sogar ihre eigene Stimme gewissermaßen zu behalten (www.projectrevoice.org/).

Wir fragen die Bundesregierung:

1. In welchen Zusammenhängen beschäftigt sich die Bundesregierung mit dem Thema Deepfakes?

   Welche Ressorts und dort jeweils welche Abteilungen, Referate oder Stabsstellen beschäftigen sich konkret mit dem Thema?

2. Welche Definition von Deepfakes legt die Bundesregierung ihrer Beschäftigung mit diesem Thema zugrunde?

3. Unterscheidet die Bundesregierung in ihrer Beschäftigung mit dem Thema Deepfakes zwischen legitimen oder harmlosen (bzw. rechtmäßigen) und illegitimen oder gefährlichen (bzw. rechtswidrigen) Zwecken zur Erstellung oder Verwendung von Deepfakes?

   In welche Kategorie fallen für die Bundesregierung Manipulationen von Medien (Audio, Foto, Video) zu Zwecken der Satire, der (kulturellen) Bildung oder der pornographischen Darstellung?

4. In welchen Bereichen sieht die Bundesregierung konkreten Nutzen, der von Deepfakes ausgeht?

   Wie schätzt die Bundesregierung den Nutzen von Deepfakes beispielsweise zum Zweck der Satire, der (kulturellen) Bildung oder der pornographischen Darstellung ein?

5. In welchen Bereichen sieht die Bundesregierung konkrete Gefahren, die von Deepfakes ausgehen?

   Wie schätzt die Bundesregierung die Gefahren von Deepfakes beispielsweise zum Zweck der Satire, der (kulturellen) Bildung oder der pornographischen Darstellung ein?

6. Hat die Bundesregierung zur Erforschung von Nutzen und Gefahren von Deepfakes bereits Studien in Auftrag gegeben?

   Wenn ja, welche?

   Welche bereits existierenden Studien zum Nutzen und zu den Gefahren von Deepfakes sind der Bundesregierung bekannt?

7. Welche rechtlichen Regelungen existieren nach Ansicht der Bundesregierung bereits, die konkret auf Deepfakes anwendbar sind?

   Welchen Regelungsbedarf in Bezug auf Deepfakes sieht die Bundesregierung darüber hinaus – möglicherweise auch nur in Bezug auf einzelne Anwendungsbereiche von Deepfakes?

8. Hat die Bundesregierung zur rechtlichen Einordnung und zum rechtlichen Regelungsbedarf in Bezug auf Deepfakes bereits Studien in Auftrag gegeben?

   Wenn ja, welche?

   Welche bereits existierenden Studien zur rechtlichen Einordnung und zum rechtlichen Regelungsbedarf in Bezug auf Deepfakes sind der Bundesregierung bekannt?

9. Wie viele gerichtliche Auseinandersetzungen oder Strafverfahren, in denen es um Deepfakes und ihre Auswirkungen ging, gab es nach Kenntnis der Bundesregierung seit dem Jahr 2015 (bitte nach Jahren aufschlüsseln)?

10. Wie schätzt die Bundesregierung die Möglichkeit der Auslösung oder Vertiefung diplomatischer Spannungsfälle durch Deepfakes ein?

    Wie bereitet sich die Bundesregierung auf mögliche diplomatische Spannungsfälle vor, die durch Deepfakes ausgelöst oder vertieft werden?

    Welche konkreten Maßnahmen hat die Bundesregierung bisher dazu ergriffen oder sind in Planung (wie z. B. die Entwicklung von Strategien oder Leitfäden zur Krisenkommunikation, Szenarienworkshops, Media Forensik, Aufbau von Expertise im Auswärtigen Amt)?

11. Welche Maßnahmen plant die Bundesregierung, um die gesellschaftliche Resilienz und Medienkompetenz der Bevölkerung zu stärken und die Bürgerinnen und Bürger dazu zu befähigen, Deepfakes und ihre Auswirkungen besser zu erkennen?

12. Welche Hilfemöglichkeiten existieren nach Kenntnis der Bundesregierung für Betroffene von Deepfakes?

    Welche Beratungs- und Hilfestellen existieren nach Kenntnis der Bundesregierung, die insbesondere Betroffene von Deepfakes adressieren?

13. Welchen gesamtgesellschaftlichen Einfluss könnten Deepfakes nach Ansicht der Bundesregierung entfalten?

    Wie schätzt die Bundesregierung etwa das Potential von Deepfakes zur Verunsicherung der Bevölkerung in Bezug auf das Vertrauen in wahre und unwahre Informationen ein?

14. Was plant die Bundesregierung, um Deepfakes insbesondere im Zusammenhang mit Wahlen zu bekämpfen?

    Plant die Bundesregierung in diesem Bereich Maßnahmen in Bezug auf Social-Media-Plattformen?

    Wenn ja, welche?

15. Welche Bemühungen und Maßnahmen oder Vorschläge für Maßnahmen in Bezug auf Deepfakes sind der Bundesregierung auf EU-Ebene und auf Ebene der anderen EU-Mitgliedstaaten bekannt?

16. Wird die Bundesregierung den Umgang mit Deepfakes – im Zusammenhang mit, aber auch außerhalb von Wahlen – als ein Thema der deutschen EU-Ratspräsidentschaft 2021 festlegen?

17. Wurde das Thema Deepfakes nach Kenntnis der Bundesregierung in den Verhandlungen zum Medienstaatsvertrag behandelt?

    Wenn ja, in welcher Form?

    Wenn nein, warum nicht?

18. Welche technischen Möglichkeiten zur Erkennung von Deepfakes sind der Bundesregierung bekannt?

    Welche Forschungsvorhaben gibt es nach Kenntnis der Bundesregierung hierzu in Deutschland und weltweit?

Berlin, den 6. November 2019

Christian Lindner und Fraktion

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