Deutscher Bundestag **Drucksache 19/15657**

19. Wahlperiode 02.12.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/15210 –

Beschäftigung der Bundesregierung mit Deepfakes

Vorbemerkung der Fragesteller

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: www.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

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Justiz und für Verbraucherschutz vom 28. November 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

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 (www.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 (www.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 (www.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/).

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?

Das Thema Deep Fakes wird in der Bundesregierung übergreifend – auch innerhalb der obersten Bundesbehörden – behandelt. Insbesondere im Rahmen der Kabinettklausur am 17. und 18. November 2019 in Meseberg hat sich die Bundesregierung mit dem Thema auseinandergesetzt.

Deep Fakes können eine große Gefahr für Gesellschaft und Politik darstellen, wenn sie dazu genutzt werden, die öffentliche Meinung zu manipulieren und den politischen Prozess gezielt zu beeinflussen. Mit dem Themenkomplex Desinformation beschäftigen sich im Auswärtigen Amt verschiedene Arbeitseinheiten unter der Federführung der Steuerungsgruppe Strategische Kommunikation und ebenfalls die Beauftragte der Bundesregierung für Kultur und Medien sowie das Bundesministerium der Justiz und für Verbraucherschutz. Im Bundesministerium für Bildung und Forschung beschäftigt sich die Abteilung „Forschung für Digitalisierung und Innovationen“ mit dem Thema Deep Fakes durch die Förderung von Forschungsvorhaben zur Erkennung und Bekämpfung von Desinformationen („Fake News“) und im Rahmen der IT-Forensik.

Deep Fakes stellen bei der Kriminalitätsbekämpfung eine große Herausforderung dar und stehen daher aufgrund der hierbei genutzten KI-gestützten Technologien auch mit im Fokus des entsprechenden Arbeitsbereichs der Abteilung Cyber- und Informationssicherheit im Bundesministerium des Innern, für Bau und Heimat (BMI). Des Weiteren beschäftigt sich das BMI federführend mit hybriden Bedrohungen. In diesem Kontext sind Deep Fakes ein denkbares Mittel der Einflussnahme durch Verbreitung von Desinformation.

Die Arbeitseinheiten in den Abteilungen „Digitale Gesellschaft; Verwaltungsdigitalisierung und Informationstechnik“ und „Öffentliche Sicherheit“ beschäftigen sich mit dem Thema im Kontext der Fernidentifizierung. Durch den Einsatz von Deep Fakes ist es möglich, videobasierte Verfahren zu manipulieren. Beispielsweise kann eine zu identifizierende Person eine andere Person auf einem gestohlenen Ausweisdokument imitieren.

Mit Deep Fakes aus sozialwissenschaftlicher Perspektive als Instrument hybrider Kriegsführung beschäftigt sich an der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg, welche dem Bundesministerium der Verteidigung (BMVg) zugeordnet ist, die Professur für Politische Theorie im Rahmen der thematischen Schwerpunkte „Digitale Demokratie“ und „Hybride Bedrohungen“ und fragt danach, welche funktionalen Voraussetzungen liberaler Demokratien dadurch beschädigt werden.

Darüber hinaus beobachtet das BMVg technologische Entwicklungen in Zusammenhang mit Deep Fakes in ihren Implikationen für den Geschäftsbereich BMVg wachsam.

Die zielgruppengerechte Vermittlung von Digitalkompetenzen ist eine Kernherausforderung der digitalen Gesellschaft. Dazu gehört auch die zeitgemäße und dem jeweiligen Stand der Technik entsprechende Kompetenz, Falschinformationen aller Art zu erkennen und bewerten zu können. Das Bundesministerium für Familie, Senioren Frauen und Jugend entwickelt und fördert in unterschiedlichen Projekten und Maßnahmen Kompetenzvermittlung (vgl. Maßnahmen im Handlungsfeld Digitale Kompetenz der Umsetzungsstrategie Digitalisierung der Bundesregierung) als auch entsprechende grundlegende Konzepte und Forschung (wie z. B. im Rahmen des Projektes Digitales Deutschland www.digid.jff.de).

Auch das Bundeskanzleramt befasst sich im Rahmen seiner Aufgaben mit dem Themenkomplex hybride Bedrohungen und betrachtet hierbei u. a. Fragen der (gesellschaftlichen) Resilienz.

Im Presse- und Informationsamt der Bundesregierung beschäftigen sich alle Abteilungen im Rahmen ihrer Zuständigkeiten auch mit diesem Thema.

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

Die Bundesregierung sieht kein Erfordernis einer eigenen, von öffentlichen Quellen abweichenden Definition.

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?

Die Fragen 3 bis 5 werden gemeinsam beantwortet.

Die Entwicklung und Forschung zum Thema Deep Fakes steht noch am Anfang. Auf dieser noch fortzuentwickelnden wissenschaftlichen Basis ist eine strikte Unterscheidung zwischen harmlos und gefährlich zurzeit nicht zielführend. Vor diesem Hintergrund kann auch das konkrete Nutzungspotential von Deep-Fake-Anwendungen noch nicht sicher abgeschätzt werden. Positive Aspekte können aber unter Umständen zum Beispiel in der Museumspädagogik oder für künstlerische und satirische Zwecke erzielt werden.

Gleichzeitig können Deep-Fake-Anwendungen auch eine Gefahr darstellen, da Deep Fakes grundsätzlich zur Manipulation der öffentlichen Meinung und damit zur gezielten Einflussnahme auf den politischen Prozess eingesetzt werden können. Grundsätzlich führen moderne Methoden der Künstlichen Intelligenz (KI) wie die durch neuronale Netze gestützte künstliche Erzeugung von Bildern und Videoclips oder auch das gezielte Verändern von Bildern dazu, dass künstliches Bild- und Videomaterial immer echter wirkt. So wird es in der Praxis zunehmend schwieriger, zwischen authentischem und künstlich erzeugtem bzw. verändertem Material zu unterscheiden. Dies könnte auch für Angriffe auf videobasierte Fernidentifizierungsverfahren genutzt werden. Mit fortschreitender Entwicklung der Technik verbessern sich gleichzeitig auch die Mechanismen zur Erkennung von Fälschungen und Fälschungsversuchen, wenngleich kaum eine 100prozentige Verifizierung möglich sein wird. Daher ist es wichtig, dass die Sicherheitsbehörden ihre technologiegestützten Fähigkeiten und Methoden stetig weiterentwickeln.

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?

Die Bundesregierung hält die Stärkung der Medienkompetenz, insbesondere der Nachrichten- und der digitalen Informationskompetenz, für entscheidend, um gegen Desinformation im Allgemeinen und Deep Fakes im Besonderen gewappnet zu sein. Dies beinhaltet u. a. Fähigkeitenausbau zur Identifizierung von Deep Fakes, Zusammenarbeit mit der Privatwirtschaft, der Zivilgesellschaft und unabhängigen Medien sowie die Stärkung von Resilienz gegenüber Desinformation.

Die Beauftragte der Bundesregierung für Kultur und Medien fördert aktuell eine Studie der Stiftung Neue Verantwortung, die die digitale Nachrichtenkompetenz in Deutschland altersübergreifend erfassen und damit Ansatzpunkte zu ihrer Verbesserung aufzeigen soll.

Der Schwerpunkt der Medienkompetenzförderung der Beauftragten für Kultur und Medien soll in Zukunft auf der Stärkung der Nachrichten- und digitalen Informationskompetenz liegen.

Im Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015–2020“ stellen Untersuchungen zur sicheren und demokratischen Gestaltung der direkten politischen und gesellschaftlichen Beteiligung einen wichtigen Bestandteil dar. Ein Beispiel dafür ist das Projekt DORIAN, in dem ein Podcast beim Hessischen Rundfunk entstand, der als Material in Schulen dienen wird, um Schülerinnen und Schüler für die Merkmale von Desinformation zu sensibilisieren. Ein weiteres Beispiel sind die verschiedenen Aufklärungsformate (bspw. bürgerorientierte Veranstaltungen, Beiträge in überregionalen Medien) des Nationalen Forschungszentrums für angewandte Cybersicherheit CRISP/ATHENE zum Thema Deep Fake. Im Übrigen wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/3649 verwiesen.

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?

Auf so genannte Deep Fakes finden generell-abstrakte Regelungen Anwendung. Spezifische Regelungen auf Bundesebene, die ausschließlich Deep-Fake-Anwendungen erfassen oder für diese geschaffen wurden, existieren nicht. Die Bundesregierung überprüft den Rechtsrahmen auf Bundesebene fortlaufend daraufhin, ob aufgrund von technologischen oder gesellschaftlichen Herausforderungen ein Anpassungsbedarf besteht.

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?

Es wird auf die Antwort zu Frage 6 verwiesen.

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)?

Die Führung von Zivil- und Strafverfahren fällt grundsätzlich in die Zuständigkeit der Länder. Die Bundesregierung äußert sich grundsätzlich nicht zu Sachverhalten, die in die Zuständigkeit der Länder fallen. Ergänzend ist darauf hinzuweisen, dass keine bundesweite statistische Erfassung von gerichtlichen Auseinandersetzungen, in denen es um das Phänomen der Deep Fakes und ihren Auswirkungen geht, existiert.

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)?

Es kann nicht ausgeschlossen werden, dass aufgrund der schnellen technologischen Fortschritte künftig auch eine Bedrohung demokratischer Prozesse durch Deep Fakes erfolgen kann. So könnten Desinformationskampagnen durch Deep Fakes begleitet und ihr Effekt verstärkt werden. Mit Desinformation im Kontext hybrider Bedrohungen befasst sich die ressortübergreifende Arbeitsgruppe zur Strategischen Koordination des Umgangs mit Hybriden Bedrohungen (vgl. Ziffer 2 der Vorbemerkung der Bundesregierung zur Antwort auf die Kleine Anfrage auf Bundestagsdrucksache 19/12489). Die Bundesregierung stimmt sich in der Horizontalen Arbeitsgruppe „Stärkung der Resilienz und Abwehr hybrider Bedrohungen“ mit den anderen Mitgliedstaaten der EU ab. Die Mitgliedstaaten sind außerdem über das Rapid Alert System (RAS) miteinander verbunden, in welchem Erkenntnisse zu Desinformation und damit auch zu Deep Fakes geteilt werden können. Auch die Klausurtagung des Bundeskabinetts im November 2019 behandelte u. a. das Thema Deep Fakes.

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?

Es wird auf die Antwort zu Frage 6 verwiesen.

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?

Die Beratung der Verbraucherinnen und Verbraucher ist grundsätzlich Aufgabe der Länder. Die Bundesregierung verfügt derzeit nicht über Informationen darüber, ob in den Ländern entsprechende Beratungs- und Hilfeeinrichtungen speziell zu Deep-Fake-Anwendungen bestehen. Unabhängig davon bestehen Beratungseinrichtungen für die Opfer von Straftaten und die Beratungsstellen der Verbraucherzentralen.

Vorkommnisse im Zusammenhang mit Deep Fakes können im Geschäftsbereich des BMVg über die etablierten Meldewege dienstlich zur Kenntnis gebracht werden.

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?

Deep Fakes können das gesellschaftliche Vertrauen in die grundsätzliche Echtheit von Audio- und Videoaufnahmen und damit die Glaubwürdigkeit öffentlich verfügbarer Informationen schwächen. Noch können auch komplexe Deep Fakes zeitnah und schnell erkannt werden. Ein problematisches Szenario wäre eine schwererkennbare Technik in Massenanwendung im Rahmen plausibler, aber verfälschter Narrative. Angesichts der noch geringen Relevanz für die Öffentlichkeit warnen Wissenschaftler vor einer Überbewertung der Gefahren von Deep Fakes für demokratische Prozesse (z. B. verglichen mit Desinformation).

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?

Es besteht die Möglichkeit, dass Deep Fakes mit dem Ziel der Desinformation beispielsweise über soziale Netzwerke verbreitet werden, um Einfluss auf den politischen Prozess zu nehmen. Die Bundesregierung begrüßt in diesem Zusammenhang den EU Code of practice on disinformation, den die großen Online-Plattformen und Verbände der Werbewirtschaft im Dezember 2018 mit der EU-Kommission unterzeichnet haben. Die Bundesregierung begrüßt gleichfalls, dass die EU sich nach dem Zwischenbericht zur Umsetzung des Aktionsplans gegen Desinformation (JOIN(2019) 12 final) weitere Schritte, einschließlich regulatorischer Maßnahmen, vorbehält.

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?

Gemäß dem EU-Aktionsplan gegen Desinformation (JOIN(2018) 36 final) wird die Kommission gegebenenfalls Informationskampagnen unterstützen, um

die Öffentlichkeit für neueste Technologien wie Deep Fakes zu sensibilisieren. Darüber hinaus könnte der geplante Digital Services Act Regulierungsmaßnahmen zu Deep Fakes beinhalten.

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?

Es wird auf die Vorbemerkung der Bundesregierung in der Antwort auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN (Bundestagsdrucksache 19/15236) verwiesen.

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

Wenn ja, in welcher Form?

Wenn nein, warum nicht?

Der Medienstaatsvertrag fällt in die Zuständigkeit der Länder. Der Bundesregierung liegen keine Informationen vor, ob bzw. inwieweit das Thema Deep Fakes in den Verhandlungen zur Novellierung des Medienstaatsvertrags erörtert wurde.

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?

Mit jeder neuen Technologie entstehen seit jeher auch neue Möglichkeiten und Angriffsszenarien im Zusammenhang mit Straftaten. KI-Technologie, die von Straftätern bei der Erstellung von Deep Fakes verwendet wird, kann auf Seiten der Sicherheitsbehörden als Instrument maßgeblich bei der Strafverfolgung, Ermittlung und Analyse unterstützen. So können beispielsweise Methoden der Künstlichen Intelligenz (KI) bzw. des maschinellen Lernens auch herangezogen werden, um Deep Fakes, welche mittels KI-Methoden erzeugt werden, gezielt zu erkennen. Weiterhin wird der aktuelle Forschungsstand beobachtet, z. B. zur Erkennung und zu Nutzen und Gefahren von Deep Fakes.

Zur Erkennung von Deep Fakes eignen sich Werkzeuge der Multimediaforensik, mit denen sich Manipulationsspuren in Multimediadaten technisch erkennen und nachweisen lassen. In Deutschland beschäftigt sich insbesondere das Nationale Forschungszentrum für angewandte Cybersicherheit CRISP/ATHENE, aber auch die TU München oder das Fraunhofer-Institut mit diesem Thema. Zudem haben der deutsche Auslandssender Deutsche Welle (DW), das Fraunhofer-Institut für Digitale Medientechnologie (IDMT) und das Athens Technology Center (ATC) das gemeinsame Forschungsprojekt „Digger“ gestartet. Ziel des Projekts ist es, die webbasierte Verifikationsplattform „Truly Media“ von DW und ATC u. a. um die Audioforensik-Technologien des Fraunhofer IDMT zu erweitern und Journalisten auf diese Weise zu helfen, Manipulationen an audiovisuellen Inhalten zu erkennen. Weltweit wird die Erkennung von Deep Fakes zudem beispielsweise von Wissenschaftlern an der New York University oder an der University of California/Berkeley erforscht. Zudem ist die Software „Face Forensics“ bekannt, die mittels Künstlicher Intelligenz die zugrundeliegenden Muster bei der Erstellung von Deep Fakes erkennt.

Noch nicht abgeschlossen ist nach Kenntnis der Bundesregierung ein aktuelles Forschungsvorhaben der Konrad-Adenauer-Stiftung zu den gesellschaftlichen Auswirkungen von Deep Fakes, das in Zusammenarbeit mit Counter Extremism Project unter Beteiligung von Prof. Dr. Hany Farid (University of California, Berkeley) durchgeführt wird.

Im Übrigen wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 30 des Abgeordneten Konstantin Kuhle auf Bundestagsdrucksache 19/13020 verwiesen, deren Aussagen auch hier sinngemäß gelten.

Auch die Datenethikkommission der Bundesregierung hat sich ihren am 23. Oktober 2019 veröffentlichten Empfehlungen mit dem Thema Deep Fakes beschäftigt. Die Empfehlungen der Datenethikkommission sind abrufbar unter https://datenethikkommission.de/wp-content/uploads/191028_DEK_Gutachten_bf.pdf .

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