

## **Antwort**

### **der Bundesregierung**

**auf die Kleine Anfrage der Abgeordneten Joana Cotar, Uwe Schulz,  
Dr. Michael Esendiller, weiterer Abgeordneter und der Fraktion der AfD  
– Drucksache 19/7677 –**

### **Mögliche Zusammenarbeit der Bundesregierung mit Facebook zur Bekämpfung von Wahlmanipulationen bei den Wahlen zum Europäischen Parlament 2019**

#### **Vorbemerkung der Fragesteller**

Die EU-Kommission schätzt, dass bereits ein Drittel der eingesetzten Wahlkampfgelder in sozialen Medien eingesetzt werden ([www.nrz.de/politik/eu-kommission-warnt-vor-cyberattacken-auf-die-europawahl-id214981453.html](http://www.nrz.de/politik/eu-kommission-warnt-vor-cyberattacken-auf-die-europawahl-id214981453.html)).

Daher warnte die EU-Kommission schon im Sommer 2018 alle EU Mitgliedstaaten davor, dass im Zusammenhang mit der Wahl zum Europäischen Parlament im Mai 2019 mit Manipulationen und Einflüssen in sozialen Medien gerechnet werden könne. Der EU-Sicherheitskommissar, Julian King, drängte daher die EU-Mitgliedstaaten, Internetplattformen und politische Parteien zum Handeln. „Alle Mitgliedstaaten müssen die Bedrohung der demokratischen Prozesse und Institutionen durch Cyberangriffe und Desinformationen ernst nehmen und nationale Pläne zur Vorbeugung aufstellen. Wir müssen verhindern, dass staatliche und nichtstaatliche Akteure unsere demokratischen Systeme untergraben und als Waffe gegen uns einsetzen“, so King ([www.nrz.de/politik/eu-kommission-warnt-vor-cyberattacken-auf-die-europawahl-id214981453.html](http://www.nrz.de/politik/eu-kommission-warnt-vor-cyberattacken-auf-die-europawahl-id214981453.html)).

Soziale Netzwerke wie Facebook oder Google+ haben großes Potential dahingehend, dass politische Anzeigen in ihren Netzwerken missbraucht werden, wie etwa bei den US-Wahlen 2016 ([www.nrz.de/politik/facebook-russische-politbeitraege-verbreiteter-als-bekannt-id212401989.html](http://www.nrz.de/politik/facebook-russische-politbeitraege-verbreiteter-als-bekannt-id212401989.html)) oder im Zusammenhang mit dem Skandal um das Unternehmen „Cambridge Analytica“. Im Zuge des Datenschutzskandals um „Cambridge Analytica“ wurden Datenlecks und Sicherheitsverletzungen bei Facebook besonders intensiven Untersuchungen unterzogen ([www.nrz.de/leben/digital/hacker-entdeckt-potentielles-daten-leck-bei-facebook-app-id214720561.html](http://www.nrz.de/leben/digital/hacker-entdeckt-potentielles-daten-leck-bei-facebook-app-id214720561.html)). Laut einem Bericht der „Washington Post“, unter Berufung auf Insiderquellen, soll Facebook von der FTC (Federal Trade Commission) eine „Rekordstrafe“ erwarten, welche im Zusammenhang mit dem Datenschutzskandal um das Unternehmen Cambridge Analytica ausgesprochen werden soll ([www.deraktionaeer.de/aktie/horror-bericht-fuer-facebook-432920.htm](http://www.deraktionaeer.de/aktie/horror-bericht-fuer-facebook-432920.htm)).

Laut Medienberichten (z. B: [www.nzz.ch/digital/facebook-will-mit-behoerden-wahlmanipulation-bekaempfen-ld.1453468](http://www.nzz.ch/digital/facebook-will-mit-behoerden-wahlmanipulation-bekaempfen-ld.1453468)) möchte Facebook nun mit deutschen Behörden zusammenarbeiten, um im Vorfeld der EU-Wahlen 2019 etwaige Wahlmanipulationen und Wahlbeeinflussungen zu bekämpfen. Facebook habe, laut eigenen Angaben, den Datenschutz verbessert und gehe massiv gegen Hassrede und Manipulation, vor allem vor Wahlen, vor.

Im Zuge der Innovationskonferenz DLD 2019 in München kündigte Sheryl Sandberg (Facebook-Vizechefin) an, dass Facebook mit dem Bundesamt für Sicherheit und Informationstechnik (BSI) eine strategische Zusammenarbeit vereinbart habe ([www.spiegel.de/netzwelt/netzpolitik/facebook-sheryl-sandberg-gelobt-auf-der-dld-besserung-a-1248991.html](http://www.spiegel.de/netzwelt/netzpolitik/facebook-sheryl-sandberg-gelobt-auf-der-dld-besserung-a-1248991.html); [www.sueddeutsche.de/digital/sandberg-facebook-dld-bsi-europawahl-1.4295176](http://www.sueddeutsche.de/digital/sandberg-facebook-dld-bsi-europawahl-1.4295176)).

1. Wie definiert die Bundesregierung folgende Begriffe:

- a) Hate Speech,
- b) Fake News?

Der Begriff der sogenannten Hate Speech oder Hassrede ist gesetzlich nicht definiert. In bestimmten Fällen kann die Verbreitung von Inhalten, die nach allgemeinem Verständnis als „Hate Speech“ bezeichnet werden können, den Tatbestand einer deutschen Strafnorm erfüllen. Einschlägig können beispielsweise der Tatbestand der Volksverhetzung nach § 130 des Strafgesetzbuches (StGB) oder die Beleidigungstatbestände nach §§ 185 ff. StGB sein. Die Anforderungen ergeben sich aus dem jeweiligen Straftatbestand anhand der dortigen Tatbestandsmerkmale. Die Bundesregierung sieht aufgrund der bestehenden einschlägigen Strafnormen keinen Anlass, eine Definition von „Hate Speech“ vorzunehmen (so auch schon zum Begriff der „Online-Hetze“, vgl. die Antworten der Bundesregierung zu den Fragen 4 bis 5b der Kleinen Anfrage der Fraktion der AfD auf Bundestagsdrucksache 19/4295).

Der Begriff der sogenannten Fake News ist gesetzlich nicht definiert. Auf die Antwort der Bundesregierung zu Frage 8 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 19/2224 wird verwiesen.

2. Wann, und mit wem wurde eine Zusammenarbeit mit Facebook, welche Sheryl Sandberg bei der Innovationskonferenz DLD 2019 bekanntgegeben hat, verhandelt und abgeschlossen (bitte alle Bundesbehörden und Bundesministerien bekanntgeben, welche an den Verhandlungen teilgenommen haben)?

Bereits im Rahmen der Bundestagswahl 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit Facebook Deutschland, insbesondere bezüglich der Sicherheit und Verifizierung von Accounts, zusammengearbeitet. Seit September 2018 verhandelt das BSI mit Blick auf zukünftige Wahlen über eine Institutionalisierung und Erweiterung der Zusammenarbeit.

3. Welche konkrete Zusammenarbeit mit Facebook, welche Sheryl Sandberg bei der Innovationskonferenz DLD 2019 bekanntgegeben hat, hat die Bundesregierung mit Facebook abgeschlossen (bitte die konkreten Maßnahmen der Zusammenarbeit bekanntgeben)?

Ausgehend von den positiven Rückmeldungen politischer Parteien, Kandidaten und parteinaher Stiftungen, die im Rahmen der Bundestagswahl 2017 Unterstützungsangebote des BSI in Anspruch genommen haben, plant das BSI in Zusammenarbeit mit Betreibern sozialer Netzwerke, Forschungsinstituten und Vertretern aus Verbänden und sogenannten Thinktanks die Entwicklung von Sicherheitsempfehlungen für politische Parteien, Kandidaten und parteinahe Stiftungen im Bereich der Cyber-Sicherheit.

4. Welche Bundesbehörden sind in die Zusammenarbeit mit Facebook (Fragen 2 und 3) eingebunden (bitte alle Bundesbehörden und deren Aufgaben und Zuständigkeiten im Zusammenhang mit der Zusammenarbeit mit Facebook auflisten)?

Das BSI arbeitet im Rahmen seines gesetzlichen Auftrags in Bezug auf das Thema Informationssicherheit mit Facebook zusammen.

5. Kann die Bundesregierung ausschließen, dass Wahlmanipulationen und Wahlbeeinflussungen zukünftig bei Wahlen zum Europäischen Parlament, bei der Bundestagswahl und bei Landtagswahlen stattfinden?

Nein.

6. Welche konkreten Maßnahmen hat die Bundesregierung schon umgesetzt, um Wahlen sicherer vor Wahlbeeinflussung und Wahlmanipulation zu machen, und damit die festgeschriebenen demokratischen Werte in der Bundesrepublik Deutschland zu schützen?
7. Welche konkreten Maßnahmen plant die Bundesregierung, um Wahlen sicherer vor Wahlbeeinflussung und Wahlmanipulation zu machen, und damit die festgeschriebenen demokratischen Werte in der Bundesrepublik Deutschland zu schützen?

Die Fragen 6 und 7 werden gemeinsam beantwortet.

Zur Reduzierung der Risiken für die Sicherheit von Netz- und Informationssystemen, die für die Organisation der Wahl zum Europäischen Parlament genutzt werden, hat eine Bund-Länder-Arbeitsgruppe mit dem Bundeswahlleiter und dem BSI im Jahr 2018 Maßnahmen zur Absicherung der Übermittlung der Ergebnisse in der Wahlnacht ausgearbeitet. Die Maßnahmen betreffen nur die Ermittlung des vorläufigen Wahlergebnisses in der Wahlnacht, nicht die Ermittlung des endgültigen Wahlergebnisses, das nach der Wahl anhand der schriftlichen Wahlniederschriften ermittelt wird.

Die Stimmabgabe selbst erfolgt in Deutschland auch bei den Europawahlen in Folge des Urteils des Bundesverfassungsgerichts vom 3. März 2009 (BVerfGE 123, 39) ausschließlich papierbasiert und ist daher nicht von der Sicherheit von Netz- und Informationssystemen abhängig und darum insofern nicht manipulationsanfällig.

Die Verbesserung der Widerstandsfähigkeit von Kritischen Infrastrukturen im Bereich der Cybersicherheit hat die Bundesregierung bereits durch das IT-Sicherheitsgesetz von 2015 adressiert. Im Kern beinhaltet das IT-Sicherheitsgesetz verpflichtende Mindestsicherheitsstandards und Meldepflichten für Betreiber Kritischer Infrastrukturen.

Dieser Ansatz wurde durch das NIS-Umsetzungsgesetz 2017 insbesondere durch die Befugnis zur Einrichtung von Mobile Incident Response Teams (MIRTs) beim BSI zur Unterstützung von Betreibern Kritischer Infrastrukturen bei Cybersicherheitsvorfällen ergänzt und soll in der laufenden Legislaturperiode auch gesetzlich weiterentwickelt werden.

Am 1. Oktober 2017 ist zudem das Netzwerkdurchsetzungsgesetz in Kraft getreten, das Compliance-Regeln einführt, um soziale Netzwerke zu einer schnellen Bearbeitung von Nutzerbeschwerden über strafbare Hasskriminalität, strafbare Falschnachrichten und andere bestimmte strafbare Inhalte anzuhalten.

Sofern die ordnungsgemäße Durchführung der Europawahl in erheblichem Umfang gestört werden sollte, kann das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe seine Kommunikationskanäle für Warnhinweise an die Bevölkerung für amtliche Mitteilungen des Bundeswahlleiters verfügbar machen. Die Verfahrensweise war bereits für die Bundestagswahl 2017 vorgesehen.

Zur Sensibilisierung der Beteiligten weisen die Sicherheitsbehörden von Bund und Ländern in verschiedenen Veröffentlichungen regelmäßig auf die bestehenden Cyberbedrohungen hin. Zur Gewährleistung der IT-Sicherheit der Europawahl 2019 besteht zwischen dem Bundeswahlleiter, den Landeswahlleitern und dem BSI bereits ein enges Kooperationsverhältnis. Das BSI hat vor der Bundestagswahl 2017 Parteien und politischen Stiftungen zu Fragen der IT-Sicherheit beraten und will diese Beratung als dauerhaftes Angebot fortführen. Zur Abwehr von Versuchen politischer Einflussnahme – auch mittels Social Bots – hat das Bundesamt für Verfassungsschutz bereits vor der Bundestagswahl 2017 Akteure in Politik und Medien sowie die Öffentlichkeit entsprechend sensibilisiert, um das Bewusstsein für solche Aktivitäten zu schärfen und die Gefahr negativer Auswirkungen zu minimieren. Diese Aufklärungsaktivitäten werden auch mit Blick auf die Europawahl 2019 fortgesetzt.

Hinsichtlich der von Social Bots ausgehenden Gefahren wird auf den Medien- und Kommunikationsbericht der Bundesregierung 2018 (Bundestagsdrucksache 19/6970) sowie auf die Antwort der Bundesregierung auf die Schriftliche Frage 29 des Abgeordneten Konstantin Kuhle auf Bundestagsdrucksache 19/6663 hingewiesen.

8. Hat die Bundesregierung die Amadeu-Antonio-Stiftung in irgendeiner Weise in die Gespräche mit Facebook bzw. die Umsetzung der Maßnahmen gegen Fake News bzw. Hate Speech mit einbezogen oder plant sie, diese mit einzubeziehen?

Wenn ja, wie?

Im Zusammenhang mit der Bekämpfung von Wahlmanipulationen im Vorfeld der Wahlen zum Europäischen Parlament im Mai 2019 hat die Bundesregierung die Amadeu-Antonio-Stiftung bisher nicht in Gespräche oder in die entsprechende Umsetzung von Maßnahmen gegen Fake News und/oder Hate Speech mit Facebook eingebunden. Dies ist auch nicht geplant.

9. Kann die Bundesregierung bestätigen, dass die EU-Kommission, namentlich der EU-Sicherheitskommissar Julian King, die EU-Mitgliedstaaten schon im Sommer 2018 auf die Gefahren von Manipulationen und Einflüssen, vor allem über soziale Netzwerke, im Hinblick auf die EU-Wahl 2019 gewarnt hat?

Wenn ja, wie, und in welchem Umfang fiel diese Warnung aus?

Der EU-Kommissar für die Sicherheitsunion Julian King hat im Rahmen verschiedener Veranstaltungen vor einer Gefährdung der Europawahl 2019 durch Desinformation und Cyberangriffe gewarnt (vgl. die auf der Homepage der Europäischen Kommission einsehbaren Pressemeldungen

- [https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-speech-cert-eu-conference-2018\\_en](https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-speech-cert-eu-conference-2018_en),
- [https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-remarks-symposium-german-domestic-intelligence-service-hybrid-threats\\_en](https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-remarks-symposium-german-domestic-intelligence-service-hybrid-threats_en),
- [https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-speech-centre-european-policy-studies-how-tackle-cyber-threats-digital\\_en](https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-speech-centre-european-policy-studies-how-tackle-cyber-threats-digital_en),
- [https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-remarks-press-conference-commission-proposals-tackle-spread-disinformation-online\\_en](https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-remarks-press-conference-commission-proposals-tackle-spread-disinformation-online_en)).

10. Wurde im Zusammenhang mit Frage 9 von der EU-Kommission eine schriftliche Unterrichtung mit einer Gefahrenanalyse und/oder Vorschlägen zur Gefahrenabwehr an die Bundesregierung gesandt, und wenn ja, mit welchem Inhalt, und ist diese öffentlich einsichtig?

Die Europäische Kommission hat bereits in ihrer Mitteilung vom 26. April 2018 zur Bekämpfung von Desinformation im Internet (COM(2018) 236 final) verschiedene Maßnahmen u. a. zur Verbesserung der Online-Transparenz und gegen Desinformationskampagnen im Kontext der Europawahlen vorgeschlagen. Dazu gehört die Ausarbeitung eines ehrgeizigen Verhaltenskodex, der auch den Umgang mit Social Bots umfassen soll. Online-Plattformen und Werbeindustrie sollen sich u. a. verpflichten, Kennzeichnungsregeln und -systeme für Bots zu entwickeln und zu gewährleisten, dass die Tätigkeit von Bots nicht mit menschlicher Interaktion verwechselt wird. Am 26. September 2018 hat die Industrie einen der Kommissions-Mitteilung entsprechenden Verhaltenskodex vorgelegt, der u. a. eine Selbstverpflichtung vorsieht, klare Regeln gegen den Missbrauch automatisierter Bots aufzustellen und diese innerhalb der EU durchzusetzen (<https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>). Zu den Unterzeichnern gehören die Online-Plattformen Facebook, Google und Twitter.

Am 12. September 2018 hat die Europäische Kommission ein Maßnahmenpaket zur Gewährleistung freier und fairer Europawahlen vorgelegt.

Neben dem darin enthaltenen Vorschlag für eine Änderung der Verordnung (EU, Euratom) Nr. 1141/2014 des Europäischen Parlaments und des Rates vom 22. Oktober 2014 über das Statut und die Finanzierung europäischer politischer Parteien und europäischer politischer Stiftungen (ABl. 2014 L 317, S. 1) im Hinblick auf ein Überprüfungsverfahren für im Zusammenhang mit Wahlen zum Europäischen Parlament begangene Datenschutzverstöße (COM (2018) 636) sind als nicht-legislative Teile des Maßnahmenpakets zu nennen:

- a) die Mitteilung der Kommission an Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über das Maßnahmenpaket (Dokument COM(2018) 637 final),
- b) der Leitfaden zur Anwendung des EU-Datenschutzrechts in Zusammenhang mit Wahlen (Dokument COM (2018) 638 final) sowie
- c) die Empfehlung der Kommission zu Wahlkooperationsnetzen, zu Online-Transparenz, zum Schutz vor Cybersicherheitsvorfällen und zur Bekämpfung von Desinformationskampagnen im Zusammenhang mit Wahlen zum Europäischen Parlament (Dokument C(2018) 5949 final).

In dem unter c) genannte Dokument empfiehlt die Kommission den Mitgliedstaaten unter anderem die Einrichtung von aus Wahlbehörden, Sicherheitsbehörden und Datenschutzbehörden bestehenden nationalen Wahlkooperationsnetzwerken sowie eines europäischen Wahlkooperationsnetzwerkes, die Unterrichtung der Behörde für europäische politische Parteien und europäische politische Stiftungen über jede Entscheidung, mit der Datenschutzverstöße, die auf eine Einflussnahme der Europawahlen zielen, festgestellt wurden, die Verhängung angemessener Sanktionen bei Verstößen gegen die Vorschriften zum Schutz personenbezogener Daten im Zusammenhang mit den Europawahlen, die Förderung der Transparenz bezahlter politischer Werbeanzeigen im Vorfeld der Europawahlen sowie die Ergreifung angemessener Maßnahmen zum Schutz der Sicherheit, Authentizität, Vertraulichkeit und Integrität der Wahlsysteme in jeder Wahlphase der Europawahlen. Zudem empfiehlt die Kommission darin den europäischen und nationalen politischen Parteien und Stiftungen sowie Wahlkampforganisationen, geeignete Maßnahmen zu treffen, um sich vor Cyberangriffen zu schützen.

Am 5. Dezember 2018 hat die Europäische Kommission den Aktionsplan gegen Desinformation vorgelegt (JOIN(2018) 36 final).

Die genannten Dokumente wurden auf der Internetseite der Europäischen Kommission veröffentlicht und sind auch im bundestagseigenen Informationssystem EuDoX hinterlegt.

11. Nimmt die Bundesregierung die Aussagen, Analysen und Einschätzungen der EU-Kommission und des EU-Sicherheitskommissars in Bezug auf Wahlmanipulationen und Einflüsse als Bedrohung demokratischer Prozesse wahr?

Wenn ja, wurden in diesem Zusammenhang auch Analysen und Einschätzungen der EU-Kommission in Bezug auf Internetplattformen wie Facebook, Google, Twitter usw. angefordert bzw. abgefragt, um die Lage in der Bundesrepublik Deutschland besser bewerten zu können?

Die Bundesregierung nimmt die Aussagen, Analysen und Einschätzungen der Europäischen Kommission zu den Möglichkeiten der Manipulation und Beeinflussung von Wahlen nicht als Bedrohung demokratischer Prozesse wahr, sondern als einen Beitrag zu deren Schutz.

Eine gesonderte Anforderung von Analysen und Einschätzungen der Europäischen Kommission durch die Bundesregierung fand nicht statt.

Die Bundesregierung befindet sich in ständigem Austausch sowohl mit der Europäischen Kommission als auch mit anderen EU-Mitgliedstaaten.

12. Hat die Bundesregierung eigene Analysen und Einschätzungen über Internetplattformen dahingehend erhoben, um Sicherheitslecks rund um den Datenschutz vor allem im Hinblick auf den Datenschutzskandal Cambridge Analytica vorbeugen zu können und zukünftig abwehren zu können?

Auf die Antwort der Bundesregierung zu Frage 1 der Kleinen Anfrage der Fraktion der FDP „Zusammenarbeit zwischen Facebook und Definers“ auf Bundestagsdrucksache 19/6782 wird verwiesen. Die Überwachung und Anwendung der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) obliegt ausschließlich den unabhängigen Datenschutzaufsichtsbehörden.

13. Hat die Bundesregierung dem Drängen der EU-Kommission auf vorbeugende Sicherheitsmaßnahmen in Bezug auf Wahlmanipulationen zur EU-Wahl 2019 dahingehend Folge geleistet und nationale Pläne zur Vorbeugung und Abwehr von Cyberangriffen und Desinformation, wie von der EU-Kommission gefordert, erstellt?
14. Wenn ja, welche konkreten Pläne wurden aufgrund der Informationen der EU-Kommission (Frage 13) von der Bundesregierung aufgestellt?
15. Welche Bundesbehörden wurden mit der Umsetzung solcher nationalen Pläne (Frage 13) betraut, und sind diese Pläne schon umsetzungsreif?

Die Fragen 13 bis 15 werden gemeinsam beantwortet.

Auf die Antworten zu den Fragen 6, 7 und 10 sowie auf die Antworten der Bundesregierung auf die Schriftlichen Fragen 32 und 33 des Abgeordneten Alexander Graf Lambsdorff auf Bundestagsdrucksache 19/5155 und die Schriftliche Frage 27 der Abgeordneten Franziska Brantner auf Bundestagsdrucksache 19/6961 sowie auf die Antwort der Bundesregierung auf die Mündliche Frage 48 der Abgeordneten Renate Künast in der Fragestunde vom 16. Januar 2019 (Plenarprotokoll 19/73, S. 8563) wird verwiesen.

