Deutscher Bundestag **Drucksache 21/5919**

21. Wahlperiode 13.05.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Tobias Matthias Peterka, Thomas Fetsch, Ulrich von Zons, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/5638 –

Deepfakes, digitale Persönlichkeitsrechtsverletzungen und Wirksamkeit bestehender rechtlicher Instrumente

Vorbemerkung der Fragesteller

Täuschend echte, aber künstlich erzeugte Videos, Bilder oder Tonaufnahmen (sog. Deepfakes) eröffnen neue Möglichkeiten digitaler Manipulation. Sie können gezielt zur Rufschädigung, Täuschung und Demütigung von Personen eingesetzt werden, insbesondere im Zusammenhang mit Identitätsmissbrauch oder sexualisierten Darstellungen.

Einzelne öffentlich bekannt gewordene Fälle digitaler Identifikationsmanipulation zeigen, dass entsprechende Handlungen über längere Zeiträume erfolgen können, ohne dass Betroffene wirksamen Schutz erfahren oder eine effektive Strafverfolgung stattfindet (www.welt.de/politik/deutschland/article69c9f1bbb33459bf52773dcf/digitale-gewalt-bundesjustizministerin-hubig-kuendigt-neue-gesetze-an-deepfakes-sollen-strafbar-werden.html). Gleichzeitig ist unklar, in welchem Umfang entsprechende Fälle tatsächlich auftreten und inwieweit diese durch staatliche Stellen systematisch erfasst werden.

Vor diesem Hintergrund ist bekannt geworden, dass die Bundesministerin der Justiz und für Verbraucherschutz, Dr. Stefanie Hubig, einen Referentenentwurf zur besseren Bekämpfung digitaler Persönlichkeitsrechtsverletzungen vorgelegt hat (www.welt.de/politik/deutschland/article69c9f1bbb33459bf52773dcf/digitale-gewalt-bundesjustizministerin-hubig-kuendigt-neue-gesetze-an-deepfakes-sollen-strafbar-werden.html). Dieser Referentenentwurf ist Gegenstand öffentlicher Berichterstattung und fachlicher Stellungnahmen, lag jedoch zunächst dem Deutschen Bundestag nicht vor und war nach Kenntnis der Fragesteller zuerst auch nicht offiziell veröffentlicht worden.

In der rechtswissenschaftlichen und anwaltlichen Praxis wird dieser Vorstoß teilweise kritisch bewertet, insbesondere mit Blick auf die Frage, ob ein hinreichender empirischer Regelungsbedarf besteht oder ob bestehende straf- und zivilrechtliche Vorschriften bereits ausreichend sind, deren Anwendung und Durchsetzung jedoch Defizite aufweisen (www.lto.de/recht/hintergruende/h/gesetz-digitale-gewalt-hubig-gesetz-deepfakes-kritik-dav).

Zugleich bestehen auf europäischer Ebene umfangreiche Regulierungen für digitale Plattformen sowie für den Einsatz künstlicher Intelligenz, insbesondere durch den Digital Services Act sowie die geplanten Regelungen zur künstli-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Justiz und für Verbraucherschutz vom 12. Mai 2026 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

chen Intelligenz (KI). Dennoch kommt es weiterhin zu entsprechenden Vorfällen. Dies wirft aufseiten der Fragesteller die Frage auf, ob bestehende Regelungen in der Praxis greifen oder ob zusätzliche gesetzgeberische Maßnahmen tatsächlich geeignet sind, die Probleme wirksam zu adressieren.

Vor diesem Hintergrund besteht bei den Fragestellern Aufklärungsbedarf hinsichtlich der tatsächlichen Verbreitung entsprechender Fälle, der Erfassbarkeit durch staatliche Stellen, der Wirksamkeit bestehender Regelungen sowie möglicher rechtlicher und tatsächlicher Vollzugsdefizite – auch im internationalen Kontext.

1. Welche konkreten Erkenntnisse liegen der Bundesregierung über die Anzahl von Fällen digitaler Persönlichkeitsrechtsverletzungen durch manipulierte oder künstlich erzeugte Inhalte seit 2020 vor (bitte nach Jahren und, soweit möglich, Deliktsgruppen aufschlüsseln)?

Der Bundesregierung liegen keine über öffentliche Quellen hinausgehenden Informationen zu der Anzahl von Fällen digitaler Persönlichkeitsrechtsverletzungen durch manipulierte oder künstlich erzeugte Inhalte seit 2020 vor.

2. Wenn der Bundesregierung hierzu keine belastbaren Zahlen vorliegen (vgl. Frage 1), aus welchen Gründen werden entsprechende Fälle bislang nicht gesondert statistisch erfasst?

Die Erfassung in der Polizeilichen Kriminalstatistik (PKS) orientiert sich im Wesentlichen an den entsprechenden Normen des Strafgesetzbuches (StGB) beziehungsweise strafrechtlicher Nebengesetze. Strafrechtlich können bei solchen Sachverhalten je nach Einzelfall verschiedene Straftatbestände erfüllt werden. Zu diesen Straftatbeständen erfolgt jeweils eine PKS-Erfassung.

In der PKS werden beispielsweise Betrugsstraftaten, die mithilfe von Künstlicher Intelligenz begangen wurden, unter dem allgemeinen Straftatenschlüssel „Betrug“ (510000) subsumiert, allerdings ist hierbei das Vorliegen einer Täuschung maßgeblich. Eine gesonderte Aufgliederung nach mit Künstlicher Intelligenz gestützten Betrugsstraftaten erfolgt im Rahmen der PKS nicht.

Bei den insoweit einschlägigen Statistischen Berichten „Staatsanwaltschaft“ und „Strafgerichte“ handelt es sich um Verfahrensstatistiken, deren Durchführungen auf bundeseinheitlichen Verwaltungsanordnungen der Länder basieren.

Eine Erfassung entspricht nicht der Systematik der Statistiken, bei denen es sich gemäß § 3 Absatz 3 des Bundestatistikgesetzes um zu einem Bundesergebnis zusammengefasste Länderstatistiken handelt.

3. Welche bestehenden amtlichen Statistiken enthalten nach Kenntnis der Bundesregierung zumindest mittelbar Informationen zu entsprechenden Sachverhalten, und warum hält die Bundesregierung diese für ausreichend bzw. nicht ausreichend?

Es wird auf die Antwort zu Frage 2 verwiesen.

4. Welche Maßnahmen hat die Bundesregierung bislang ggf. ergriffen oder plant sie, zu ergreifen, um eine belastbare Datengrundlage zu schaffen?

Die Berichterstattungsstelle geschlechtsspezifische Gewalt ist mit der kontinuierlichen und unabhängigen innerstaatlichen Berichterstattung zur Umsetzung der Istanbul-Konvention (Artikel 10 der Istanbul-Konvention) beauftragt. Die

Berichterstattungsstelle trägt unter anderem mit dem periodischen Bericht „Monitor Gewalt gegen Frauen“ dazu bei, eine breite und belastbare Datengrundlage zu schaffen, die auch die digitale Dimension von Gewalt gegen Frauen umfasst.

Im Übrigen wird auf die Antwort zu Frage 2 verwiesen.

5. Inwieweit liegen der Bundesregierung ggf. Erkenntnisse über ein mögliches Dunkelfeld bei entsprechenden Delikten, vor und auf welche konkreten Quellen stützen sich diese Erkenntnisse?

Die geschlechterübergreifende Dunkelfeldbefragung LeSuBiA (Lebenssituation, Sicherheit und Belastung im Alltag, www.bka.de/lesubia), die das Bundeskriminalamt (BKA) in Kooperation mit dem Bundesministerium des Innern und dem Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend durchführt, hat neben Partnerschaftsgewalt und sexualisierte Gewalt auch das Thema digitale Gewalt als Schwerpunkt. Im ersten Themenheft wird digitale Gewalt in einem gesonderten Kapitel ausgewertet (Leitgöb-Guzy und Bieber 2026, Kapitel 4.4, Seite 97-106). In Kapitel 4.4.1. werden Lebenszeit- und 5-Jahresprävalenzen zu verschiedenen digitalen Gewalterfahrungen i. e. S. dargestellt.

Hier sind Auswertungen der Lebenszeit- und 5-Jahresprävalenz dargestellt (Seite 99; unter anderem auch Item „Informationen oder Bilder über Sie im Internet manipuliert“; 5-Jahresprävalenz bei Frauen: 0,7 Prozent und bei Männern: 0,8 Prozent). Die Anzeigequote bei digitaler Gewalt i.e.S. (insgesamt, nicht nur Deepfake) liegt bei Frauen bei 2,4 Prozent und bei Männern bei 0,9 Prozent (Seite 101).

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) hat im Auftrag des Ausschusses für Forschung, Technologie, Raumfahrt und Technikfolgenabschätzung die Kurzstudie „Rechtliche und gesellschaftliche Herausforderungen und Potenziale von Deepfakes“ erstellt (Bundestagsdrucksache 21/3952). Dort wird auf Studien Bezug genommen, die davon ausgehen, dass ein Großteil der Deepfakes (96 bzw. 98 Prozent) pornografischer Art sind (Abschnitt 3.7 m. w. N.). Das TAB hebt jedoch hervor, dass nicht klar ist, wie belastbar diese Ergebnisse sind, und dass es an empirischer Forschung hierzu fehlt. Als Beispiel nennt das TAB die Plattform MrDeepFakes, die nahezu 70 000 Videos und Bilder mit nicht einvernehmlichen sexualisierten Deepfakes mit milliardenfachen Aufrufen angeboten und 650 000 Nutzern auch die Erstellung von Deepfakes angeboten haben soll.

6. Welche Straftatbestände werden nach Kenntnis der Bundesregierung derzeit typischerweise auf Fälle digitaler Identitätsmanipulation angewendet?

Es wird Bezug genommen auf die Ausführungen zur strafrechtlichen Erfassung des „Identitätsmissbrauchs“ auf Seite 19 des Referentenentwurfs des Bundesministeriums der Justiz und für Verbraucherschutz – Entwurf eines Gesetzes zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt (abrufbar unter www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_GgdG.pdf?__blob=publicationFile&v=2).

7. Wie viele Ermittlungsverfahren wurden nach Kenntnis der Bundesregierung seit 2020 im Zusammenhang mit digitaler Identitätsmanipulation, der Verwendung von manipulierten oder künstlich erzeugten Bild-, Ton- oder Videomaterials oder vergleichbaren Formen digitaler Persönlichkeitsrechtsverletzungen geführt (bitte nach Jahren und, soweit möglich, zugrunde liegenden Straftatbeständen aufschlüsseln)?

Daten zu Ermittlungsverfahren liegen auf Basis der PKS grundsätzlich nicht vor. In ihr werden die der Polizei bekanntgewordenen und durch sie endbearbeiteten Straftaten, einschließlich der mit Strafe bedrohten Versuche und der vom Zoll bearbeiteten Rauschgiftdelikte, erfasst. Nicht enthalten sind Staatsschutzdelikte, Verkehrsdelikte (mit Ausnahme der Verstöße gegen §§ 315, 315b StGB und § 22a des Straßenverkehrsgesetzes), Ordnungswidrigkeiten und Verstöße gegen strafrechtliche Landesgesetze, mit Ausnahme der einschlägigen Vorschriften in den Landesdatenschutzgesetzen.

Im Übrigen wird auf die Antworten zu den Fragen 1 und 2 verwiesen.

8. In wie vielen dieser in Frage 7 erfragten Verfahren konnten nach Kenntnis der Bundesregierung Tatverdächtige identifiziert werden?

Es wird auf die Antworten zu den Fragen 1 und 7 verwiesen.

9. Wenn hierzu (vgl. Vorfragen) keine gesonderten Daten vorliegen, aus welchen Gründen erfolgt keine entsprechende Erfassung, und welche Schlussfolgerungen zieht die Bundesregierung aus dem Fehlen entsprechender Daten im Hinblick auf die Wirksamkeit der Strafverfolgung?

Es wird auf die Antwort zu Frage 2 verwiesen.

Ohne eine entsprechende Norm oder hinreichende Konkretisierung des Deliktsbereichs kann keine Betrachtung erfolgen. Unklar ist zudem, was unter „Wirksamkeit der Strafverfolgung“ im Sinne der Fragestellung gemeint ist.

10. Wenn eine entsprechende differenzierte Erfassung von Ermittlungsverfahren im Sinne von Frage 7 nicht erfolgt, welche fachlichen oder praktischen Gründe sprechen nach Auffassung der Bundesregierung dagegen, entsprechende Verfahren gesondert auszuwerten?

Es wird auf die Antwort zur Frage 2 verwiesen.

11. Welche konkreten praktischen Schwierigkeiten bestehen nach Kenntnis der Bundesregierung bei der Strafverfolgung in diesem Zusammenhang (insbesondere Beweisführung, Täteridentifikation, internationale Zuständigkeit)?

Für die Strafverfolgung sind die Staatsanwaltschaften der Länder und ihre Ermittlungspersonen zuständig.

Allgemein lässt sich feststellen, dass die Anonymität des Internets die Strafverfolgungsbehörden vor allem im Bereich der Identifizierung mutmaßlicher Tatverdächtiger vor Herausforderungen stellt. Damit die Identität von Tatverdächtigen künftig häufiger aufgeklärt werden kann, hat die Bundesregierung am 22. April 2026 den Gesetzentwurf zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren beschlossen.

12. Inwieweit hat die Bundesregierung ggf. geprüft, ob bestehende strafrechtliche Vorschriften in der Praxis konsequent angewendet werden, und wenn eine solche Prüfung erfolgt ist, zu welchem Ergebnis ist diese Prüfung gelangt?

Mit dem vorgelegten Referentenentwurf (vergleiche Antwort auf Frage 6) wird auf eine insbesondere von Betroffenen digitaler Gewalt, der Praxis und aus der Wissenschaft wiederholt und nachdrücklich erhobene Forderung, das Strafrecht an die neuen Phänomene des digitalen Zeitalters anzupassen, reagiert. Vor dem Hintergrund, dass ein wesentlicher Teil der öffentlichen und privaten Kommunikation mittlerweile im virtuellen Raum stattfindet und es in diesem Kontext insbesondere in sozialen Netzwerken immer wieder auch zu rechtswidrigen Inhalten wie bildbasierter sexualisierter Gewalt (etwa in Form von KI-generierten sexualisierten Deepfakes) kommt, war ein gesetzgeberisches Vorgehen erforderlich. Ergänzend wird auf die Ausführungen in der Begründung des Referentenentwurfs, insbesondere Seite 23 folgend, Bezug genommen.

13. Hält die Bundesregierung die bestehenden strafrechtlichen Vorschriften für ausreichend, um Persönlichkeitsrechtsverletzungen durch Deepfakes effektiv zu erfassen, und wenn ja, warum?

14. Wenn die Bundesregierung dies verneint (vgl. Frage 13), welche konkreten Fallkonstellationen werden nach ihrer Auffassung derzeit nicht vom geltenden Recht erfasst?

15. Inwieweit betreffen etwaige Regelungslücken insbesondere Fälle vollständig künstlich erzeugter Inhalte ohne reale Vorlage?

Die Fragen 13 bis 15 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Es wird Bezug genommen auf die Ausführungen zum geltenden und künftigen Recht auf Seite 23 folgend des Referentenentwurfs (vergleiche Antwort auf Frage 6). Insbesondere wird künftig schon das Herstellen sexualisierter Deepfakes unter Strafe stehen.

16. Welche zivilrechtlichen Ansprüche stehen Betroffenen derzeit zur Verfügung, und welche Erkenntnisse liegen der Bundesregierung zu deren praktischer Durchsetzbarkeit vor (vgl. Vorfragen)?

Deepfakes können einen Eingriff in das Recht am eigenen Bild nach § 22 des Kunsturheberrechtsgesetzes sowie einen Eingriff in das Allgemeine Persönlichkeitsrecht darstellen. Insoweit können Unterlassungs- und gegebenenfalls auch Schadensersatzansprüche der betroffenen Person gemäß § 823 des Bürgerlichen Gesetzbuches (BGB) gegebenenfalls i. V. m. Artikel 2 Absatz 1 und Artikel 1 Absatz 1 des Grundgesetzes beziehungsweise § 1004 BGB bestehen.

Die Durchsetzung dieser Ansprüche stößt in der Praxis oft auf erhebliche Hürden. Ein zentrales Hindernis ist die Identifizierung der schädigenden Person: Da die Täter oft unter Pseudonymen bei den Diensteanbietern registriert sind, bleibt dem Betroffenen die für eine Klage notwendige ladungsfähige Anschrift ohne Schaffung einer gerichtlichen Hilfe verborgen. Betroffene sind daher häufig auf kostspielige und langwierige Vorbereitungen angewiesen. In der aktuellen Rechtspraxis führt das Fehlen der Nutzerdaten dazu, dass Betroffene von digitaler Gewalt oft den Umweg über das Strafverfahren wählen, indem sie Strafanzeige erstatten, bevor sie eine zivilrechtliche Klage erheben.

17. Welche konkreten Verpflichtungen ergeben sich für Plattformbetreiber aus dem Digital Services Act im Umgang mit Deepfake-Inhalten?

Die Regelungen zu systemischen Risiken sind ein Werkzeug des Digital Services Act (DSA), das bei rechtswidrigen Deepfakes helfen kann.

Sie verpflichten sehr große Online-Plattformen, Maßnahmen zu ergreifen, um systemische Risiken, zum Beispiel die massenhafte Verbreitung rechtswidriger Inhalte, zu analysieren und zu mindern. Diese Risikominderungsmaßnahmen können nach dem DSA ausdrücklich insbesondere auch die Sicherstellung der Kennzeichnungen von Deepfakes sowie die Bereitstellung einer entsprechenden Anzeigefunktion für Nutzerinnen und Nutzer umfassen.

Darüber hinaus enthält der DSA für Plattformbetreiber keine gesonderten Verpflichtungen zu Deepfakes. Der DSA trägt als horizontale Regelung aber allgemein dazu bei, rechtswidrige Inhalte auf Plattformen zu bekämpfen. Die allgemeinen Regeln des DSA können daher auch helfen, Deepfakes einzudämmen, soweit diese rechtswidrig sind. Der DSA ist damit bei rechtswidrigen Deepfakes ein hilfreiches Werkzeug neben anderen – etwa neben bestehenden straf- und zivilrechtlichen Instrumenten.

Zentral – auch bei Deepfakes – sind zudem die Melde- und Abhilfeverfahren für rechtswidrige Inhalte, die alle Plattformen nach dem DSA vorhalten müssen. Sie ermöglichen Betroffenen und Dritten, potenziell rechtswidrige Deepfakes direkt zu melden. Plattformen sind dann haftbar, wenn sie trotz Meldung rechtswidrige Deepfakes nicht löschen oder den Zugang nicht sperren. Diese Haftung bestimmt sich allerdings nicht nach dem DSA, sondern nach dem allgemeinen Zivilrecht oder sonstigen Fachrecht.

18. Welche Erkenntnisse liegen der Bundesregierung ggf. zur praktischen Wirksamkeit dieser Regelungen vor, insbesondere hinsichtlich der Geschwindigkeit und Vollständigkeit von Löschungen, und auf welche konkreten Quellen oder eigenen Erhebungen stützt sie diese Erkenntnisse gegebenenfalls?

19. Wenn der Bundesregierung hierzu keine eigenen Erkenntnisse vorliegen (vgl. Frage 18), auf welche Daten oder Studien stützt sie ihre Bewertung der Wirksamkeit des Digital Services Act?

Die Fragen 18 und 19 werden wegen Sachzusammenhangs gemeinsam beantwortet.

Der europäische Gesetzgeber hat vorgeschrieben, dass die Europäische Kommission den DSA bis November 2027 evaluiert. Hintergrund dabei ist, dass der DSA erst seit Februar 2024 vollumfänglich wirksam ist. Eine Evaluierung Ende 2027 gibt also allen Beteiligten Zeit, tatsächlich Erfahrungen mit dem DSA zu sammeln, um die Wirksamkeit des DSA seriös bewerten zu können.

20. Welche konkreten Grenzen bestehen bei der Anwendung dieser Regelungen (vgl. Vorfragen), insbesondere bei Anbietern außerhalb der Europäischen Union oder bei nicht öffentlichen Kommunikationskanälen?

Generell lassen sich Regelungen stets schwerer durchsetzen, wenn Rechtssubjekte ihren Sitz, ihr Personal und ihre Infrastruktur ausschließlich außerhalb der Europäischen Union haben. Mit dieser tatsächlichen Herausforderung bei der Rechtsdurchsetzung sieht sich auch der DSA konfrontiert.

21. Welche konkreten Anforderungen bestehen auf europäischer Ebene für Anbieter generativer KI im Hinblick auf Transparenz und Kennzeichnung von Inhalten?

Nach Artikel 50 der Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (KI-VO) müssen Anbieter und Betreiber von KI-Systemen, einschließlich KI-Systemen mit allgemeinem Verwendungszweck, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, sicherstellen, dass die Ausgaben des KI-Systems in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind.

22. Welche Behörden sind in Deutschland für die Durchsetzung dieser in Frage 21 erfragten Anforderungen zuständig, und wie erfolgt die praktische Kontrolle und Durchsetzung dieser Anforderungen?

Der Entwurf eines Gesetzes zur Durchführung der Verordnung über künstliche Intelligenz (Bundestagsdrucksache 21/4594), der aktuell Gegenstand der parlamentarischen Beratungen ist, sieht vor, dass die für die KI-VO in § 2 des Entwurfs des KI-Marktüberwachungs- und Innovationsförderungsgesetzes benannten Marküberwachungsbehörden die Aufsicht in ihren jeweiligen Sektoren umfassend sowohl über die Hochrisiko-KI-Systeme (Kapitel III KI-VO) als auch über verbotene Praktiken im KI-Bereich (Artikel 5 KI-VO) und die Transparenz- bzw. Kennzeichnungspflichten (Artikel 50 KI-VO) übernehmen. Die Befugnisse der Marktüberwachungsbehörden ergeben sich gemäß Gesetzentwurf insbesondere aus Artikel 14 Absatz 4 und 5 und Artikel 16 der Verordnung (EU) 2019/1020 sowie nach der KI-VO.

23. Welche Erkenntnisse liegen der Bundesregierung zur Einhaltung dieser Anforderungen vor (vgl. Frage 22)?

Artikel 50 der KI-VO ist nach geltender KI-VO ab dem 2. August 2026 anwendbar. Erkenntnisse zur Einhaltung der Anforderungen liegen daher noch nicht vor.

24. Wenn hierzu (vgl. Frage 23) keine Erkenntnisse vorliegen, wie begründet die Bundesregierung die Annahme, dass bestehende Regelungen ausreichend sind?

Die Transparenzverpflichtungen nach Artikel 50 KI-VO beziehen sich umfassend auf KI-generierte Inhalte (siehe Antwort auf Frage 21).

25. Welche Schnittstellenprobleme bestehen nach Auffassung der Bundesregierung zwischen KI-Regulierung und geltendem Straf- und Zivilrecht gegebenenfalls?

Die Bundesregierung berücksichtigt bei der KI-Regulierung das geltende Straf- und Zivilrecht und achtet darauf, potentielle Schnittstellenprobleme zu vermeiden.

26. Welche konkreten Schwierigkeiten bestehen bei der Strafverfolgung nach Auffassung der Bundesregierung ggf., wenn Täter oder technische Infrastruktur im Ausland angesiedelt sind?

Muss über Landesgrenzen hinweg ermittelt werden, stellen die zuständigen Behörden regelmäßig Rechtshilfeersuchen, was mit Zeitverlust einhergehen kann. Hier soll das ab Sommer 2026 geltende E-Evidence-Paket der Europäischen Union (EU) Abhilfe schaffen: Diensteanbieter (auch aus Drittstaaten), die auf dem EU-Markt tätig sind, müssen künftig einen Empfangsbevollmächtigten in einem EU-Mitgliedstaat einrichten, der Entscheidung und Anordnungen zur Erhebung elektronischer Beweismittel umzusetzen hat. Grundlage hierfür kann die E-Evidence-Verordnung sein, die Richtlinie über die Europäische Ermittlungsanordnung oder das EU-Rechtshilfeübereinkommen aus dem Jahre 2000. Soweit die E-Evidence-Verordnung angewendet wird, haben die Anbieter die angefragten Daten unmittelbar herauszugeben oder zu sichern. Die grenzüberschreitende Ermittlung wird damit künftig erheblich erleichtert.

27. Welche rechtlichen und tatsächlichen Möglichkeiten bestehen, rechtsverletzende Inhalte aus Drittstaaten entfernen zu lassen (vgl. Frage 26)?

Aufgrund der primären Zuständigkeit der Länder für die Bereiche des Gefahrenabwehr- und Medienrechts ist die gesetzliche Regelung von Lösch- oder Sperranordnungsbefugnissen sowie deren Durchsetzung in Deutschland in erster Linie Aufgabe der Länder. Anordnungen über die Löschung und Sperrung rechtswidriger Inhalte im Netz, die eine Störung der öffentlichen Sicherheit darstellen, können zunächst im Rahmen eines allgemeinen gefahrenabwehrrechtlichen Vorgehens ergehen. Sofern nicht durch Spezialbefugnis geregelt, sind dafür die Generalklauseln der Landespolizeigesetze einschlägig.

Darüber hinaus haben die Länder den unabhängigen Landesmedienanstalten im Rahmen des Jugendmedienschutz-Staatsvertrags (JMStV) spezielle Befugnisse eingeräumt. So enthält § 4 Absatz 1 JMStV einen Katalog bestimmter Angebote, die unbeschadet strafrechtlicher Verantwortlichkeit stets unzulässig sind. Auf Grundlage des § 20 Absatz 1 und 4 JMStV in Verbindung mit § 109 des Medienstaatsvertrags kann die zuständige Landesmedienanstalt durch die Kommission für Jugendmedienschutz die erforderlichen Maßnahmen (insbesondere Anordnung von Löschungen oder Sperrungen) treffen. Außerhalb der Bundesrepublik Deutschland beziehungsweise der Europäischen Union können diese Anordnungen gegenüber den Urhebern der Inhalte und den Hostingdiensteanbietern in der Regel nicht durchgesetzt werden. Durchsetzbar ist in diesen Fällen jedoch eine Anordnung der Sperrung des Zugangs zu den Inhalten aus Deutschland, zum Beispiel durch die in Deutschland ansässigen Internetzugangsdiensteanbieter.

Mit dem DSA bestehen zudem europarechtliche Bestimmungen zum Verfahren bei nationalen Lösch- und Sperranordnungen, wenn nationale Behörden solche Anordnungen auf Basis nationaler Rechtsgrundlagen erlassen. Auch verpflichtet der DSA Plattformen, Meldeverfahren vorzuhalten, damit rechtswidrige Inhalte gemeldet werden können. Die Bundesnetzagentur ist die zentrale Koordinierungsstelle (Digital Services Coordinator, DSC) für die Durchsetzung des DSA in Deutschland. Wenn ein Dienst beispielsweise keine wirksame Meldemöglichkeit vorhält, können Betroffene beim DSC diesen Verstoß gegen den DSA melden.

Das Recht auf Löschung gemäß Artikel 17 der Datenschutz-Grundverordnung (DSGVO) ermöglicht es Betroffenen, die Löschung ihrer personenbezogenen Daten von Diensteanbietern oder Suchmaschinen zu verlangen, unter anderem wenn die Daten unrechtmäßig verarbeitet wurden. Gegen eine Entscheidung

der Diensteanbieter haben Betroffene die Möglichkeit einer Beschwerde bei der zuständigen Datenschutzaufsichtsbehörde.

Die zuständige Datenschutzaufsichtsbehörde hat gemäßArtikel 58 Absatz 2 DSGVO eine Reihe von Abhilfebefugnissen, unter anderem kann sie die Löschung personenbezogener Daten anordnen. Betroffene können ihre Rechte aus der DSGVO, einschließlich eines Rechts auf Schadenersatz, auf dem zivilrechtlichen Klageweg einklagen.

Die von rechtsverletzenden Inhalten Betroffenen können vor Zivilgerichten auf deren Beseitigung klagen. Entscheidungen deutscher Gerichte können in Drittstaaten nach Durchführung eines Anerkennungs- und Vollstreckbarerklärungsverfahrens vollstreckt werden, wenn es zwischen Deutschland und dem betreffenden Staat ein Anerkennungs- und Vollstreckungsübereinkommen gibt; ansonsten richtet sich die Anerkennung und Vollstreckung im Drittstaat nach dessen nationalem Recht. Daneben können zur Erzwingung der Beseitigung Zwangsmittel eingesetzt oder Ersatzvornahmen angeordnet werden. Kosten dieser Maßnahmen können gegen den Verpflichteten geltend gemacht werden.

28. Welche internationalen Kooperationsmechanismen werden in diesem Zusammenhang genutzt (vgl. Frage 27), und wie bewertet die Bundesregierung deren Effektivität?

Durch die „International Association of Internet Hotlines“ INHOPE, ein globales Netzwerk von Internethotlines, besteht die Möglichkeit, Deepfakes mit kinderpornografischem Inhalt schnell und gezielt zu identifizieren und eine Löschung anzuregen. Für Deutschland kooperieren die Meldestellen des Verbandes der Internetwirtschaft eco, die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter und jugendschutz.net in dem transnationalen Kooperationswerk zur Durchsetzung von Löschungen. Zwischen den deutschen Hotlines und dem BKA besteht eine enge vertrauensvolle Zusammenarbeit. Die Effektivität hängt stark von der Mitwirkungsbereitschaft der beteiligten Akteure ab, wird aber in Bezug auf das Notice-and-Take-Down-System im Kontext kinderpornografischer Inhalte als wichtige Komponente der internationalen Kooperation bewertet.

29. Welche Erkenntnisse liegen der Bundesregierung ggf. zur internationalen Verbreitung entsprechender Delikte (vgl. Frage 28) vor, und auf welche konkreten Quellen stützen sich diese Erkenntnisse?

30. Wenn keine belastbaren Vergleichsdaten vorliegen (vgl. Frage 29), welche Gründe sieht die Bundesregierung hierfür?

Die Fragen 29 und 30 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Der Bundesregierung liegen keine statistischen Informationen im Sinne der Fragestellung vor. Aufgrund der zunehmenden Nutzung von Künstlicher Intelligenz im Alltag und in der Gesellschaft ist davon auszugehen, dass der Missbrauch Künstlicher Intelligenz für kriminelle Zwecke weltweit zunimmt.

Im Übrigen wird auf die rechtsvergleichenden Ausführungen auf Seite 24 folgend des Referentenentwurfs (vergleiche Antwort auf Frage 6) Bezug genommen.

31. Auf welche konkreten empirischen Erkenntnisse stützt die Bundesregierung den von der Bundesjustizministerin vorgelegten Referentenentwurf, insbesondere im Hinblick auf Häufigkeit und Entwicklung entsprechender Fälle?

32. Welche konkreten Fallkonstellationen sollen durch den Referentenentwurf (vgl. Frage 31) künftig strafbar sein, die nach geltendem Recht nicht erfasst sind?

33. Inwieweit wurde vor Erstellung des Referentenentwurfs (vgl. Frage 32) geprüft, ob bestehende strafrechtliche Vorschriften konsequent angewendet werden?

Die Fragen 31 bis 33 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Es wird auf die Antwort auf Fragen 5 und 12 verwiesen. Ergänzend wird auf Seite 1 folgend, 19 folgend und 23 folgend des Referentenentwurfs Bezug genommen. Der bisherige strafrechtliche Bildnisschutz wird in unserem zunehmend digitalen Zeitalter als unzureichend wahrgenommen. Wie in der Antwort auf Frage 15 ausgeführt, wird künftig insbesondere schon das Herstellen sexualisierter Deepfakes unter Strafe stehen.

34. Hat sich die Bundesregierung eine Auffassung erarbeitet zu der in der rechtswissenschaftlichen und anwaltlichen Praxis geäußerten Kritik, wonach der Referentenentwurf zu einer erheblichen Ausweitung strafrechtlicher Tatbestände führen könnte, und wenn ja, wie lautet diese?

Die Bundesregierung wird eingehende Stellungnahmen zum Referentenentwurf auswerten und auf dieser Grundlage etwaigen Änderungsbedarf prüfen.

35. Wie stellt die Bundesregierung sicher, dass die geplanten Regelungen (Referentenentwurf) den Anforderungen des Bestimmtheitsgebots gerecht werden?

Der Referentenentwurf wurde verfassungsrechtlich geprüft, auch mit Blick auf das Bestimmtheitsgebot.

36. Welche Abgrenzungskriterien sieht die Bundesregierung zwischen strafbarer digitaler Manipulation und zulässiger Nutzung digitaler Bild- oder Videobearbeitung?

Eine Handlung ist nur dann strafbar, wenn die Voraussetzungen eines Straftatbestands erfüllt sind. Bei § 184k Absatz 1 Nummer 4 des Strafgesetzbuches in der Entwurfsfassung (StGB-E) kommt es insbesondere darauf an, ob der Anschein erweckt wird, dass sexuelle Handlungen oder die unbekleideten Genitalien, das unbekleidete Gesäß oder die unbekleidete weibliche Brust einer anderen Person abgebildet seien. Maßgeblich bei § 201b StGB-E ist vor allem, dass der Inhalt den Anschein erweckt, ein tatsächliches Geschehen in Bezug auf eine andere Person wiederzugeben, und der geeignet ist, dem Ansehen dieser Person erheblich zu schaden. Gemäß § 184k Absatz 3, § 201b Absatz 2 StGB-E gelten die Strafvorschriften nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen. Die Beurteilung der Frage, welches Interesse im konkreten Fall überwiegt, hängt – wie

bereits nach geltender Rechtslage etwa bei der Verwendung von Fotomontagen zu satirischen Zwecken – von den Umständen des Einzelfalles ab und obliegt den zuständigen Strafverfolgungsbehörden und Gerichten (vergleiche Antwort der Bundesregierung auf die Schriftliche Frage des Abgeordneten Tobias Matthias Peterka vom 27. April 2026 (Bundestagsdrucksache 21/5661, Frage Nummer 90, Seite 65).

37. Welche besonderen Gründe sieht die Bundesregierung für eine gesonderte strafrechtliche Behandlung pornografischer Deepfake-Inhalte?

Es wird Bezug genommen auf die Antworten zu den Fragen 15 und 33. § 184k Absatz 1 Nummer 4 StGB-E und § 201b StGB-E unterscheiden sich insbesondere dadurch, dass erstgenannte Vorschrift auch das Herstellen (und nicht nur das Zugänglichmachen) erfasst.

38. Inwieweit wurde ggf. geprüft, ob bestehende Vorschriften zum Schutz vor Persönlichkeitsrechtsverletzungen durch Bild- oder Videoinhalte bereits ausreichend sind?

Es wird auf die Antworten zu den Fragen 15 und 33 Bezug genommen.

39. Inwieweit sieht die Bundesregierung vor dem Hintergrund der bestehenden Erkenntnislage ggf. die Notwendigkeit, die tatsächliche Anwendung und Durchsetzung des geltenden Rechts systematisch zu evaluieren?

40. Wenn eine solche Evaluation (vgl. Frage 39) nicht vorgesehen ist, aus welchen Gründen hält die Bundesregierung dies für entbehrlich?

Die Fragen 39 und 40 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Es ist vorgesehen, das Gesetz zur Stärkung des zivilrechtlichen und strafrechtlichen Schutzes vor digitaler Gewalt hinsichtlich seines zivilrechtlichen Teils spätestens fünf Jahre nach Inkrafttreten zu evaluieren.

41. Welche konkreten Maßnahmen plant die Bundesregierung ggf., um bestehende Vollzugsdefizite zu identifizieren und zu beheben?

Es wird auf die grundsätzliche Zuständigkeit der Polizeibehörden der Länder für die Verfolgung von Straftaten verwiesen. Im Übrigen wird auf die Antworten zu den Fragen 12 sowie 31 bis 33 und 39/40 verwiesen.

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.bundesanzeiger-verlag.de
ISSN 0722-8333