Gesetz gegen digitale Gewalt – Häufige Fragen

I. Gesetzentwurf gegen digitale Gewalt im Überblick

1. Was sieht der Gesetzentwurf vor?

- **Besserer strafrechtlicher Schutz vor digitaler Gewalt:** Strafbarkeitslücken im Bereich digitaler Gewalt sollen geschlossen und der Phänomenbereich insgesamt strafrechtlich klarer erfasst werden. Es geht dabei insbesondere um das unbefugte Herstellen und verbreiten von sexualisierten Deepfakes, von voyeuristischen Bildaufnahmen (z. B. in der Sauna), von Vergewaltigungsvideos und sogenannte Rache-Pornos. Auch das unbefugte Zugänglichmachen sonstiger Deepfakes soll unter Strafe gestellt werden, wenn sie geeignet sind, dem Ansehen der dargestellten Person erheblich zu schaden. Darüber hinaus soll auch das Cyberstalking mittels GPS-Trackern erfasst werden.
- **Erleichterung der Rechtsdurchsetzung:** Betroffene von digitaler Gewalt sollen ihre Rechte besser durchsetzen können. Online-Plattformen und Internetzugangsanbieter sollen dafür stärker in die Pflicht genommen werden. Zu diesem Zweck soll Betroffenen insbesondere ein neuer Auskunftsanspruch gewährt werden: Betroffene sollen einfacher und weitergehend als bisher von Online-Plattformen und Internetzugangsanbietern Auskunft über die Identität von Rechtsverletzern erlangen können (nach gerichtlicher Anordnung). Außerdem sollen Gerichte anlassbezogen beweissichernde Anordnungen gegenüber Online-Anbietern und Internetzugangsanbietern treffen können. Darüber hinaus sollen Betroffene bei schwerwiegenden Rechtsverletzungen und bestehender Wiederholungsbefahr eine zeitweilige Accountsperre des Verletzter-Accounts beantragen können. Und Betreiber von sozialen Netzwerken sollen neue Pflichten zur Benennung eines inländischen Zustellungsbevollmächtigten unterliegen.

2. Warum schlägt das BMJV diese Änderungen vor?

„Digitale Gewalt“ (das sind insbesondere schwerwiegende Verletzungen von Persönlichkeitsrechten im digitalen Raum) hat in den letzten Jahren drastisch zugenommen. Die

Folgen für die Betroffenen sind oft gravierend. Das geltende Strafrecht bietet gegen digitale Gewalt unzureichend Schutz: Mehrere Formen von digitaler Gewalt sind nicht angemessen erfasst. Außerdem haben Betroffene von digitaler Gewalt es oftmals schwer, selbst rechtlich gegen digitale Gewalt vorzugehen. Das liegt insbesondere daran, dass die Täter oft mit anonymen Accounts vorgehen – und sich die Identität der Rechtsverletzer für Betroffene oft nicht aufklären lässt.

3. Wie groß ist das Problem der digitalen Gewalt in Deutschland?

Die vom Bundeskriminalamt (BKA) herausgegebene Polizeiliche Kriminalstatistik (PKS) erfasst auch Delikte aus dem Phänomenbereich digitale Gewalt. Vom BKA werden diese unter anderem in dem Bundeslagebild „Geschlechtsspezifisch gegen Frauen gerichtete Straftaten“ zusammengefasst. Die Fälle von in der PKS erfasster digitaler Gewalt gegen Frauen haben sich seit 2020 mehr als verdoppelt. Das aktuellste Lagebild erfasst für das Jahr 2024 rund 18.000 Fälle mit weiblichen Opfern. Frauen sind demnach in rund 61 % der polizeilich erfassten Fälle digitaler Gewalt betroffen.

Auch die im Februar 2026 vorgestellte Dunkelfeldstudie Lebenssituation, Sicherheit und Belastung im Alltag (LeSuBiA) des Bildungs- und Innenministeriums sowie des Bundeskriminalamts erfasst den Bereich der digitalen Gewalt. Demnach erlebte jede fünfte Frau (20,0 %) und jeder siebte Mann (13,9 %) in den letzten fünf Jahren digitale Gewalt.

4. Wie ist der Zeitplan?

Zunächst wird der Entwurf regierungsintern sowie mit Ländern und Verbänden diskutiert und anschließend vom Kabinett beschlossen. Erst danach finden die Beratungen in Bundesrat und Bundestag statt.

5. Wann soll das Gesetz in Kraft treten?

Es ist geplant, dass das Gesetz gegen digitale Gewalt noch in diesem Jahr in Kraft tritt.

6. Was hat sich im Vergleich zum Entwurf der letzten Legislaturperiode geändert?

Der jetzt vorgelegte Gesetzentwurf sieht auch strafrechtliche Änderungen vor. Das war beim Gesetzentwurf aus der letzten Legislaturperiode nicht der Fall. Auch bei den vorgeschlagenen Regelungen zur Stärkung der Rechtsdurchsetzung von Betroffenen hat es

Änderungen gegeben: Insbesondere sind die Regeln nunmehr spezifisch auf Fälle zugeschnitten, in denen die erlittene Rechtsverletzung zugleich eine Straftat darstellt. Eine entsprechende Begrenzung gab es bei dem Entwurf in der letzten Legislaturperiode nicht.

II. Anpassungen im Strafrecht im Detail

1. Welche Formen bildbasierter sexualisierter Gewalt sollen zukünftig strafrechtlich erfasst werden?

Die neue Regelung soll bildbasierte sexualisierte Gewalt in ihren unterschiedlichen Erscheinungsformen erfassen. Dies betrifft computergenerierte Inhalte wie sexualisierte Deepfakes und den sogenannten „digitalen Voyeurismus“, also das heimliche Filmen oder Fotografieren an öffentlichen Orten (z. B. Saunalandschaften) oder Aufnahmen, die in sexuell bestimmter Weise bekleidete intime Körperteile zeigen. Auch Bildmaterial von nicht-einvernehmlichen, gewalttätigen sexuellen Handlungen (Vergewaltigungsvideos) und das nicht-einvernehmliche Teilen von einvernehmlich erlangten Bildern oder Videos (z. B. sogenannte „Revenge Porns“) sollen von dem Straftatbestand erfasst sein.

2. Soll die Verbreitung von sexualisierten Deepfakes straffrei sein, wenn eine Darstellung als KI-generiert gekennzeichnet ist?

Die neue Regelung richtet sich gezielt gegen die Verbreitung sexualisierter Deepfakes. Geschützt wird hier nicht die Wahrheit oder Authentizität sexualisierter Darstellungen, sondern das allgemeine Persönlichkeitsrecht in der Ausprägung der sexuellen Selbstbestimmung beziehungsweise der Intimsphäre. Für die Verletzung dieses geschützten Rechtsguts ist es unerheblich, ob die Darstellung als KI-erstellt gekennzeichnet ist. Entscheidend ist, ob die Darstellung realistisch eine sexuelle Handlung einer echten Person abbildet, die diese nicht vorgenommen hat.

3. Was plant das BMJV gegen sonstige (nicht sexualisierte) Deepfakes?

Ein neuer Straftatbestand soll das unbefugte Zugänglichmachen eines Deepfakes unter Strafe stellen, wenn diese geeignet sind, dem Ansehen der dargestellten Person erheblich zu schaden. Satire und andere künstlerische oder wissenschaftliche Darstellungen sind von dem Straftatbestand nicht erfasst. Erfasst sein kann beispielsweise ein täuschend echt aussehendes, nicht als Satire erkennbares Video, durch das der Anschein erweckt wird, eine Person habe eine Straftat begangen.

4. Welche strafrechtlichen Regelungen gelten bisher im Hinblick auf Deepfakes?

Die Verbreitung von Deepfakes kann unter gewissen Voraussetzungen bereits bestraft werden. Sie können zum Beispiel strafbar sein als Verleumdung oder als sexualisierte Deepfakes Tatbestände des Pornographiestrafrechts erfüllen. Auch eine strafbare Verletzung des Rechts am eigenen Bild nach dem Kunsturhebergesetz liegt bei der Verbreitung von Deepfakes in aller Regel vor. Das Strafgesetzbuch enthält aber keine Vorschrift, die auf das Problem konkret zugeschnitten ist – und das Unrecht zum Beispiel der Verbreitung von sexualisierten Deepfakes angemessen adressiert. Auch das Herstellen von Deepfakes allein unterliegt in der Regel keiner Strafbarkeit. Mit den vorgeschlagenen neuen Regelungen sollen das Verbreiten und mit Blick auf sexualisierte Deepfakes auch bereits das Herstellen gezielt im Strafrecht adressiert und Strafbarkeitslücken im Bereich bildbasierter sexualisierter Gewalt geschlossen werden.

5. Welche strafrechtlichen Regelungen plant das BMJV gegen digitales Tracking?

Ein neuer Straftatbestand soll die unbefugte elektronische Überwachung mit digitalen Trackern und anderer Informations- oder Kommunikationstechnik strafrechtlich besser erfassen. So könnte beispielsweise auch die erstmalige Überwachung einer Person erfasst sein, wenn der Tracker eine ständige Aufenthaltsbestimmung erlaubt. Das ist beim Straftatbestand der Nachstellung (§ 238 StGB) bisher nicht der Fall.

6. Ist die Verwendung von GPS-Trackern nicht schon nach geltendem Recht strafbar?

Viele Fälle des Cyberstalkings sind zwar bereits jetzt strafbar. Der Gesetzgeber hat beispielsweise 2021 die Verwendung von Spähsoftware als besonders schweren Fall der

Nachstellung (§ 238 StGB) aufgenommen. Es gibt aber strafwürdige Konstellationen, bei denen die geltende Rechtslage nicht immer eindeutig ist. Beispielsweise erfordert die Nachstellung (§ 238 StGB) eine wiederholte Handlung. In der Regel muss man einen GPS-Tracker aber nur einmal verstecken, um dann dauerhaft eine Person verfolgen zu können. Die neue Regelung soll auch diese Konstellation erfassen.

7. Inwieweit dient der Gesetzentwurf der Umsetzung der Richtlinie der EU zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt?

Die Richtlinie (EU) 2024/1385 vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt enthält Vorgaben betreffend die Strafbarkeit der Verbreitung von Abbildungen intimer Körperteile und zum Cyberstalking.

Die Richtlinie fordert beispielsweise von den Mitgliedsstaaten, die Verbreitung von Abbildungen intimer Körperteile unabhängig von der Individualisierbarkeit der dargestellten Person unter Strafe zu stellen, sofern diese Handlungen wahrscheinlich dazu führen, dass der betreffenden Person schwerer Schaden zugefügt wird (Artikel 5 der Richtlinie). Die Richtlinie sieht auch eine Strafbarkeit für die wiederholte oder ständige Überwachung einer anderen Person ohne deren Einwilligung oder ohne rechtliche Genehmigung mittels Informations- und Kommunikationstechnologien vor, sofern diese Handlungen wahrscheinlich dazu führen, dass dieser Person schwerer Schaden zugefügt wird (Artikel 6 der Richtlinie).

Mit dem Gesetzentwurf sollen die Vorgaben der Richtlinie umgesetzt werden – innerhalb der bis zum 14. Juni 2027 laufenden Umsetzungsfrist. Der Gesetzentwurf geht über die Vorgaben der Richtlinie in mehreren Punkten hinaus, um den strafrechtlichen Schutz vor digitaler Gewalt zu verbessern.

III. Geplante Änderungen bei der Rechtsdurchsetzung durch Betroffene

1. Wie soll es Betroffenen von digitaler Gewalt konkret erleichtert werden, gegen die Rechtsverletzer vorzugehen?

Online-Plattformen und Internetzugangsanbieter sollen dafür stärker in die Pflicht genommen werden:

- **Auskunftsanspruch:** Betroffene sollen von Online-Plattformen und Internetzugangsanbietern einfacher und weitergehend als bisher Auskunft über die Identität von Rechtsverletzern erhalten können; dafür soll ein neues Auskunftsverfahren **mit Richtervorbehalt** etabliert werden.
- **Beweissichernde Anordnungen:** Gerichte sollen Online-Plattformen und Internetzugangsanbieter **anlassbezogen** verpflichten können, bereits bei ihnen vorhandene Daten über einen mutmaßlichen Rechtsverletzer zu sichern. So soll erreicht werden, dass die Rechtsdurchsetzung nicht an einem Datenverlust scheitert.
- **Zeitweilige Accountsperre:** Bei schwerwiegenden Rechtsverletzungen und Wiederholungsgefahr sollen Betroffene eine zeitweilige Sperre des Verletzter-Accounts gerichtlich beantragen können.
- **Pflicht zur Benennung eines Zustellungsbevollmächtigten:** Betreiber von sozialen Netzwerken mit Sitz außerhalb der EU sollen einen inländischen Zustellungsbevollmächtigten benennen müssen. Bei Anbietern mit Sitz in einem anderen EU-Mitgliedstaat kann ein Gericht eine solche Benennung im Einzelfall, d.h. in einem konkreten Gerichtsverfahren, anordnen können. Dadurch soll es Betroffenen einfacher möglich sein, Rechte gegenüber den Plattformen durchzusetzen.

2. Für welche Fälle von Rechtsverletzungen sind die neuen Möglichkeiten zur Rechtsdurchsetzung (Auskunftsanspruch; Anspruch auf Accountsperren) konkret gedacht?

Die neuen Möglichkeiten zu Rechtsdurchsetzung finden Anwendung ausschließlich auf bestimmte Fälle von strafbaren Rechtsverletzungen. Voraussetzung ist zunächst, dass die strafbare Rechtsverletzung über eine Online-Plattform (soziales Netzwerk) oder einen Hosting-Dienst (z.B. Blog-Post) erfolgt. Die vom Gesetzentwurf erfassten Rechtsverletzungen sind abschließend definiert. Es handelt sich dabei um Straftaten, die häufig im digitalen Raum begangen werden und den Betroffenen direkt in seinen Persönlichkeitsrechten verletzen.

Auf folgende Tatbestände werden im Gesetzentwurf für die Auskunftsverfahren und den Anspruch auf Accountsperren Bezug genommen:

<u>Aus dem Strafgesetzbuch:</u>

- § 111 Öffentliche Aufforderung zu Straftaten
- § 126 Störung des öffentlichen Friedens durch Androhung von Straftaten
- § 126a Gefährdendes Verbreiten personenbezogener Daten
- § 130 Volksverhetzung
- § 130a Anleitung zu Straftaten
- § 131 Gewaltdarstellung
- § 140 Belohnung und Billigung von Straftaten
- 166 Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen
- § 176a Sexueller Missbrauch von Kindern ohne Körperkontakt mit dem Kind
- § 176b Vorbereitung des sexuellen Missbrauchs von Kindern
- § 184 Verbreitung pornographischer Inhalte
- § 184a Verbreitung gewalt- oder tierpornographischer Inhalte
- § 184b Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte
- § 184c Verbreitung, Erwerb und Besitz jugendpornographischer Inhalte
- § 184k-E Verletzung der Intimsphäre durch Bildaufnahmen
- § 185 Beleidigung
- § 186 Üble Nachrede
- § 187 Verleumdung
- § 188 Gegen Personen des politischen Lebens gerichtete Beleidigung, üble Nachrede und Verleumdung
- § 189 Verunglimpfung des Andenkens Verstorbener
- § 192a Verhetzende Beleidigung
- § 201 Verletzung der Vertraulichkeit des Wortes
- § 201a Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen
- § 201b StGB-E Verletzung von Persönlichkeitsrechten durch täuschende Inhalte
- § 238 Nachstellung
- § 241 Bedrohung

<u>Aus strafrechtlichen Nebengesetzen:</u>

- § 33 des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie oder
- § 42 des Bundesdatenschutzgesetzes.

3. Welche Daten sollen von Online-Plattformen, Internetzugangsanbietern und Hosting-Diensten auf gerichtliche Anordnung hin rausgegeben werden müssen?

Folgende Daten sollen auf gerichtliche Anordnung vom Betreiber von Online-Plattformen (sozialen Netzwerken) oder Hosting-Diensten herausgegeben werden müssen, sofern sie vorliegen:

- die Personalien des rechtswidrig handelnden Nutzers, wie den Namen, das Geburtsdatum, die Anschrift, die E-Mail-Adresse und die Telefonnummer,
- die gespeicherte Internetprotokoll-Adresse einschließlich der Portnummer, die bei der Rechtsverletzung verwendet wurde, und den Zeitpunkt des Zugriffs auf den Dienst unter Angabe der zugrunde liegenden Zeitzone sowie
- die gespeicherte Internetprotokoll-Adresse einschließlich der Portnummer, die vor der Zustellung der gerichtlichen Anordnung bei Nutzung des betreffenden Nutzerkontos zuletzt verwendet wurde, und den Zeitpunkt des letzten Zugriffs unter Angabe der zugrunde liegenden Zeitzone.

Folgende Daten sollen vom Internetzugangsdienst herausgegeben werden, sofern sie vorliegen:

- die Personalien des Nutzers, die bei einem Anbieter eines Internetzugangsdienstes hinterlegt sind, wie den Namen, das Geburtsdatum, die Anschrift, die E-Mail-Adresse und die Telefonnummer.

Zudem soll eine Kopie des angegriffenen Inhalts übermittelt werden, damit dieser nicht nachträglich gelöscht werden kann.

4. Welchen Schutz soll es geben, damit Daten nicht willkürlich abgefragt werden können?

Die Auskunft der Daten erfolgt nur nach richterlicher Anordnung (**Richtervorbehalt**). Das Gericht muss eingehend prüfen, ob der unbekannte rechtswidrig handelnde Nutzer die Betroffenen in ihren Rechten verletzt hat. Der Betroffene muss zudem die Absicht

haben, zivilrechtliche Ansprüche gegen den unbekannten rechtswidrig handelnden Nutzer geltend zu machen (bspw. eine Unterlassung oder Löschung des Inhaltes). Zudem sind die in Betracht kommenden Straftatbestände im Gesetzentwurf abschließend definiert. Dadurch soll sichergestellt werden, dass nur bei den definierten Straftaten eine Auskunftsverfahren durchgeführt werden kann.

5. **Welche Beteiligungsrechte haben mutmaßliche Rechtsverletzer in den gerichtlichen Verfahren betreffend Auskunft über ihre Identität oder die Sperrung ihres Accounts?**

Sofern die Identität des mutmaßlichen Rechtsverletzers (Nutzers) dem Gericht bekannt ist, ist er zu den Verfahren heranzuziehen. Falls er nicht bekannt ist, so hat das Gericht den Diensteanbieter (Betreiber des sozialen Netzwerks; Internetzugangsdienst) zu verpflichten, den Nutzer über die Einleitung des Verfahrens zu unterrichten. Der Diensteanbieter hat die Einreichung von Stellungnamen anonym oder unter einem Pseudonym zu ermöglichen. Der Nutzer ist auf seinen Antrag als Beteiligter zu dem Verfahren hinzuziehen. Ein Rechtsverletzer kann eine Accountsperre dadurch abwenden, dass er eine strafbewehrte Unterlassungserklärung abgibt.

6. **Wie soll das Auskunftsverfahren konkret ablaufen, mit dem der Betroffene Auskunft über die Identität des Rechtsverletzers erlangen kann?**

Zuständig für Anträge auf Auskunft ist das Landgericht, in dessen Bezirk die verletzte Person (Antragsteller) ihren Wohnsitz hat. Das Verfahren richtet sich nach dem FamFG (Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit). Es besteht deshalb kein Anwaltszwang; es fallen keine Gerichtsgebühren an.

Die verletzte Person (Antragsteller) muss gegenüber dem Gericht die Tatsachen glaubhaft machen, aus denen sich ergibt, dass ein ihr unbekannter Nutzer eine strafbare Rechtsverletzung im Sinne des Gesetzes gegen digitale Gewalt begangen hat – und sie muss ihre Absicht bekunden, gegen diesen Nutzer zivilrechtliche Ansprüche geltend zu machen.

Das Gericht ordnet ggf. **in einem ersten Schritt** gegenüber der Online-Plattform (Betreiber des sozialen Netzwerks) bzw. dem Hosting-Dienst (Host einer Website) an, dass diese

dem Gericht die dort gespeicherten Personalien des unbekannten Nutzers und die dem Nutzer zugeordnete IP-Adresse übermitteln muss.

In vielen Fällen werden die im ersten Schritt erlangten Personalien eine Identifizierung des unbekannten Nutzers nicht erlauben (weil viele Nutzer bei der Registrierung in sozialen Netzwerken unzutreffende Personalien angeben). In einem **zweiten Schritt** kann das Gericht ggf. gegenüber dem maßgeblichen Internetzugangsanbieter anordnen, dass dieser die IP-Adresse, die dem rechtsverletzenden Nutzer zugeordnet war, einem Anschlussinhaber zuordnet.

Abschließend entscheidet das Gericht über den Auskunftsantrag. Ist der Antrag begründet, so müssen die Online-Plattform und der Internetzugangsdienst die maßgeblichen Informationen direkt an den Antragsteller übermitteln. Anschließend müssen sie gelöscht werden.

7. Woher weiß das Gericht, welcher Internetzugangsanbieter Auskunft darüber erlangen kann, welchem Anschlussinhaber eine IP-Adresse zugeordnet war?

Anhand einer IP-Adresse lässt sich regelmäßig ablesen, welcher Internetzugangsanbieter die fragliche IP-Adresse vergeben hat. Das Gericht kann also einfach ermitteln, an welchen Internetzugangsanbieter es sich wenden muss. Der Anschlussinhaber ist nicht immer Täter des vorgeworfenen Delikts. Ihn können aber im Einzelfall Sicherungsobliegenheiten treffen zu verhindern, dass sein Anschluss für kriminelle Handlungen genutzt wird.

8. Was ist vorgesehen, damit die Daten über den Rechtsverletzer bei den Online-Plattformen nicht zwischenzeitlich gelöscht werden?

Sofern tatsächliche Anhaltspunkte für eine Rechtsverletzung vorliegen, soll das Gericht unverzüglich nachdem ein Auskunftsantrag gestellt wurde eine vorläufige Speicherung der vorhandenen Daten über die rechtswidrig handelnden Nutzer beim Betreiber der Online-Plattform oder des Hosting-Dienstes anordnen **(Sicherungsanordnung)**. Dadurch soll sichergestellt werden, dass die Daten nicht während des Verfahrens gelöscht werden.

9. Wie lange sollen die Daten nach einer beweissichernden Anordnung gespeichert werden?

Die Daten sollen bis zu einem rechtskräftigen Beschluss über das Datenauskunftsverfahren gespeichert bleiben. Nach rechtskräftigem Abschluss des Verfahrens sind die Daten bei einer Verpflichtung zur Auskunft nach Übermittlung an den Antragsteller irreversibel zu löschen. Wenn keine Verpflichtung zur Auskunft besteht, sollen die Daten nach rechtskräftigem Abschluss sofort gelöscht werden.

10. Was soll eine zeitweise Accountsperre bezwecken?

Bei einer Accountsperre sollen rechtswidrig handelnde Nutzer keine Inhalte veröffentlichen, kommentieren und teilen können. Zudem sollen Nutzer während der Sperrung keine neuen Nutzerkonten anlegen können. Es soll sichergestellt werden, dass bei schwerwiegenden Rechtsverletzungen keine Wiederholung stattfindet. Betroffene sollen sich sicher sein können, dass derselbe rechtswidrig handelnde Nutzer nicht durch andere Accounts weiter digitale Gewalt ausübt. Eine passive Nutzung, ein sogenannter Lesemodus, soll jedoch weiterhin möglich sein.

Die Accountsperre ist insbesondere relevant, wenn rechtsverletzende Accounts eine große Reichweite haben. Diese große Reichweite wird den Rechtsverletzern durch die Sperre genommen.

11. Wann soll eine zeitweise Accountsperre angeordnet werden können?

Eine Accountsperre soll nur auf Antrag des Betroffenen nach richterlichem Beschluss erfolgen können. Sie soll voraussetzen, dass eine schwerwiegende Persönlichkeitsrechtsverletzung begangen wurde und eine Sperre erforderlich ist, um eine Wiederholung zu verhindern. Im Regelfall wird eine Sperrung erforderlich sein, wenn der rechtswidrig handelnden Nutzer keine Unterlassungserklärung abgibt oder gegen eine Unterlassungserklärung verstößt sowie es Anhaltspunkte gibt, die weitere Rechtsverletzungen befürchten lassen. Eine Accountsperre soll ein letztes Mittel darstellen, wenn Abhilfe nicht durch mildere Mittel erreicht werden kann.

12. Wie lange soll eine Accountsperre andauern?

Die Dauer der Accountsperre wird durch das Gericht festgelegt. Sie muss im Verhältnis zu weiteren zu erwartenden Rechtsverletzungen angemessen sein. Was angemessen ist, bestimmt sich nach den Umständen des Einzelfalls (z.B. Anzahl und Anteil der rechtswidrigen Inhalte, Schwere und Folgen der Rechtsverletzung, Absichten des Rechtsverletzers).

13. Entsteht durch die neue Möglichkeit von Accountsperren die Gefahr von Overblocking?

Accountsperren sind als Mittel letzter Wahl (Ultima Ratio) konzipiert. Die Entscheidung, ob eine Accountsperre zulässig ist, ist eine Einzelfallentscheidung des Gerichtes. Plattformen müssen die Accountsperre lediglich nach gerichtlicher Anordnung vornehmen. Die Accountsperre ist nur möglich, wenn Persönlichkeitsrechte schwerwiegend beeinträchtigt werden und wenn Wiederholungsgefahr besteht. Der Rechtsverletzer kann eine Accountsperre dadurch abwenden, dass er eine strafbewehrte Unterlassungserklärung abgibt. Außerdem gilt die Accountsperre nur für einen angemessenen Zeitraum.

14. Stellen Accountsperren eine Verletzung der Meinungsfreiheit dar?

Nein. Die vorgeschlagenen Accountsperren dienen ausschließlich dem Zweck, zukünftige strafbare Äußerungen, die digitale Gewalt darstellen, zu unterbinden. Es sind hohe Hürden für eine Accountsperre im Einzelfall angelegt. Grundsätzlich findet das Gesetz

gegen digitale Gewalt nur bei den im Gesetz definierten Rechtsverletzungen Anwendungen. Was eine Rechtsverletzung darstellt, ist im Gesetz gegen digitale Gewalt abschließend definiert. Der Gesetzentwurf beschränkt sich auf strafbare Verletzungen des Persönlichkeitsrechts.

15. Sollen Nutzerkonten auch bei kritischen Meinungsäußerungen, bspw. gegenüber Unternehmen, gesperrt werden können?

Nein. Der Gesetzentwurf beschränkt sich auf strafbare Verletzungen des Persönlichkeitsrechts. Im Gegensatz zum Eckpunktepapier in der vorigen Legislaturperiode reicht eine Verletzung des sog. Rechts am eingerichteten und ausgeübten Gewerbebetrieb nicht aus.

16. Was droht Plattformen, wenn sie den Anordnungen nicht nachkommen?

Wenn Plattformen den gerichtlichen Anordnungen nicht nachkommen, haben Gerichte bereits heute die Möglichkeit, Ordnungsmittel wie Zwangsgelder zu verhängen. Wenn die neuen Verpflichtungen zur Bereitstellung eines inländischen Zustellungsbevollmächtigen nicht erfüllt werden, sollen auch Bußgelder verhängt werden können.

17. In welchem Zusammenhang steht das Gesetz gegen digitale Gewalt mit der geplanten Verpflichtung von Internetzugangsdiensten zu einer dreimonatigen IP-Adressspeicherung?

IP-Adressen sind häufig der einzige Anhaltspunkt, um die Identität von Tätern im Internet aufzuklären. Das BMJV hat daher ein Gesetzentwurf vorgelegt, der Internetzugangsanbieter verpflichtet, IP-Adressen für 3 Monate zu speichern. Im Gesetz gegen digitale Gewalt ist geplant, dass diese gespeicherte IP-Adresse auch für die Durchsetzung von Ansprüchen durch die Betroffenen von digitaler Gewalt genutzt werden kann. Ohne die IP-Adressspeicherung werden IP-Adressen häufig nach kurzer Zeit gelöscht, in der Regel schon nach wenigen Tagen. Betroffenen von digitaler Gewalt und Gerichten ist somit eine Identifikation der rechtswidrig handelnden Nutzer oftmals nicht möglich. Mit der geplanten IP-Adressspeicherpflicht sollen Betroffene und Gerichte mehr Zeit erhalten, die Identität des rechtswidrig handelnden Nutzers aufzuklären.

18. Sind die vorsorgliche Speicherung und die Nutzung der gespeicherten IP-Adresse für zivilrechtliche Durchsetzung mit Grundrechten vereinbar?

Ja. Der Europäische Gerichtshof hat zuletzt mehrfach ausdrücklich klargestellt, dass eine vorsorgliche Speicherung von IP-Adressen mit europäischen Grundrechten vereinbar ist. Der Entwurf bewegt sich im Rahmen der grundrechtlichen Vorgaben. Die gesetzlichen Regelungen, die in der Vergangenheit für grundrechtswidrig erklärt wurden, waren andere als die jetzt vorgeschlagenen Regeln. Sie hätten insbesondere die Erstellung von Persönlichkeits- und Bewegungsprofil ermöglicht.

19. Werden die Digitalunternehmen durch die neuen Verpflichtungen unverhältnismäßig belastet?

Nein. Die Anwendung der neuen Datenauskunfts- und Datenspeicherungspflichten beschränken sich auf Einzelfälle und nur nach gerichtlicher Anordnung. Es ist daher von einem eher geringen Mehraufwand für Digitalunternehmen auszugehen. Zudem überwiegt das Interesse an einer effektiven Rechtsdurchsetzung.

Allgemein dient der Entwurf zudem der Rechtsvereinfachung. Der Gesetzentwurf sorgt für Rechtsklarheit im Hinblick auf wesentliche Maßnahmen der privaten Rechtsverfolgung im Internet, indem er diese in einem eigenen Stammgesetz zusammenfasst und transparent ausgestaltet.

20. Sind die geplanten Regelungen mit dem EU-Recht vereinbar?

Der Entwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar. Im Digital Services Act (DSA) ist ausdrücklich geregelt, dass nationale Justiz- oder Verwaltungsbehörden von Plattformen verlangen dürfen, bestimmte Verstöße gegen das Recht des jeweiligen Mitgliedstaats abzustellen oder zu verhindern. Solche einzelfallbezogenen Anordnungen beschränken nicht die Freiheit der Anbieter, ihre Dienste grenzüberschreitend zu erbringen. Der Anspruch auf Sperrung des Nutzerkontos steht ebenfalls unter dem Vorbehalt einer gerichtlichen Anordnung und ermöglicht daher ebenfalls ein konkretes Vorgehen gegen rechtswidrige Inhalte. Der DSA enthält keine Regelungen, die gerichtlich angeordnete Sperrungen eines Nutzerkontos in einem Verfahren zwischen zwei Privaten ausschließt.

21. Wird eine Klarnamenpflicht eingeführt?

Nein – eine Klarnamenpflicht wird nicht eingeführt: Die Nutzung von anonymen Accounts bleibt weiterhin möglich. Auch eine Identifizierungspflicht gegenüber dem Diensteanbieter wird nicht geregelt. Die Datenauskunftsrechte beschränken sich außerdem auf den Einzelfall. Es obliegt der Entscheidung der unabhängigen Gerichte, ob dem Datenauskunftsersuchen stattgegeben wird. Anonyme Meinungsäußerungen, die nicht strafrechtlich relevant sind, bleiben weiterhin anonym. Eine Auskunft zur Identifizierung wird in diesen Fällen nicht erteilt.