Stellungnahme Google zum Gesetzesentwurf zur Stärkung des zivil- und strafrechtlichen Schutzes vor digitaler Gewalt (GgdG-E)

22. Mai 2026

1. Verletzung der Intimsphäre durch Bildaufnahmen

Google setzt sich nachdrücklich dafür ein, die schädlichen Auswirkungen zu bekämpfen, die die Erstellung und Weitergabe von nicht einvernehmlich erstellten realen oder synthetischen intimen Darstellungen haben. Wir verurteilen diese Darstellungen und sind uns der schweren Belastung der betroffenen Personen bewusst, die entstehen, wenn solche Darstellungen ohne ihre Zustimmung geteilt werden und online auffindbar sind.

Aus diesem Grund haben wir unsere Tools zur Bildgenerierung und -bearbeitung mit integrierten Sicherheitsvorkehrungen ausgestattet. So verbieten unsere Richtlinien die nicht einvernehmliche Erstellung intimer Bilder, und wir nutzen eine Kombination aus automatisierten Systemen und menschlicher Überprüfung, um Versuche zur Erstellung solcher Bilder zu erkennen.

Unabhängig davon haben wir im Einklang mit dem DSA Mechanismen zur Verfügung gestellt, mit deren Hilfe Nutzende uns über das Vorhandensein bestimmter Inhalte auf unseren Hosting-Diensten informieren können, die sie für illegal halten. Wir entscheiden über solche Nutzerhinweise zeitnah, sorgfältig, nicht willkürlich und unvoreingenommen. Außerdem benachrichtigen wir Nutzende unverzüglich über unsere Entscheidungen und informieren sie über Möglichkeiten, diese Entscheidungen anzufechten.

Auf EU-Ebene haben wir im Rahmen der kürzlich abgeschlossenen Verhandlungen zum AI-Omnibus die Einführung einer neuen Kategorie verbotener KI-Systeme gemäß Artikel 5 der KI-Verordnung unterstützt. Dort einigte man sich darauf, das Inverkehrbringen von KI-Systemen zu verbieten, deren Hauptzweck die Erzeugung nicht einvernehmlicher intimer Darstellungen ist, und verpflichteten Anbieter von KI-Modellen mit allgemeinem Verwendungszweck zur Umsetzung geeigneter Sicherheitsmaßnahmen und technischer Schutzvorkehrungen, um die Erzeugung solcher Darstellungen zu verhindern.

Im Einklang mit unserer langjährigen Position zu nicht einvernehmlichen intimen Darstellungen unterstützen wir den Vorschlag, einen neuen § 184k in das deutsche Strafgesetzbuch aufzunehmen.

Wir sind der Ansicht, dass der Vorschlag ein gutes Gleichgewicht herstellt: Er geht gegen die schädlichen Inhalte vor und ist gleichzeitig innovationsfreundlich und ermöglicht die Nutzung der Vorteile der sich rasch entwickelnden KI-Technologie. Wir begrüßen insbesondere die

Feststellung, dass Nutzende haften sollten, die die rechtsverletzenden Inhalte erstellen und Dritten zugänglich machen, und nicht der Anbieter des KI-Tools, mit dem diese Inhalte erstellt wurden. Dies steht im Einklang mit der Fokussierung auf die Absicht der Nutzenden und würdigt den Umstand, dass solche KI-generierten Inhalte rechtmäßig sein können, wenn die Zustimmung der abgebildeten Person vorliegt oder wenn sie unter die Ausnahmen nach Absatz 4 des Paragraphen fallen. Eine andere Regelung würde die Meinungsfreiheit untergraben, den Zugang zu Informationen erschweren sowie die Entwicklung und Einführung von KI-Anwendungen in Deutschland beeinträchtigen.

2. Verletzung von Persönlichkeitsrechten durch täuschende Inhalte

Der neue § 201b des Strafgesetzbuchs wirft einige Fragen im Hinblick auf generative KI und digitale Doppelgänger auf.

Google hat Verständnis für das politische Ziel, sicherzustellen, dass Einzelpersonen gegen nicht autorisierte, realistische KI-generierte Inhalte vorgehen können, die rufschädigend sind. Wir hegen jedoch Bedenken hinsichtlich der Auswirkungen, die die vorgeschlagene Änderung auf Meinungs- und Kunstfreiheit haben könnte.

Vor allem befürchten wir, dass der Vorschlag die subjektive Absicht eines Nutzenden, die fraglichen Inhalte Dritten zugänglich zu machen, nicht berücksichtigt. Auch wenn Inhalte täuschend sein und erheblichen Schaden verursachen können, teilen Nutzende sie möglicherweise nicht in übler Absicht mit Dritten. Das nicht böswillige Teilen könnte aber laut vorliegendem Entwurf vom Gesetz umfasst sein, zumindest ist der Entwurf in dieser Hinsicht nicht klar genug.

In diesem Zusammenhang möchten wir anmerken, dass der Entwurf keine Anforderung an die Kenntnis der Nutzenden enthält, die den Inhalt Dritten zugänglich machen. Dies könnte zu einer Haftung für Inhalte führen, die versehentlich und ohne Kenntnis ihrer synthetischen Natur geteilt werden.

Wir empfehlen daher eine Klarstellung, dass Nutzende, die Inhalte Dritten zur Verfügung stellen, nur dann haftbar sind, wenn sie positive Kenntnis davon haben, dass die Inhalte synthetisch sind, und sie kumulativ die Absicht haben, andere durch das Teilen zu täuschen. Damit würden Einzelpersonen nicht unangemessen für versehentliche oder unvorhergesehene Folgen der Nutzung von Technologie bestraft, Chilling-Effekte mit Blick auf die Meinungsfreiheit würden vermieden und der Einsatz von KI-Tools würde zur Entfaltung von Kreativität sowie technologischem Fortschritt beitragen.

Der DSA verlangt von Anbietern von Vermittlungsdiensten, auf denen solche Inhalte geteilt werden können, dass sie bei der Anwendung und Durchsetzung von Beschränkungen, die sie Nutzenden in Bezug auf die von ihnen bereitgestellten Inhalte auferlegen, sorgfältig, objektiv und verhältnismäßig vorgehen. Sie müssen die Grundrechte der Nutzenden des Dienstes, etwa die Meinungsfreiheit und die Freiheit der Kunst, angemessen berücksichtigen. Der DSA sieht außerdem vor, dass jede Maßnahme, die ein Anbieter von Hosting-Diensten nach Erhalt einer

Mitteilung zu problematischen Inhalten ergreift, zielgerichtet sein muss, d.h. die Inhalte, die als illegal eingestuft wurden, müssen entfernt oder gesperrt werden, ohne die Meinungs- und Informationsfreiheit der Nutzenden unangemessen zu beeinträchtigen.

Zwar sieht der Gesetzentwurf Ausnahmen zum Schutz der Meinungs- und Kunstfreiheit vor, doch es dürfte für Anbieter in der Praxis oft äußerst schwierig zu entscheiden sein, ob ein gemeldeter Inhalt eine rechtswidrige oder eine legitime, unter die Ausnahmeregelung fallende Nutzung darstellt. Begriffe wie Parodie, Karikatur, Pastiche, politischer Kommentar und Gesellschaftskritik sind von Natur aus vage und in hohem Maße auslegungsfähig, was wiederum die Rechtssicherheit beeinträchtigt. Darüber sehen wir die Gefahr missbräuchlicher Löschungsanträge, d.h. von Beschwerden, die in böser Absicht eingereicht werden, um rechtmäßige Meinungsäußerungen und künstlerischen Ausdruck zu unterdrücken. Solche Taktiken könnten beispielsweise von politischen oder anderen Akteuren genutzt werden, um Kritiker zum Schweigen zu bringen oder unerwünschte Standpunkte zu entfernen. Ohne starke verfahrensrechtliche Schutzvorkehrungen und Abschreckungsmaßnahmen gegen Missbrauch (wie z. B. das Recht des Inhaltseigentümers, vom Meldenden Schadenersatz für missbräuchliche Meldungen zu verlangen), bleiben auch rechtmäßige Meinungsäußerungen anfällig für gezielte Unterdrückung. Solche Schutzvorkehrungen sind besonders wichtig, da Plattformen in vielen Fällen nicht feststellen können, ob Inhalte echt sind oder es sich um Deepfakes handelt.

3. Vereinfachtes Auskunftsverfahren durch gerichtliche Anordnungen

Zwar unterstützen wir das Ziel, Opfern rasche Rechtsbehelfe zu bieten, doch stellt die vorgeschlagene „Vermittlerrolle“ für Diensteanbieter bei Offenlegungs- und Kontosperrungsverfahren erhebliche verfahrensrechtliche und rechtliche Herausforderungen dar. Wir sind der Ansicht, dass eine direkte Kommunikation zwischen Gericht und Nutzer den Interessen der Opfer besser dient, die Effizienz der Justiz gewährleisten und die Übereinstimmung mit dem harmonisierten Rechtsrahmen der Europäischen Union wahren würde.

3.1. Schutz der Opfer und Verhinderung einer Eskalation

Die Verpflichtung der Diensteanbieter, Nutzende über eingeleitete Verfahren zu informieren, bevor Maßnahmen ergriffen werden, könnte unbeabsichtigt die Sicherheit der Opfer untergraben. Die Vorschrift einer frühzeitigen Offenlegung gegenüber der beschuldigten Partei birgt das Risiko von Abschreckungseffekten. Opfer könnten davon abgehalten werden, Rechtsmittel einzulegen, wenn sie befürchten müssen, dass die Benachrichtigung eine weitere Verbreitung schädlicher Inhalte oder direkte Vergeltungsmaßnahmen der beschuldigten Partei auslöst, bevor ein Gericht tätig werden kann.

3.2. Verfahrensökonomie und Rechtsökonomie

Der Grundsatz der *von Amts wegen* erfolgenden Ermittlung nach dem Familienverfahrensgesetz (FamFG) ermächtigt die Gerichte, die Beweisaufnahme und die

Beteiligung der Parteien direkt zu regeln. Die Verfahrensbeteiligten unterliegen gemäß § 27 FamFG einer Mitwirkungspflicht. Die Nutzung dieses bestehenden Rahmens für eine direkte Interaktion zwischen Gericht und Nutzenden wäre effizienter als der vorgeschlagene „Ping-Pong“-Prozess zwischen Gericht, Diensteanbieter und Nutzenden.

Da das Gericht bereits über die relevanten Inhalte und Daten verfügen würde, besteht keine Informationsasymmetrie, die die Einbeziehung des Diensteanbieters erforderlich macht. Vielmehr führt die Einbeziehung von Diensteanbietern als „Vermittler“ zu unnötigen, fehleranfälligen Verzögerungen, die dem im Entwurf genannten Ziel einer raschen Identifizierung zuwiderlaufen.

3.3. Wirtschaftliche Auswirkungen und operative Durchführbarkeit

In der Gesetzesbegründung wird mit 53.000 EUR für die jährlichen Compliance-Kosten gerechnet. Dies unterschätzt die operativen Erfüllungskosten erheblich:

- Die Einhaltung der Vorschriften wäre keine einfache, automatisierbare Aufgabe. Sie würde vielmehr komplexe Arbeitsabläufe erfordern, darunter beispielsweise manuelle Sachverhaltsklärungen, die Überprüfung von Nutzerantworten, Fristenmanagement und die Schulung von Fachpersonal.

- Die daraus erwachsenden wirtschaftlichen Belastungen für einen Dienstanbieter spiegeln sich nicht im angenommenen jährlichen Erfüllungsaufwand wider. Verglichen mit den wirtschaftlichen Auswirkungen, die die Umsetzung des Netzwerkdurchsetzungsgesetzes (NetzDG) auf die Verpflichteten hatte, berücksichtigt die Begründung hier nur einen Bruchteil der entstehenden Kosten.

- Die Begründung basiert auf falschen Annahmen. Sie bezieht sich ausschließlich auf Kosten, die im Zusammenhang mit Auskunftsersuchen entstehen. Es werden 6.400 Auskunftsersuchen pro Jahr angenommen, deren Bearbeitung jeweils 10 Minuten dauert. Diese Zahlen spiegeln folgende Gegebenheiten nicht wider:

    - Grundsätzlich wird pro Fall mehr Zeit benötigt, um eine gründliche Prüfung zu gewährleisten. Dies gilt insbesondere, weil Auskunfts- und Sperranträge oft nicht die erforderlichen Informationen enthalten, um § 6 Abs. 2 GgdG-E zu erfüllen. Das Gericht ist nicht verpflichtet, die darin aufgeführten Informationen bereitzustellen. Daher muss der Dienstleister möglicherweise eigene Sachverhaltsklärungen durchführen (z. B. den betreffenden Inhalt und Nutzer ausfindig machen, Screenshots erstellen, mit dem Gericht klären, ob Nutzende nicht eindeutig identifiziert sind, Fall-IDs erstellen usw.).

    - Die Nutzerbeteiligung bindet Ressourcen und/oder erfordert zusätzliche Mittel. Es würden etwa neue Kosten für Personal und Schulungen anfallen. Eigene Teams müssten beispielsweise Recherchen durchführen, den gesamten Prozess überwachen sowie sicherstellen, dass keine Fehler gemacht werden und die Übermittlungen an das Gericht korrekt sind. Dies gilt umso mehr angesichts des

Risikos von Geldbußen gemäß § 35 FamFG und Verstößen gegen die DSGVO (z. B. wenn der falsche Nutzer identifiziert oder kontaktiert wird) sowie zivilrechtlicher Haftung. Die Kosten für die Einrichtung eines solchen von Menschen überprüften Arbeitsablaufs wurden nicht berücksichtigt.

3.4. Widerspruch zum EU-Recht

Aus unserer Sicht steht das vorgeschlagene Verfahren im Widerspruch zu dem durch den Digital Services Act (DSA) und die E-Commerce-Richtlinie (ECD) geschaffenen harmonisierten Rahmen:

- Die Verpflichtung des Diensteanbieters, unverzüglich Nutzende zu unterrichten und das Gericht darüber zu informieren (§ 6 Abs. 2 Nr. 2 GgdG-E), kann als Anordnung zur Bereitstellung von Informationen über Nutzende des Dienstes im Sinne von Artikel 10(1) DSA angesehen werden. Eine solche Anordnung wäre nicht mit Artikel 10(2)(b) DSA vereinbar. Die Verpflichtung zur Bereitstellung von Informationen über Nutzende beschränkt sich auf „Informationen, die bereits zum Zwecke der Erbringung des Dienstes erhoben wurden und die im Einflussbereich des Diensteanbieters liegen“.

- Zu den Mindestvoraussetzungen, die eine Anordnung nach den Artikeln 9 und 10 DSA erfüllen muss, gehört u. a. die Vermeidung „unverhältnismäßiger Belastungen für die Anbieter“ (Erwägungsgrund 31). Diese Voraussetzungen stellen sicher, dass Anordnungen „auf wirksame und effiziente Weise“ befolgt werden können. Ein komplexer Prozess, der umfangreiche manuelle Eingriffe seitens des Diensteanbieters erfordert, erfüllt diesen Standard nicht.

- Artikel 9(2)(a)(v) und 10(2)(a)(v) DSA regeln, wie und zu welchem Zeitpunkt betroffene Nutzende in den Prozess einbezogen werden müssen: nachdem eine Offenlegungsanordnung oder eine Anordnung zur Entfernung von Inhalten erlassen wurde. Solche Anordnungen müssen Informationen über mögliche Rechtsbehelfe enthalten, die Nutzenden zur Verfügung stehen, die den Inhalt bereitgestellt haben oder von der Anordnung betroffen sind. Das GgdG-E verlangt jedoch schon eine vorherige Einbeziehung der Nutzenden und verpflichtet den Diensteanbieter nicht nur, eine Anordnung lediglich weiterzuleiten, sondern vielmehr selbst zum Prozess beizutragen und aktiv und wiederholt mit diesen Nutzenden zu interagieren.

- Der Europäische Gerichtshof hat in der Rechtssache C-376/22 entschieden, dass abstrakte oder allgemeine Maßnahmen, die in anderen Mitgliedstaaten niedergelassenen Anbietern weitreichende Verpflichtungen auferlegen, im Widerspruch zum Herkunftslandprinzip stehen. Während sich der GgdG-E auf spezifische Anordnungen bezieht, wirkt § 6(2) faktisch als allgemeine Verpflichtung für die Betriebsstruktur von Diensteanbietern. Sie werden verpflichtet, im Vorfeld umfangreiche Maßnahmen zu ergreifen, um den in § 6(2) GgdG-E vorgesehenen Prozess zu bewältigen, insbesondere die unverzügliche Weiterleitung von Informationen oder die Zusicherung gegenüber dem Gericht, die Informationen weitergeleitet zu haben (was eine menschliche Überwachung erfordert).

4. Beweissicherung und Offenlegung

Wir erkennen zwar die Bedeutung der Beweissicherung für Opfer digitaler Gewalt an, doch der derzeitige Vorschlag gemäß § 3 GgdG-E führt zu erheblicher betrieblicher Ineffizienz und zu Rechtsunsicherheit für Opfer und Diensteanbieter. Wir schlagen die folgenden Präzisierungen vor, um sicherzustellen, dass das Verfahren verhältnismäßig und konsistent bleibt.

4.1. Optimierung des Offenlegungsablaufs

Die Verpflichtung der betroffenen Diensteanbieter, einen doppelten Offenlegungsprozess durchzuführen – zunächst die Daten an das Gericht und anschließend erneut an den Antragsteller zu übermitteln – ist grundsätzlich ineffizient und führt zu vermeidbaren operativen Reibungsverlusten.

Um diesen Prozess zu straffen, sollten die Anbieter lediglich verpflichtet sein, die relevanten Daten nach Erhalt einer Sicherungsanordnung zu sichern. Die tatsächliche Übermittlung dieser Daten durch die Anbieter sollte einmalig erfolgen: direkt an das Gericht, sobald das Offenlegungsverfahren abgeschlossen ist und eine verbindliche Offenlegungsanordnung vorliegt. Es sollte in der Verantwortung des Gerichts liegen, diese Daten an den Antragsteller weiterzuleiten. Dieser gestraffte Ansatz gewährleistet Verfahrenseffizienz und minimiert gleichzeitig Fehler bei der Datenverarbeitung. Um den harmonisierten Rechtsrahmen der EU zu wahren, sollten solche Offenlegungsanordnungen zudem an nicht in Deutschland ansässige Anbieter gemäß der Neufassung der Europäischen Zustellungsverordnung zugestellt werden, wobei etablierte grenzüberschreitende Dienstleistungsmechanismen anstelle innerstaatlicher Anforderungen genutzt werden sollten.

4.2. Technische Klarheit und Formatneutralität

Dem aktuellen Entwurf fehlt es an Konkretheit hinsichtlich der Frage, wie die betroffenen Dienstleister den Verletzer oder den rechtsverletzenden Inhalt identifizieren sollen. Um Verzögerungen zu vermeiden und Genauigkeit zu gewährleisten, ist es unerlässlich, dass gerichtliche Anordnungen spezifische technische Identifikatoren enthalten, die eindeutig sind. Sich auf Screenshots oder vage Beschreibungen zu stützen, könnte dazu führen, dass falsche Daten identifiziert werden, und ist operativ nicht durchführbar.

Darüber hinaus haben wir erhebliche Bedenken hinsichtlich der in § 3(2) GgdG-E enthaltenen Verpflichtung, Daten in „Textform“ bereitzustellen. Diese Anforderung ist übermäßig formalistisch und berücksichtigt moderne, sichere Datenübertragungsmethoden nicht. Anbieter sollten die Freiheit haben, geeignete elektronische Formate (z. B. sichere Download-Portale) zu wählen, die den von der EU genehmigten Sicherheitsstandards für die Datenübertragung entsprechen.

4.3. Übereinstimmung mit den Grundsätzen der Datenminimierung

Abschnitt 3(5) GgdG-E schreibt eine allgemeine Verpflichtung vor, gespeicherte Daten nach Abschluss eines Gerichtsverfahrens zu löschen. Wir halten diese spezifische Vorschrift für unnötig und sind der Ansicht, dass sie Rechtsunsicherheit schafft. Gemäß Artikel 5(1)(c) der DSGVO sind betroffene Diensteanbieter bereits an den Grundsatz der Datenminimierung gebunden, der die Löschung von Daten vorschreibt, sobald der rechtmäßige Zweck für deren Speicherung weggefallen ist. Die im GgdG-E vorgeschlagene Verpflichtung berücksichtigt nicht, dass Anbieter möglicherweise anderweitige rechtliche Gründe oder sogar Verpflichtungen haben, bestimmte Daten für andere Zwecke zu speichern. Die spezifische Löschpflicht in § 3(5) sollte gestrichen werden oder zumindest klarstellen, dass sie nur für Kopien gilt, die ausschließlich zum Zweck des GgdG-E-Verfahrens erstellt wurden, unbeschadet anderer gesetzlicher Speicherbefugnisse oder -pflichten.

5. Kontosperrung

Eine von einem Gericht angeordnete Kontosperrung nach §4(1) GgdG-E ist ein probates aber nur kurzfristig wirksames Mittel, weitere Rechtsverletzungen und Beeinträchtigungen von Persönlichkeitsrechten zu unterbinden. Allerdings ist die in §4(2) GgdG-E vorgeschriebene Anforderung, gesperrte Nutzende daran zu hindern, neue Konten zu eröffnen, angesichts der derzeitigen Funktionsweise von Online-Plattformen technisch und organisatorisch nicht umsetzbar und würde zudem erhebliche Datenschutzbedenken aufwerfen. Diese Anforderung lässt lediglich die Wahl zwischen einer nur kurzfristig wirksamen, rein symbolischen Sperrung und einer restriktiven, überwachungsintensiven Konstruktion, die die Zugänglichkeit und Offenheit des digitalen Raums grundlegend untergräbt.

Damit eine Sperre gegenüber einer vom Gericht identifizierten bestimmten Person wirksam ist, wären Plattformen im Grunde gezwungen, von *allen* Nutzenden (einschließlich Nutzenden, die den Dienst im abgemeldeten Modus besuchen) verifizierte, von Behörden ausgestellte Identitätsnachweise zu verlangen.

Alternativ könnten Plattformen eine Option anbieten, diesen Verifizierungsschritt zu überspringen. Böswillige Akteure würden sich unweigerlich für diese Option entscheiden, was den Sperrmechanismus unwirksam machen würde.

Aus organisatorischer Sicht würde die Implementierung eines solchen Verifizierungssystems die Erstellung komplexer, länderspezifischer ID-Sperrlisten erfordern, da sich die Identitätssysteme von Land zu Land erheblich unterscheiden. Die Entwicklung und Pflege eines solchen länderspezifischen Verifizierungsregimes stellte eine massive, aus dem Rahmen fallende Produktänderung dar, die wirtschaftlich kaum vertretbar wäre und die Nutzererfahrung erheblich beeinträchtigen würde.

6. Inländischer Zustellungsbevollmächtigter

Die Verpflichtung, einen inländischen Zustellungsbevollmächtigten zu benennen (siehe § 9(3) GgdG-E), verstößt gegen vorrangiges EU-Recht und stellt eine ungerechtfertigte Beschränkung der Dienstleistungsfreiheit dar.

Die Neufassung der EU-Zustellungsverordnung bietet ein harmonisiertes, funktionierendes System für die grenzüberschreitende Zustellung von Dokumenten. Diese Verordnung gewährleistet eine effiziente Zustellung, da sie ausdrücklich eine mögliche elektronische grenzüberschreitende Übermittlung von Dokumenten vorsieht. Es ist nicht erforderlich, die Bestellung eines inländischen Zustellungsbevollmächtigten vorzuschreiben.

Darüber hinaus ist es nach dem DSA sowohl verfahrensrechtlich ausreichend als auch eine Mindestvoraussetzung, behördliche Anordnungen der Mitgliedstaaten im Sinne der §§ 9 und 10 DSA an die von den Dienstleistern gemäß § 11 DSA benannte elektronische Kontaktstelle zu übermitteln. Dies dient dem Zweck, eine unverhältnismäßige Belastung des Dienstleisters zu vermeiden und einen zügigen Ablauf zu gewährleisten. Es ist unnötig und unverhältnismäßig, für Briefpost einen inländischen Zustellungsempfänger zu verlangen.

Schließlich verstößt § 9(3) GgdG-E gegen das Herkunftslandprinzip der ECD. Der Gesetzgeber kann sich nicht auf eine Ausnahme unter Verweis auf Erwägungsgrund 38 DSA berufen. Die Anordnung zur Benennung eines inländischen Zustellungsbevollmächtigten ist keine Anordnung zur Identifizierung und Entfernung rechtswidriger Inhalte im Sinne von Artikel 9 DSA.

* * *