20. Wahlperiode

Deutscher Bundestag
Ausschuss für Digitales

# Wortprotokoll
der 30. Sitzung

**Ausschuss für Digitales**
Berlin, den 1. März 2023, 14:00 Uhr
10117 Berlin, Adele-Schreiber-Krieger-Str. 1
Sitzungssaal: MELH 3.101

Vorsitz: Tabea Rößner, MdB

## Tagesordnung - Öffentliche Anhörung

**Tagesordnungspunkt 1** **Seite 03**

Chatkontrolle

**Liste der Sachverständigen**

**Ausschussdrucksache SB20(23)15**

**Fragenkatalog**

**Ausschussdrucksache SB20(23)16**

**Mitglieder des Ausschusses**

| | Ordentliche Mitglieder | Stellvertretende Mitglieder |
|---|---|---|
| SPD | Becker, Dr. Holger<br>Kassautzki, Anna<br>Klüssendorf, Tim<br>Marvi, Parsa<br>Mesarosch, Robin<br>Mieves, Matthias David<br>Schätzl, Johannes<br>Wagner, Dr. Carolin<br>Zimmermann, Dr. Jens<br>Zorn, Armand | Bartz, Alexander<br>Diedenhofen, Martin<br>Esken, Saskia<br>Hakverdi, Metin<br>Kaiser, Elisabeth<br>Leiser, Kevin<br>Müller (Chemnitz), Detlef<br>Papendieck, Mathias<br>Schneider, Daniel |
| CDU/CSU | Biadacz, Marc<br>Brandl, Dr. Reinhard<br>Durz, Hansjörg<br>Hoppermann, Franziska<br>Jarzombek, Thomas<br>Kemmer, Ronja<br>Reichel, Dr. Markus<br>Santos-Wintz, Catarina dos<br>Zippelius, Nicolas | Bär, Dorothee<br>Hahn, Florian<br>Hauer, Matthias<br>Heilmann, Thomas<br>Henrichmann, Marc<br>Metzler, Jan<br>Müller, Florian<br>Schön, Nadine<br>Steiniger, Johannes |
| BÜNDNIS 90/DIE GRÜNEN | Außendorf, Maik<br>Bacherle, Tobias B.<br>Gelbhaar, Stefan<br>Khan, Misbah<br>Rößner, Tabea | Bär, Karl<br>Christmann, Dr. Anna<br>Grützmacher, Sabine<br>Klein-Schmeink, Maria<br>Notz, Dr. Konstantin von |
| FDP | Funke-Kaiser, Maximilian<br>Mordhorst, Maximilian<br>Redder, Dr. Volker<br>Schäffler, Frank | Föst, Daniel<br>Höferlin, Manuel<br>Konrad, Carina<br>Kruse, Michael |
| AfD | Lenk, Barbara<br>Naujok, Edgar<br>Schmidt, Eugen<br>Storch, Beatrix von | Höchst, Nicole<br>Janich, Steffen<br>König, Jörn<br>Wiehle, Wolfgang |
| DIE LINKE. | Domscheit-Berg, Anke<br>Sitte, Dr. Petra | Pau, Petra<br>Reichinnek, Heidi |
| Fraktionslos | Cotar, Joana | |

**Tagesordnungspunkt 1**

**Chatkontrolle**

Die **Vorsitzende Tabea Rößner**: Es sind alle da, die heute an dieser Sitzung teilnehmen wollen und die geladen wurden. Ich begrüße Sie ganz herzlich zu unserer Anhörung des Ausschusses für Digitales. Ich begrüße die Mitglieder des Ausschusses ganz herzlich und natürlich auch die Vertreterinnen und Vertreter der Bundesregierung und der Bundesländer, die an dieser Sitzung teilnehmen. Ich heiße herzlich willkommen: Andreas Könen, Abteilungsleiter CI vom Bundesministerium des Innern und für Heimat (BMI). Zudem wird nachher noch der Parlamentarische Staatssekretär Johann Saathoff (BMI) zu uns kommen. Er muss im Moment noch die Präsenz im Plenum übernehmen, dann kommt er aber in einer Viertelstunde zu dieser Anhörung. Ich begrüße vom Bundesministerium der Justiz (BMJ) Vertreterinnen und Vertreter aus dem Referat Telekommunikations- und Medienrecht, digitaler Gewaltschutz und E-Privacy.

Diese Sitzung ist öffentlich und wird live im Parlamentsfernsehen und im Internet übertragen. Daher begrüße ich ganz besonders auch alle Zuschauenden sowohl hier im Saal auf der Tribüne als auch virtuell. Ich freue mich über Ihr Interesse an unserer Arbeit. Last but not least, möchte ich natürlich ganz herzlich die Sachverständigen, die heute gekommen sind, begrüßen:

- Elina Eickstädt, Informatikerin und Sprecherin des Chaos Computer Clubs
- Markus Hartmann, Leitender Oberstaatsanwalt, Leiter der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW)
- Ella Jakubowska, European Digital Rights (EDRi), Senior Policy Advisor
- Felix Reda, Gesellschaft für Freiheitsrechte (GFF), Projektleiter
- Prof. Dr.-Ing. Martin Steinebach, Fraunhofer-Institut für Sichere Informationstechnologie SIT, Leiter Abteilung Media Security und IT Forensics
- Joachim Türk, Der Kinderschutzbund Bundesverband e.V., Mitglied des Bundesvorstandes und stv. Landesvorsitzender
- Teresa Widlok, Verein für liberale Netzpolitik (LOAD e.V.), stv. Vorsitzende.

Weiterhin begrüße ich – inzwischen schon Dauergäste unserer Anhörungen:

- Prof. Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)
- Dr. Gerhard Schabhüser, Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Herzlich willkommen allerseits.

Zum Ablauf der Sitzung: Die Sachverständigen sind gebeten, zu Beginn ein fünfminütiges Eingangsstatement abzugeben. Dann bekommt jede Fraktion ein Zeitfenster von fünf Minuten für Fragen und Antworten. Das heißt, die Sachverständigen dürfen direkt und unmittelbar antworten. Am besten, Sie lassen das Mikro an. Sie brauchen nicht darauf zu warten, dass ich Ihnen das Wort erteile, damit die fünf Minuten auch bestmöglich ausgenutzt werden. Die Reihenfolge ergibt sich aus der Stärke der Fraktionen. Bei jeder weiteren Fragerunde,

das hängt ein bisschen von der Zeit ab, lege ich als Vorsitzende die Reihenfolge entsprechend der Vorgaben des § 28 Absatz 1 GO-BT fest. Die Redezeit pro Runde wird dann bei Bedarf verkürzt, da wir im Anschluss noch unsere reguläre Ausschusssitzung haben.

Ein gemeinsamer Fragenkatalog der Fraktion liegt vor und wurde als Ausschussdrucksache mit der Nummer SB 20(23)16 verteilt und veröffentlicht. Alle abgegebenen schriftlichen Stellungnahmen der Sachverständigen wurden auf der Internetseite des Ausschusses veröffentlicht. Das habe ich selber überprüft. Es wird ein Wortprotokoll über die Sitzung angefertigt und die Anhörung wird auf Kanal 2 live im Parlamentsfernsehen gestreamt und ist anschließend über die Online-Mediathek des Deutschen Bundestages abrufbar.

Die Besucherinnen und Besucher auf der Tribüne möchte ich noch einmal darauf hinweisen, dass – auch wenn es sich hier um eine öffentliche Sitzung handelt – das Fertigen von Ton- und Bildaufnahmen dieser Sitzung nicht zulässig ist. Entsprechende Geräte sind daher bitte abzuschalten. Zuwiderhandlungen gegen dieses Gebot können nach dem Hausrecht des Deutschen Bundestages zu einem dauernden Ausschluss von den Sitzungen des Ausschusses sowie des ganzen Hauses führen, wenn nicht sogar strafrechtliche Konsequenzen nach sich ziehen. Ich denke, das will keiner.

Zum technischen Verfahren möchte ich noch den Hinweis an die Sachverständigen geben: Bitte die Mikrofone anschalten – vor allem wenn Sie sich virtuell beteiligen – und nach Ihren Redebeiträgen wieder ausschalten. Wir haben heute eine englischsprachige Sachverständige eingeladen. Es findet eine simultane Verdolmetschung des gesprochenen Wortes sowohl von Deutsch auf Englisch als auch von Englisch auf Deutsch statt. Im Sitzungssaal können Sie die zur Auswahl des Sprachkanals ausliegenden Kopfhörer nutzen. In der Zoom-Sitzung stehen beide Sprachkanäle zur Auswahl. Die im Saal Anwesenden bitte ich, ihre Saalmikrofone zu nutzen und diese ebenfalls nach den Redebeiträgen auszuschalten. Ich hoffe, es gibt keine Aufkleber auf irgendwelchen Laptops. Haben wir das kontrolliert? Gut. Dann jedenfalls nicht so, dass sie erkennbar sind. Wir sind der Neutralität verpflichtet. Vielen Dank.

Das Thema der heutigen öffentlichen Anhörung ist die sogenannte „Chatkontrolle“. Unter diesem Begriff firmiert die öffentliche Debatte über den Entwurf der EU-Kommission vom 11. Mai 2022 für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern – kurz CSAM-Verordnung. Die Ausübung sexualisierter Gewalt gegenüber Kindern und Jugendlichen ist ein besonders schweres Gewaltdelikt. Ziel des Verordnungsvorschlages ist daher die Prävention sowie die effektive Bekämpfung des sexuellen Missbrauchs von Kindern und der Verbreitung ihrer Darstellung im Internet.

Die Europäische Kommission möchte zur Erreichung dieses Ziels unter anderem Hosting- und Messengerdienste verstärkt in die Pflicht nehmen. Die bisher geltende Verordnung EU 2021/1232 ist zum August 2024 befristet. Um nach Ablauf der Befristung der Verordnung weiterhin effektive Maßnahmen auf diesem Gebiet ergreifen zu können, hat die EU-Kommission nun diesen neuen Verordnungsvorschlag vorgelegt. Grundsätzliche Änderungen zu den bisherigen Regelungen bestehen insbesondere darin, dass die inhaltliche Überprüfung einzelner Inhalte durch den Diensteanbieter unter bestimmten Voraussetzungen verpflichtend sein soll. Durch die

technologieoffene Formulierung wäre auch der Inhalt von Ende-zu-Ende verschlüsselten Nachrichten durch Maßnahmen des sogenannten Client Side Scanning (CSS) zu analysieren und von privaten Endgeräten auszuleiten.

Der Verordnungsentwurf zielt auch auf die Bekämpfung des sogenannten Grooming, also die auf sexuellen Missbrauch ausgerichtete Kontaktaufnahme eines Erwachsenen zu einem Kind. Die Diensteanbieter müssen zunächst Risikominimierungsmaßnahmen implementieren, um Grooming zu unterbinden. Wenn diese nicht ausreichen, können Aufdeckungsanforderungen erfolgen, bei denen bestimmte Techniken zum Einsatz kommen müssten. Das sind zum Beispiel Maßnahmen der Altersverifikation. In der öffentlichen Debatte kamen erhebliche Zweifel auf, ob eine solche allgemeine Chatkontrolle das geeignete Instrument ist, um Kindesmissbrauch auch wirksam zu bekämpfen. Viele Expertinnen und Experten stellen infrage, dass anlasslose Maßnahmen einen verhältnismäßigen Eingriff in die Kommunikationsfreiheit, in die informationelle Selbstbestimmung und in das IT-Grundrecht darstellen.

Viele Stimmen haben kritisiert, dass die Vorschläge der EU-Kommission zu einer anlasslosen, flächendeckenden Überwachung der privaten Kommunikation führen könnten. Mit dem Schutz der Grundrechte und dem nationalen und europäischen Recht wäre das nur schwer vereinbar. Im Kontext der CSAM-Verordnung werden aber auch Fragen der effektiven Strafverfolgung, der Prävention und der Modalitäten des neu einzurichtenden EU-Zentrums sehr kontrovers diskutiert. Mit der heutigen Anhörung holt der Ausschuss für Digitales nun externen Sachverstand ein und wir erhoffen uns Antworten auf folgende Fragen: Inwieweit ist der Kommissionsvorschlag Ihrer Meinung nach geeignet, um das Ziel zu erreichen, Kinder effektiv vor sexueller Gewalt zu schützen und die Verbreitung von illegalem Video- und Bildmaterial zu unterbinden? Welche Anpassungen sind notwendig, um unverhältnismäßige Eingriffe in Grundrechte auszuschließen? Welche Empfehlungen haben Sie für den Deutschen Bundestag und die Bundesregierung im Hinblick auf die weitere Positionierung im Rat und in den Trilogverhandlungen?

Ich freue mich auf Ihre Beiträge und vor allem auf Lösungsvorschläge. Wir beginnen nun mit den fünfminütigen Eingangsstatements. Zuerst darf ich Frau Eickstädt vom Chaos Computer Club um ihr Statement bitten. Bitte, Sie haben das Wort.

SVe **Elina Eickstädt:** Vielen Dank, Frau Vorsitzende und vielen Dank an die Mitglieder des Ausschusses. Ich spreche heute als Vertreterin des Chaos Computer Clubs zu Ihnen und der Chaos Computer Club lehnt die Cybersecurity Information Sharing Act (CISA)-Verordnung grundsätzlich ab. Das Ziel, Kinder besser vor Missbrauch zu schützen, ist ein wichtiges. Was wir aber bekommen, ist der Plan für eine Überwachungsinfrastruktur, die noch nie dagewesen ist. Es wird wieder versucht, ein sehr komplexes gesellschaftliches Problem mit einfachen, fast nicht vorhandenen technischen Lösungen zu erschlagen. Am Anfang hat die Bundesregierung etwas verhalten reagiert. Nach der letzten durchgesickerten Stellungnahme des BMI konnten wir erkennen, dass es langsam in eine richtige Richtung geht. Es wurde immerhin anerkannt, dass verschlüsselte Kommunikation auf jeden Fall zu schützen ist.

Ich möchte an dieser Stelle noch einmal anmerken, dass auch unverschlüsselte Kommunikation vertrauliche Kommunikation

sein kann. Was die Verordnung allerdings noch mit sich ziehen würde, ist eine Ausweispflicht im Internet, Netzsperren, die – wie Herr Kelber in seiner schriftlichen Stellungnahme festgestellt hat – ein Zensur-Tool ohnegleichen sein können und ein EU-Zentrum, was sehr eng an Europol gekoppelt sein wird. Bei dem Umgang von Europol mit Daten ist es eher beunruhigend, wenn bei diesen Falschmeldungsraten Daten in deren Händen landen. Insgesamt ist dieses Gesetz eine Überschätzung von Fähigkeiten von Technologien, insbesondere wenn es um das Erkennen von unbekanntem Material und Anbahnungsversuchen – wie das sogenannte Grooming – geht. Hier haben wir es mit Fehlerraten zu tun, die nicht in den Griff zu bekommen sind. Denn gerade in interpersoneller Kommunikation und Textkommunikation ist eine Kontextualisierung des Materials unerlässlich. Das werden wir einfach nicht hinbekommen.

Wenn wir uns einmal die Fehlerraten anschauen und wenn wir zum Beispiel von einer Fehlerrate von einem Prozent ausgehen, haben wir bei einer Milliarde Nachrichten am Tag trotzdem zehn Millionen Falschmeldungen. Das müssen Sie sich einmal vorstellen. Stellen Sie sich vor, Sie bekommen 100 Meldungen von Ihrem Virusscanner am Tag. Es ist ziemlich schwer, da noch den Überblick zu behalten und auch zu evaluieren, was denn nun berechtigte Meldungen sind.

Dann zum Thema Altersverifikation: So, wie die Verordnung derzeit aussieht, würde sie für eine Ausweispflicht im Internet sorgen. Die Frage ist hier: Was ist eigentlich das Ziel? Jugendliche von den Plattformen, die sie zur Partizipation nutzen, fernzuhalten oder Erwachsene rauszuhalten? Insgesamt bin ich eigentlich ziemlich froh, dass ich das Recht auf Vergessenwerden habe und unbescholten das Internet erkunden konnte, als ich jung war. Die Frage, die wir uns ganz maßgeblich hier stellen müssen, ist: Möchten wir jetzt wirklich Millionen von Euro investieren und alle Expertinnen und Experten damit beschäftigen, dieses Gesetz zu verschlimmbessern? Oder möchten wir zusammen konstruktive Lösungen erarbeiten? Vielen Dank.

Die **Vorsitzende:** Herzlichen Dank. Als nächstes hat das Wort der Leiter der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen, Oberstaatsanwalt Markus Hartmann. Bitte schön.

SV **Markus Hartmann:** Vielen Dank, Frau Vorsitzende. Meine Damen und Herren Abgeordnete, ich möchte mich herzlich bedanken für die Möglichkeit, den Verordnungsvorschlag der Europäischen Kommission hier aus Sicht der Strafverfolgung zu beleuchten. Einleitend ist es wichtig zu sagen, dass es eine grundsätzlich gute, wichtige und richtige Initiative ist, auch europaweit den Fokus auf die Bekämpfung von internetkonnexem Kindesmissbrauch zu richten. Aus der Praxiserfahrung der Arbeit der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen in diesem Bereich kann ich Ihnen mitteilen, dass es sich insgesamt um ein soziodemografisch verbreitetes Kriminalitätsphänomen handelt, das kaum auf einen spezifischen Bereich des Internets einzugrenzen ist.

Die gelegentlich kolportierte Annahme, Kindesmissbrauch und entsprechende Darstellungen würden sich nur im sogenannten Darknet finden, ist fern der Realität – jedenfalls der Realität der Ermittlungsverfahren. Tatsächlich findet der weit überwiegende Teil entsprechender Straftaten aus dem 13. Abschnitt des Besonderen Teils des Strafgesetzbuchs im

ganz normalen Internet über Messenger, Chatplattformen und Dateihostingdienste statt. Deshalb ist es aus meiner Sicht wichtig und richtig, dass die Kommission über verbesserte Bekämpfungsmöglichkeiten nachsinnt. Zu begrüßen ist in diesem Zusammenhang die Stärkung der europäischen Zusammenarbeit durch ein EU-Zentrum. Auch wenn man mit Fug und Recht über die Einzelheiten der Ausgestaltung und den genauen Aufgabenkreis der Einrichtung debattieren kann und muss, sehe ich hier eine grundsätzlich richtige Initiative. Das gilt aus meiner Sicht auch für die Meldepflicht. Die gegenwärtige Strafverfolgungspraxis greift für eine sehr hohe Zahl von Verfahren auf Meldungen ausländischer oder – genauer – außereuropäischer Meldepartner zurück.

Wenn man die Bedeutung dieser Hinweise für die Strafverfolgungspraxis ernst nimmt, ist es konsequent, wenn auch ein europäisches Äquivalent eingerichtet wird. Damit verbleibt im Kern die Frage, aus welchen Quellen Provider und Diensteanbieter ihre Meldegrundlagen beziehen sollen. Unproblematisch sind sicher Hinweise Dritter, etwa von Nutzenden der jeweiligen Dienste, an die Anbieter. Rechtlich fraglich ist aus meiner Sicht jedoch, ob und in welcher Intensität eigene Detektionsmechanismen der Anbieter angewandt werden können und sollen. Denn es gibt keine Strafverfolgung um jeden Preis. Auch wenn wir etwa, um ein analoges Beispiel zu bemühen, Kameraüberwachung an öffentlichen Orten und Kriminalitätsschwerpunkten zulassen, um Straftaten zu bekämpfen, hängen wir Kameras nicht in jede Privatwohnung. Der damit verbundene Eingriff in die Privatsphäre wäre deutlich zu hoch. Oder anders formuliert: Das staatliche Interesse an einer funktionsfähigen Strafrechtspflege ist in einen sachgerechten Ausgleich mit den betroffenen grundrechtlichen Positionen zu bringen. Strafrecht ist in diesem Sinne angewandte Verhältnismäßigkeit.

Nach diesen Grundsätzen sind vor allem zwei Defizite des Kommissionsvorschlags anzusprechen. Soweit die Kommission große Hoffnung auf den Einsatz Künstlicher Intelligenz zur automatisierten Detektion und Bewertung inkriminierter Inhalte zu setzen scheint, wird diese Hoffnung nicht tragen. Meine Zentralstelle beschäftigt sich bereits seit 2017 mit dem produktiven Einsatz von Künstlicher Intelligenz in diesem Bereich und hat mit „Aira“ ein Tool für die Praxis der Strafverfolgung entwickelt. Ich kann Ihnen aus dieser mehrjährigen Erfahrung berichten, dass KI sehr gut geeignet ist, eine kriminalistische Hypothese im Sinne eines bereits bestehenden Anfangsverdachts schnell und gründlich zu überprüfen.

KI ist jedoch ungeeignet, einen solchen Anfangsverdacht überhaupt zu begründen. Denn die Fehlerraten im Bereich von False Positives sind selbst mit einem einstelligen Prozentbereich in absoluten Zahlen noch so hoch, dass unzulässig viele Betroffene in den Fokus von Behörden gerieten. Die Detektionsmechanismen sollten sich – jedenfalls auf Basis des derzeitigen technologischen Standes – deswegen auf das Wiedererkennen bereits klassifizierten Materials über hashbasierte Verfahren begrenzen. Soweit die Kommission auch Ende-zu-Ende verschlüsselnde Dienste zum Scannen der Nutzungsinhalte verpflichten will, kann das im Ergebnis technisch nur durch einen Eingriff nach oder vor der Verschlüsselung, das heißt, auf den Endgeräten der jeweiligen Nutzenden gelingen. Damit unterminiert die Kommission faktisch das wichtigste digitale Schutzmittel. Als Leiter einer technischen Cybercrime-Dienststelle, die auch mit dem Schutz kritischer Infrastrukturen von Behörden und

Unternehmen befasst ist, kann ich Ihnen sagen: Kompromittierte Verschlüsselung ist im Ergebnis keine Verschlüsselung. Ein so weitgehender Eingriff ist bei einer umfassenden rechtlichen Bewertung nicht erforderlich, denn es gibt ein milderes Mittel. Die derzeit oftmals in den Ressourcen, teils aber auch in den gesetzlichen Grundlagen unzureichend aufgestellten Strafverfolgungsbehörden müssen national, aber auch bewusst im europäischen Kontext so gestärkt werden, dass auf Basis der Hinweise aus dem – aus meiner Sicht vertretbaren – serverseitigen, hashbasierten Scannen und aus den Erkenntnissen der Ermittlungsverfahren selbst, ausreichend Informationen generiert werden können, um damit internetkonnexe Missbrauchstaten und entsprechende Darstellung wirkungsvoll und nachhaltig zu bekämpfen. Vielen Dank.

Die **Vorsitzende:** Vielen Dank. Jetzt begrüße ich noch einmal den Parlamentarischen Staatssekretär Johann Saathoff und gebe das Wort weiter an Ella Jakuboswka, Senior Policy Advisor, European Digital Rights. Sie ist uns digital zugeschaltet. Sie haben das Wort.

SVe **Ella Jakubowska:** Guten Tag. Entschuldigung, dass ich nicht bei Ihnen vor Ort sein kann, aber dennoch bin ich dankbar für die Einladung zu dieser Sitzung, da ich der festen Überzeugung bin, dass wir einen EU-Gesetzesvorschlag auf dem Tisch haben, der die Privatsphäre und Sicherheit im Internet in einem Ausmaß bedroht, wie ich es in meiner Laufbahn noch nicht erlebt habe. Zum Hintergrund: Ich arbeite bei EDRi. Das ist eine Organisation, bei der Gesetze, die Menschenrechte im digitalen Raum beeinträchtigen, überwacht werden. Daher glaube ich, dass das wirklich etwas aussagt. Wie Sie bereits gehört haben, stellt der vorliegende Vorschlag völlig falsch dar, wozu Technologie imstande ist, insbesondere wenn es sich um ein derart komplexes gesellschaftliches Problem handelt. Sogar die Erarbeitung dieses Gesetzes auf EU-Ebene wurde von einigen ernsthaften Prozessproblemen begleitet. Ich möchte Ihnen nur ein Beispiel nennen: Der interne Überprüfungsausschuss der Europäischen Kommission hat davor gewarnt, dass der Vorschlag nicht ausreichend auf das Risiko der digitalen Massenüberwachung eingeht. Die Europäische Kommission hat diesen Hinweis jedoch vollständig ignoriert und weiter am Vorschlag festgehalten. Das heißt im Einzelnen, dass es sehr deutlich ist, dass die Privatsphäre und die private und sichere Kommunikation eines der wenigen Werkzeuge sind, die uns zur Verfügung stehen, um uns als Bürger, Journalisten, Anwälte, Menschenrechtsaktivisten, Personen auf der Suche nach Gesundheitsdiensten, queeren Gemeinschaften usw. sicher im Internet zu bewegen. Im Kern würde dieser EU-Vorschlag jedoch in die Privatsphäre der Online-Kommunikation eindringen, also in E-Mails, Chats, private Nachrichten, Texte, Fotos in persönlichen Clouds.

Für mich ist hierbei entscheidend, dass dies nach dem Vorschlag anhand freiwillig genutzter Dienste und nicht anhand des begründeten Verdachts eines Kindesmissbrauchs erfolgen würde. Das heißt kurz zusammengefasst, dass dieses Gesetz das Recht auf Privatsphäre, Datenschutz und freie Meinungsäußerung einer sehr großen Anzahl an gesetzeskonformen Internetnutzern ebenso wie von tatsächlichen Verdächtigen verletzen würde. Das ist in Bezug auf Demokratie und Rechtsstaatlichkeit nicht zu rechtfertigen. Bei diesem Ausmaß an digitalen Eingriffen handelt es sich zudem um etwas, was wir in einer demokratischen Gesellschaft noch nicht erlebt haben. Wir haben jedoch erlebt, wie zum Beispiel die chinesische Regierung, die

bereits Unternehmen zur Verwendung von Online-Filtern zwingt – angeblich um Urheberrechtsverletzungen zu ermitteln – diese Filter zweckentfremdet, um Kritik an der Politik aufzuspüren und zu entfernen. Wir können auch einen Blick nach Großbritannien werfen, wo derzeit ein Vorschlag zur Nutzung von Technologien zur Blockierung des Inhalts sozialer Medien, wenn dort Unterstützung für Asylbewerber ausgedrückt wird, vorliegt. Außerdem ist, wie wir bereits gehört haben, bekannt, dass alle Methoden, die Inhalte auf den persönlichen Geräten scannen, Hacks von bösartigen Akteuren, bösartigen Staaten, Stalkern, sogar von einem Missbrauchstäter, der das Telefon eines jungen Menschen infiltrieren möchte, Tür und Tor zu diesen Geräten öffnen würden.

Wir warnen davor, dass es, sobald diese Technologien einmal in der Welt sind, keine Möglichkeit gibt, ihren Gebrauch auf demokratische Zwecke zu beschränken. Und wir wollen auf keinen Fall, dass die EU diesen Freifahrtschein ausstellt. Ein weiterer Aspekt, der ebenfalls oft vollständig in dieser Debatte fehlt, ist das Recht von Kindern auf Privatsphäre und Datenschutz. Im EU-Vorschlag wird das Internet als grausamer und gefährlicher Ort für junge Menschen dargestellt. Wir wissen jedoch, dass es jungen Menschen auch enorme Vorteile bietet. Nach diesem Vorschlag könnten jedoch sowohl der einvernehmliche Austausch intimer Bilder zwischen Jugendlichen als auch das Teilen von Aufklärungsmaterialien kriminalisiert werden. Mit Blick auf Leitlinien von UN, UNICEF und Child Rights International lässt sich sagen, dass all diese Organisationen ausdrücklich vor der allgemeinen Überwachung der digitalen Aktivitäten junger Menschen warnen. Um abschließend kurz darauf einzugehen, was getan werden kann: EDRi ist Teil eines Bündnisses aus 124 Gruppen der Zivilgesellschaft, die alle die EU mahnen, diesen Vorschlag zurückzuziehen und einen besseren vorzulegen, der durch einen Wirksamkeitsnachweis untermauert wird und mit den EU-Menschenrechten vereinbar ist. Wir zählen sehr auf die Hilfe nationaler Parlamente und Behörden wie in Deutschland. Sie haben eine mächtige Position in EU-Verhandlungen inne und können dieses Gesetz überprüfen und sicherstellen, dass die Exekutive der EU im Zaum gehalten wird.

Die **Vorsitzende:** Vielen Dank. Wir kommen zu Felix Reda, Projektleiter der Gesellschaft für Freiheitsrechte, der uns ebenfalls digital zugeschaltet ist. Herzlich willkommen.

SV **Felix Reda:** Vielen Dank für die Einladung. Es tut mir leid, dass ich nur digital teilnehmen kann. Sehr geehrte Abgeordnete, der Schutz von Kindern vor sexueller Gewalt ist ein wichtiges Anliegen, das Grundrechtseingriffe rechtfertigen kann. Dem Kinderschutz ist aber nicht gedient, wenn wir ein evident grundrechtswidriges Gesetz wie die Chatkontrolle-Verordnung verabschieden, das dann später vor dem Europäischen Gerichtshof scheitert. Der Schaden für die Privatsphäre aller Menschen, gerade auch von Kindern und Jugendlichen, wäre aber bereits immens, wenn diese Verordnung nur für eine kurze Zeit Gültigkeit hätte.

Es ist erst einmal erfreulich, dass inzwischen die Bundesregierung einen Konsens darüber erreicht zu haben scheint, dass das Client Side Scanning abzulehnen ist. Das allein reicht aber bei weitem nicht. Aus grundrechtlicher Perspektive macht es keinen entscheidenden Unterschied, ob die Überwachung von privater Kommunikation auf einem verschlüsselten oder einem unverschlüsselten Dienst stattfindet. Die

Verschlüsselung ist ein technisches Werkzeug, mit dem sich eine verständige Nutzerin von Überwachung schützen kann. Die Grundrechte gelten aber unabhängig von dem technischen Verständnis der Grundrechtssubjekte. Die anlasslose Überwachung von privaten Chats, von E-Mails, von Videotelefonaten und so weiter, verletzt den Wesensgehalt des Rechts auf Privatsphäre und kann damit durch keine Grundrechtsabwägung gerechtfertigt werden. Das ergibt sich aus dem Urteil des Europäischen Gerichtshof (EuGH) im Fall Digital Rights Ireland. Da hat der Gerichtshof deutlich gemacht, dass Überwachungsmaßnahmen den Wesensgehalt des Grundrechts auf Privatsphäre dann antasten, wenn sie die Kenntnisnahme des Inhalts elektronischer Kommunikation gestatten – und eben nicht nur von Metadaten.

Es ist klar: Bei der Chatkontrolle geht es genau um diese Überwachung der Kommunikationsinhalte von Chats, E-Mails und Videotelefonaten. Dazu betrifft das besonders solche Inhalte, die der absoluten Intimsphäre zuzurechnen sind, nämlich die Art von Kommunikation, die von einem automatischen Algorithmus als ähnlich zu Darstellungen sexueller Gewalt gegen Kinder aufgefasst wird. Es landen dann Bilder von einvernehmlichen Sexting unter Jugendlichen oder jungen Erwachsenen auf den Tischen von EU-Beamt:innen und Strafverfolgungsbehörden. Letztere müssen bei einem Verdacht einer Straftat dann Ermittlungen aufnehmen – mit potenziell weitreichenden Folgen für die Betroffenen.

Egal, ob es sich um verschlüsselte oder unverschlüsselte Inhalte handelt: Die Chatkontrolle verletzt den Wesensgehalt des Rechts auf Privatsphäre und hat unserer Ansicht nach keine Chance, vor dem EuGH Bestand zu haben. Es ist zu wenig, die Privatsphäre nur von denjenigen Menschen zu schützen, die sich durch Verschlüsselung selbst schützen können. Ein weiteres Thema, das der Gesellschaft für Freiheitsrechte am Herzen liegt, ist die Altersverifikation. Ich glaube, es ist noch nicht allen bewusst, wie weit der Verordnungsentwurf in diesem Punkt wirklich geht. Einerseits müssen die Anbieter von allen Kommunikations- und Hosting-Diensten das Alter ihrer Nutzer ermitteln. Im Klartext heißt das für die Zukunft: kein E-Mail-Account mehr ohne einen Altersnachweis. Zusätzlich müssen alle Anbieter von App-Stores eine Altersverifizierung einführen. Diese werden darüber hinaus verpflichtet, alle Minderjährigen ausfindig zu machen und automatisch von Apps auszusperren, die ein hohes Risiko für Grooming haben.

Was passiert denn dann bei dieser doppelten Altersverifizierung mit den Menschen, die ihr Alter nicht nachweisen können, weil sie keine Papiere haben oder weil der Algorithmus sie falsch einstuft? Diese Menschen können dann nicht mehr sinnvoll online kommunizieren. Entweder, ich kann mir keinen Account bei einem Dienst erstellen, da ich mein Alter nicht verifizieren kann, oder – wenn der Dienst mir trotzdem einen Account gibt – es gilt die App als risikoreich und ich kann sie im App-Store nicht mehr herunterladen, weil ich dem App-Store nicht beweisen kann, dass ich volljährig bin. Besonders dramatisch ist die Forderung nach Altersverifikation außerdem für Open Source-Software, wie zum Beispiel dem Messenger Signal. Eine verpflichtende Altersverifizierung ist mit Open Source schlicht nicht vereinbar. Diese Garanten für IT-Sicherheit würden damit aus Europa verdrängt.

Zuletzt noch ein paar Worte zu den vorgesehenen Netzsperren. Die Chatkontrolle-Verordnung sieht nämlich Netzsperren gegen

einzelne URLs vor, also einzelne Unterseiten einer Webseite. Das ist technisch schlichtweg nicht möglich. Netzsperren finden stets auf der Ebene einer ganzen Domain statt. Wenn eine Behörde beispielsweise eine Netzsperre anordnet gegen eine einzelne Datei, die auf so einem Sharehosting-Dienst wie Dropbox hochgeladen wurde, dann müsste der ganze Dienst Dropbox gesperrt werden, um dieser Anordnung nachzukommen. URL-basierte Netzsperren wären nur mit einem vollständigen Verzicht auf https-Verschlüsselung möglich. Diese https-Verschlüsselung ist unerlässlich für IT-Sicherheit. Wenn Sie zum Beispiel bei Ihrem Online-Banking Ihr Passwort eingeben, würden Fremde dieses Passwort sonst mitlesen können. Es gibt keine technische und grundrechtskonforme Möglichkeit, diese URL-basierten Netzsperren umzusetzen. Ich möchte deshalb davor warnen, die Debatte um die Chatkontrolle-Verordnung auf das Thema Client Side Scanning zu verengen. Ich hoffe, ich konnte Ihnen deutlich machen, dass es darüber hinaus noch viele weitere Gefahren für die Grundrechte gibt, die im Rahmen der Chatkontrolle-Verordnung beseitigt werden müssen. Vielen Dank.

Die **Vorsitzende:** Vielen Dank. Als nächstes hat das Wort Professor Martin Steinebach vom Fraunhofer Institut für sichere Informationstechnologie. Bitte schön.

SV **Prof. Dr. Martin Steinebach:** Vielen Dank für das Wort. Sehr geehrte Damen und Herren, ich bin selbst ein Wissenschaftler, der zu den drei Erkennungstechnologien – jeweils im Team – Verfahren entwickelt hat. Wir haben diese Erkennung zu bekannten Darstellungen, unbekannten Darstellungen und Cybergrooming ausprobiert, und aus der Erfahrung muss man ganz klar sagen: Diese drei Typen von Erkennungsverfahren werden in dem Vorschlag gleichgestellt, haben aber einen massiven Unterschied in der Komplexität und den zu erwartenden Fehlerraten. Das heißt also: Erkennung von bekanntem Material ist relativ einfach. Cybergrooming-Erkennung auf der anderen Seite ist ein hoch komplexes Thema, das eigentlich bis jetzt nicht wirklich ausführlich erforscht ist. Es geistert manchmal die Aussage herum, dass diese Erkennungsraten bei 99,9 Prozent liegen. Diese 99,9 Prozent kann ich mir aus der Praxis nur damit erklären, dass man die Erkennung bekannter Darstellungen genommen hat und das einfach auf die anderen Konzepte übertragen hat. Bei robusten Hashverfahren und ähnlichen Technologien zur Erkennung passt das, bei den anderen ist es unrealistisch.

Bei Darstellungen von unbekanntem Kindesmissbrauch liegen wir bei Fehlerraten von im Mittel zehn Prozent als eine realistische Größenordnung. Wir hatten vor kurzem ein Treffen mit einem Forscher aus Brasilien, der mit der Polizei Systeme entwickelt hat. Die haben 84 Prozent Erkennungsrate und fünf Prozent Falsch-Positiv-Rate, nur einmal als Größenordnung. In der Literatur über Cybergrooming-Erkennung spricht man von Fehlerraten zwischen 10 und 20 Prozent. Einfach, dass man einmal eine Größenordnung hat. Dann muss man bei den Fehlerraten auch anschauen: Was bedeutet das? Wir haben Milliarden von Bildern jeden Tag. Diese Fehlerraten, die zu erwarten sind, führen dazu, dass dann viele Millionen Inhalte händisch geprüft werden müssen. Das ist auf der einen Seite natürlich ein Privatsphäreneingriff, auf der anderen Seite stellt sich die Frage: Wie will das überhaupt jemand bewältigen? Das ist ziemlich unklar.

Dann muss einem klar sein: Die Fehlerraten sind abhängig voneinander. Wenn wir zu dem Schluss kommen würden, dass die Falsch-Positiven das Problem sind, dann können wir die natürlich extrem niedrig

machen. Wir können an einen Punkt kommen, an dem wir vielleicht nur ein Promille Falsch-Positive haben. Wir werden aber auch Erkennungsraten haben, die völlig trivial sind. Dann kann es durchaus sein, dass die Erkennungsrate eben auch nur bei ein bis zwei Promille liegt. Dann ist die Frage: Was für einen Nutzen werden solche Systeme dann noch haben? Das muss wirklich beachtet werden. Was auch klar sein muss: Diese Verfahren, von denen wir reden, das Erkennen von unbekannten Inhalten über maschinelles Lernen – und das wird es sein – ist inhaltsabhängig. Das bedeutet, dass – abhängig davon, welche Art von Inhalten ich üblicherweise betrachte – ich meine Fehlalarme deutlich steigern werde. Wenn ich regelmäßig erotische Inhalte mit legalen, 20-jährigen Darstellerinnen betrachte, ist die Wahrscheinlichkeit viel, viel höher, dass ich viele Fehlalarme produziere, als wenn ich auf meinem Smartphone üblicherweise Landschaftsaufnahmen betrachte. Einfach, weil Ähnlichkeit die Erkennungsraten hochführt. Es kann durchaus sein, dass irgendwelche Fotografen von Kindergeburtstagen plötzlich höhere Fehlerraten produzieren.

Bei dem Einsatz von den Verfahren wird in dem Vorschlag gesagt, dass man irgendwelche Indikatoren für die Betreiber bereitstellt, um ihre eigenen technischen Lösungen umzusetzen. In der Praxis wird es eigentlich nur so gehen, dass sie wirklich auf dem Material ihr Training durchführen müssen, und dafür muss man sich Konzepte überlegen. Ich glaube nicht, dass wir wollen, dass wir jedem, der ein System betreibt, eine Million kinderpornografische Bilder an die Hand geben, damit er seine individuelle Lösung trainieren kann. Aus Sicht der Cybersicherheit noch ganz wichtig: Diese robusten Verfahren, diese Erkennungsverfahren, sind alles keine sicheren Verfahren. Das sind Verfahren zur Erkennung. Aber es gibt viele Angriffe auf diese Verfahren. Die werden meistens völlig ignoriert und können wirklich auch zu Problemen führen. Vielen Dank.

Die **Vorsitzende:** Vielen Dank. Und jetzt schalten wir noch einmal ins Netz zu Joachim Türk vom Kinderschutzbund Bundesverband e.V.

SV **Joachim Türk:** Ja, danke für die Möglichkeit, hier sprechen zu können und die Haltung des Kinderschutzbundes zu der EU-Initiative, an der wir uns hart abgearbeitet haben, zu erläutern. Sehr geehrte Abgeordnete, bei aller Kritik an der Initiative – sie hat auch ihre guten Seiten und wichtige Impulse. Vor allem schafft sie Öffentlichkeit für ein Thema, das den Kinderschutzbund zutiefst berührt. Sie löst öffentliche Diskussionen aus, wie diese hier, an der Experten teilnehmen, die man – mit Verlaub gesagt – vielleicht schon früher hätte fragen können. Dafür sind wir dankbar und davon wünschen wir uns mehr.

Allerdings offenbaren verschiedene Äußerungen in der Auseinandersetzung um Inhalte der Initiative seltsame Haltungen, die wir nicht teilen können. Zwei Beispiele dazu: Das hier ist kein Wettstreit von Kinderschutz gegen Datenschutz. Gesetzgeber müssen beim Eingriff in Verfassungsrechte – so sinnvoll sie in der Verbrechensbekämpfung sein mögen – immer einen Ausgleich herstellen, und das gilt auch hier. Was uns vorliegt, ist kein Ausgleich. Sowohl das Recht auf körperliche Unversehrtheit als auch das Recht auf geschützte Kommunikation sind Kinderrechte. Vertrauliche Kommunikation ist eine Säule der freien Meinungsäußerung und damit der Demokratie, in der Kinder und Jugendliche aufwachsen – und zwar möglichst angstfrei, ohne die Sorge, überwacht zu werden. Diese unsere

Überzeugung macht es uns unmöglich, die anlasslose Chatkontrolle als Option zu akzeptieren. Zudem erwarten wir eine hohe Quote fehlerhafter Ergebnisse, die die Polizeiarbeit eher erschweren wird, als sie zu stärken, und sicherlich noch mehr minderjährige Tatverdächtige als heute. Punkt zwei: Es entsteht der Eindruck – es ist heute schon angesprochen worden – dass technische Werkzeuge genügen, diese schreckliche Pandemie der Gewalt gegen Kinder zu beenden oder zumindest zu bremsen. Auch wir halten es für wichtig, öffentliche Bereiche des Netzes nach solchen Darstellungen zu durchsuchen, die Urheber zu ermitteln und die Gewalttäter dingfest zu machen. Aber wir zweifeln daran, dass die vorgeschlagenen Methoden so erfolgreich sein können, wie es momentan vorhergesagt wird.

Schon heute lösen die allermeisten der Scantreffer in Deutschland Verfahren wegen der Verbreitung von kinderpornografischem Material aus – darunter fast die Hälfte gegen Minderjährige. Verfahren gegen Gewalttäter werden deutlich seltener eingeleitet. Wir gehen mit vielen anderen Experten davon aus, dass es ein gewaltiges Dunkelfeld sexualisierter Gewalt gegen Kinder im sozialen Nahbereich gibt, zu der immer Machtmissbrauch gehört. Die Anbahnung solcher Taten geschieht in der Nachbarschaft, in Vereinen, durch Verwandte oder – mit Blick auf Wermelskirchen – durch Babysitter. Es wäre fatal, wenn wir im Vertrauen auf Scans, auf irgendeine KI, dieses Dunkelfeld nicht weiter bearbeiten würden, vor allem durch Prävention, durch sensibles Hinsehen, durch Forschung. Aber das ist mühsam und teuer, trotzdem brauchen wir es. Lassen Sie mich kurz noch ein weiteres Thema ansprechen, das mir momentan zu kurz kommt: Wir erwarten eine erhebliche Zunahme von Darstellungen sexualisierter Gewalt gegen Kinder, die von KI-Systemen erzeugt werden. Eine Strategie, die wesentlich auf die Aufdeckung von Bildern und Videos zielt, muss dies berücksichtigen.

Zuletzt noch eine weitere Anmerkung zur EU-Initiative selbst. Es ist grundsätzlich zu begrüßen, dass stärker gegen sexualisierte Gewalt angegangen wird. Wir unterstützen die Einrichtung einer zentralen Behörde, die die Abhängigkeit von der amerikanischen NCMEC (National Center for Missing & Exploited Children) beendet, europäisches Recht in den Vordergrund stellt, Strategien entwickelt und testet, Unternehmen berät und begleitet und vorbeugende Maßnahmen entwickelt, aber auch Angebote für Betroffene unterbreitet und diese vernetzt. Löschung ist wichtig. Wir wollen den Dauerkreislauf des Materials aus dem Darknet in die Öffentlichkeit durchbrechen. Unser Vorschlag: Um den zeitlichen Druck zu verringern, plädieren wir dafür, die Ausnahmeregelung zur E-Privacy-Richtlinie zu verlängern, aber unter anderem die Einrichtung einer zentralen Behörde zu beschließen und anzugehen. Vielen Dank.

Die **Vorsitzende:** Vielen Dank. Wir schalten jetzt noch einmal zurück in den Saal zu Teresa Widlok vom Verein für liberale Netzpolitik (LOAD e.V.). Sie haben das Wort.

SVe **Teresa Widlok:** Herzlichen Dank, Frau Vorsitzende. Liebe Abgeordnete, es wurde gerade schon mehrfach erwähnt: Was wir mit diesem Entwurf sehen, ist eine Überwachungsinfrastruktur in bisher unvorstellbarem Ausmaß. Ich will deshalb meinem Statement den folgenden Satz beziehungsweise den folgenden Gedanken voranstellen: Der wohlmeinende Überwachungsstaat ist ein machtvolles, gefährliches und falsches Narrativ. LOAD ist Teil des Bündnisses "Chatkontrolle stoppen". Das wurde hier auch schon zweimal

angesprochen. Deswegen lehnen wir insbesondere den Teil des Verordnungsentwurfes ab, der als sogenannte Chatkontrolle bekannt ist. Im Wesentlichen geht es darum, Strukturen aufzubauen, die das Überwachen und Durchleuchten jeglicher Kommunikation ermöglichen. Kommunikationsanbieter sind Messenger wie WhatsApp, E-Mail-Anbieter, aber auch Chatmöglichkeiten in Videokonferenzen und Games. Also auch Nebenkommunikation muss auf Anordnung in ihren Angeboten nach bereits bekannten und neuen Missbrauchsdarstellungen suchen oder Textnachrichten auswerten, um Verhalten zu erkennen, mit dem sich Erwachsene Kindern in sexueller Absicht nähern – das sogenannte Grooming.

Aus grundrechtlicher Perspektive würde eine Struktur zur Überwachung der Kommunikationen in das Recht auf informationelle Selbstbestimmung, das Recht auf Vertraulichkeit der Kommunikation, das IT-Grundrecht – je nachdem, wie man die Überwachung ausgestaltet – und das in der europäischen Grundrechte-Charta explizit erwähnte Recht auf Privatheit in massivem Umfang eingreifen. Die europäische Rechtsprechung, die Rechtsprechung des EuGH, wurde gerade auch schon erwähnt. Der hat nämlich gesagt, dass Inhalte von Kommunikation immer tabu sein müssen und schon gar nicht massenhaft überwacht werden dürfen. In Ihrem Fragenkatalog haben Sie, liebe Abgeordnete, für diese Anhörung die Konsequenzen teilweise schon selbst nahe gelegt.

Der Aufbau von Überwachungsstrukturen durch die verpflichteten Anbieter schafft Angriffsflächen für Hacking und eine Blaupause für autokratische Staaten, sich auf unsere europäische, rechtsstaatlich zustande gekommene Regulierung berufen zu können. In dem Ihnen vielleicht bekannten Papier "Bugs in our Pockets", von international anerkannten IT-Sicherheitsforschern und Experten wird auch begründet, warum jede installierte Überwachungsinfrastruktur nicht die Sicherheit stärkt, sondern im Gegenteil die Sicherheit von IT-Produkten immer schwächt. Ich will ein Zitat kurz bringen aus diesem Papier: CSS, also das Client Side Scanning – „naturgemäß für die gesamte Gesellschaft schwere Risiken für Sicherheit und Privatsphäre birgt, wogegen die Hilfe, die es dem Gesetzesvollzug bieten kann, bestenfalls als problematisch zu bezeichnen ist“. Das haben wir von Herrn Hartmann auch gerade schon gehört. An dieser Stelle will ich ganz kurz erwähnen, dass der Entwurf selbst sehr stark die Grundrechte der potenziellen Opfer von sexuellem Missbrauch oder Grooming hervorruft. Der Entwurf soll zur Aufdeckung neuer Opfer führen, die vorher unbekannt waren, sagt er an mehreren Stellen. Eine Zahl von neu aufgedeckten Opfern, von der man ausgeht, wird uns allerdings nicht genannt. Das heißt, die Durchführung einer echten Verhältnismäßigkeitsprüfung, ob die beeinträchtigten Grundrechtspositionen, die ich am Anfang aufgezählt habe, auf der einen Seite und die Rechte derjenigen, die jetzt als neue Opfer aufgedeckt wurden, auf der anderen Seite gegeneinander abgewogen werden, ist dementsprechend nicht möglich.

Als Fazit an dieser Stelle: Überall dort, wo anlasslose Strukturen für das Speichern, das Auswerten von Daten oder das anlasslose Eindringen in IT-Systeme verboten sind, muss eigentlich auch der anlasslose Einsatz von CSS verboten sein. Der Entwurf hat natürlich nicht nur Schatten, sondern es gibt auch ein paar Punkte, die positiv hervorzuheben wären – zum Beispiel die Risikoabschätzung, die grundsätzlich positiv von uns bewertet wird. Aber ich will an einer Stelle doch noch einmal einhaken, und zwar

beim Recht auf Verschlüsselung. Unserem verstorbenen Vereinsgründer Jimmy Schulz, der auch einmal Vorsitzender dieses Gremiums war, war es ein ganz besonderes Anliegen, das Recht auf Verschlüsselung an jeder Stelle hervorzuheben. Wir fordern deswegen auch als LOAD schon ganz lange, dass man Kommunikationsanbieter und auch Anbieter für das Speichern von Daten dazu verpflichten sollte, diese alle standardmäßig Ende-zu-Ende zu verschlüsseln. Auch wenn es nicht nur um verschlüsselte Kommunikation geht, sondern auch um jegliche Kommunikation und jegliche Vertraulichkeit von Kommunikation, muss konstatiert werden, dass dieser Entwurf dazu führen würde, dass das Recht auf Verschlüsselung – das so auch im Koalitionsvertrag steht – in weite Ferne rückt. Deswegen schließen wir uns aus Sicht von LOAD der Forderung des Bündnisses "Chatkontrolle stoppen" an, dass dieser Entwurf, so wie er jetzt ist, zurückgezogen werden muss und grundsätzlich überarbeitet gehört. Vielen Dank.

Die **Vorsitzende:** Ganz herzlichen Dank. Das waren die Eingangsstatements der Sachverständigen und nun kommen wir in die Frage- und Antwortrunde, in der natürlich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wie auch der Vertreter des Bundesamts für Sicherheit in der Informationstechnik (BSI) befragt werden können. Ich übergebe das Wort an Anna Kassautzki für die SPD-Fraktion.

Abg. **Anna Kassautzki** (SPD): Vielen Dank, Frau Vorsitzende. Vielen Dank auch an die Sachverständigen, sowohl für die mündlichen Erläuterungen als auch für die schriftlichen Statements zu dem Thema. Meine erste Frage richtet sich an Frau Eickstädt. In der Debatte hören wir immer wieder, vor allem auf europäischer Ebene, dass es sich bei dem Vorschlag der EU-Kommission um so etwas wie einen Virenscanner handeln würde. Virenscanner, so das Argument, scannen unsere Geräte heute schon nach Malware und anderen schädlichen Programmen. Ist denn ein Virenscanner mit dem Scannen nach CSAM vergleichbar?

SVe **Elina Eickstädt:** Ich hatte es eben schon kurz erwähnt: Nein, natürlich nicht. Der Virenscanner, so wie wir ihn als Nutzer:in verwenden, handelt zum einen in unserem Interesse und zum anderen haben wir die Kontrolle darüber, was mit dem Gefundenen passiert. Das ganz grundsätzlich. Vielleicht, um noch mit einem Argument aufzuräumen: Was wir immer häufiger in der Debatte hören – Link-Vorschauen sind nicht das gleiche wie Client Side Scanning. Die Daten, um solch eine Link-Vorschau zu laden, sind schon in dem Link eingebettet. Dafür muss zum Beispiel Signal nicht unsere Kommunikation scannen. Signal macht durch einen Proxy sogar sehr viel, um ein anonymisiertes Laden der Daten zu ermöglichen.

Abg. **Anna Kassautzki** (SPD): Vielen herzlichen Dank. Meine zweite Frage richtet sich an Herrn Türk. Welche grundrechtskonformen Maßnahmen erachten Sie aus Sicht des Kinderschutzbundes für besonders wirkungsvoll? Wo kann und sollte die Politik ihre Aufmerksamkeit hinlenken für einen effektiven Kinderschutz?

SV **Joachim Türk:** In erster Linie müssen wir mit Experten wie in dieser Runde zusammenarbeiten und solche Maßnahmen entwickeln. Wir haben als Corpus Delicti für die Ermittler, für die Strafverfolger lediglich die Dateien, und die müssen wir weiter scannen, wo dies im öffentlichen Internet möglich ist. Sonst werden die Ermittler blind. Das kann nicht in unserem Sinne sein und wir halten das auch für grundrechtskonform.

Nachgeschaut wird dann, wenn ein Treffer kommt. Wir haben sie eben gehört – bei gehashtem alten Material ist die Trefferquote nahe 100 Prozent, und Ermittler sagen, dass in der Nähe von altem Material in der Regel auch neues Material zu finden ist, und damit kommen wir zusammen. Wir würden gerne die Plattformanbieter stärker verpflichten. Die Chatkontrolle hat diesen etwas paranoiden Ansatz, dass die Leute nicht bestraft werden, die den Fehler machen, nämlich die Serviceprovider, sondern die Kunden der Serviceprovider, indem man ihnen ein Grundrecht entzieht. Das ist nicht verständlich. Wir wollen, dass die Plattformbetreiber – was die Risikoabschätzung und vorbeugende Maßnahmen, aber auch leicht erreichbare Hilfemöglichkeiten für Kinder anbelangt – auf einem hohen Niveau finanzieren.

Abg. **Anna Kassautzki** (SPD): Vielen herzlichen Dank. Meine dritte Frage richtet sich an Professor Kelber. Mich würde aus Ihrer Perspektive interessieren, welche datenschutzrechtlichen Implikationen dieser Vorschlag hätte und ob man das damit vergleichen kann, was Strafverfolgungsbehörden heute schon offline machen dürfen. Können Sie insbesondere auf die Unterschiede zwischen risikobezogenen und anlassbezogenen Ermittlungen eingehen?

**Prof. Ulrich Kelber** (BfDI): Herzlichen Dank für die Frage. Ich glaube, es ist nicht vergleichbar mit dem, was heute schon im Offlinebereich stattfindet. Ganz im Gegenteil. Man würde sich übrigens wünschen, dass manche der Technologien, über die wir uns unterhalten, einmal offline oder bei einmal gefundenem Material, auch zur Unterstützung der Arbeit, angewendet werden, um zum Beispiel die Arbeit zu klassifizieren, zu sieben, auszuwählen und zu konzentrieren. Die Datenschutz- und grundrechtlichen Auswirkungen der verschiedenen Punkte, die vorhin in den Eingangsstatements angesprochen wurden, sind umfangreich. Sie sind weit außerhalb jeglicher Maßstäblichkeit, auch jenseits der Verhältnismäßigkeit und der Effizienz. Es wurde nicht geprüft, wo mildere Mittel zur Verfügung stehen. Es werden mindestens immer dann, wenn es beispielsweise eine Aufdeckungsverpflichtung oder Ähnliches gibt, sämtliche Daten, Kommunikations- und Bestandsdaten sämtlicher Nutzerinnen und Nutzer eines Dienstes durchleuchtet. Das Gleiche gilt für die Kommunikation – übrigens nicht nur von Textnachrichten, sondern auch von Audionachrichten, die grundrechtlich noch einmal besonders geschützt sind. Es zieht sich durch die verschiedenen Bereiche durch, dass die Verhältnismäßigkeit der Maßnahmen nicht getroffen wird und – wie Herr Türk vom Deutschen Kinderschutzbund zurecht gesagt hat – natürlich auch in Grundrechte eingegriffen wird, gerade von Kindern und Jugendlichen, bei denen besondere Gefahren vorliegen, und dass es bis hin zur Nicht-Möglichkeit der Teilnahme an Kommunikation geht. So, wie es auch um die besondere Aufdeckung von Kommunikationsinhalten und damit zusammenhängend auch mit „Chilling Effects“-Gefahren in der Ausübung von Freiheitsrechten geht. Es ist zu beobachten, dass in dem Entwurf gesagt wird, dass sehr wenig Aufsicht über einmal gewählte Technologien existiert. Wenn sie einmal eingeführt werden, sind die Datenschutzaufsichtsbehörden draußen. Da haben wir selbst bei der Aufsicht über die Nachrichtendienste mehr Kompetenzen.

Die **Vorsitzende:** Vielen Dank. Für die CDU/CSU-Fraktion Catarina dos Santos-Wintz.

Abg. **Catarina dos Santos-Wintz** (CDU/CSU): Auch von mir noch einmal ganz herzlichen

Dank für die schriftlichen und die mündlichen Stellungnahmen. Ich möchte am Anfang auch betonen, dass wir uns heute mit einem Thema beschäftigen, was sehr ernst ist und was gut abgewogen werden sollte. Ich glaube, das ist hier im Raum auch allen klar. Aber manchmal geht mir das in der öffentlichen Diskussion flöten. Für mich gehört zum Beispiel die Frage dazu, wie unsere Strafverfolgungsbehörden gut ermitteln können und wie man Menschen dingfest machen kann, die sich nicht an die Regeln halten. Deswegen würde ich gerne Herrn Hartmann am Anfang fragen. Sie haben in Ihrer Stellungnahme festgehalten, dass die Ende-zu-Ende-Verschlüsselung von Täterkommunikationen in dem betrachteten Feld des Kindesmissbrauchs nur in einer deutlich untergeordneten Zahl von Fällen ein durchgreifendes Ermittlungshemmnis sei. Könnten Sie das bitte noch einmal erläutern?

SV **Markus Hartmann:** Das kann ich gerne tun. Es ist eine rein empirische Feststellung, dass wir in einer Vielzahl der Ermittlungsverfahren gar nicht mit der Fragestellung, Ende-zu-Ende-Verschlüsselung aufbrechen zu müssen, um Erkenntnisse zu erlangen, konfrontiert sind, sondern dass eine überwiegende Zahl von Tätern unverschlüsselt kommuniziert. Woran das liegt – da kann man viele Mutmaßungen anstellen: technische Kompetenz oder ähnliches. Ich will noch betonen: Es gibt eine ganze Reihe von Ermittlungsmaßnahmen, die wir einsetzen und anwenden, um auch in Fällen, wo verschlüsselte Nachrichten vorliegen, sachgerecht vorgehen zu können. Einfaches Beispiel: A und B kommunizieren Ende-zu-Ende verschlüsselt. Es reicht uns, wenn wir A oder B auf irgendeine andere Weise identifizieren und die Erkenntnisse bei ihm oder ihr vor Ort finden, um ein Netzwerk aufzuklären. Insofern wird das Thema Ende-zu-Ende-Verschlüsselung ein wenig überhöht in der Betrachtung.

Abg. **Catarina dos Santos-Wintz** (CDU/CSU): Vielen Dank, dann würde ich meine zweite Frage gerne an Professor Steinebach stellen. Sie haben in Ihrer Stellungnahme geschrieben, dass die Datengrundlage im Bereich des Groomings in vielen Fällen zu gering ist, um überhaupt effektive Ergebnisse zu erzielen. Sie haben in Ihrem Eingangsstatement noch einmal darüber gesprochen, wie schwierig das ist. Herr Türk vom Kinderschutzbund hat als technische Option zum Beispiel über Pattern-Analyse gesprochen. Könnten Sie eine kurze Stellungnahme dazu abgeben, wie Sie das bewerten? Geht es nur darum, beispielsweise strukturierte Daten zu anonymisieren oder gibt es noch weitere Möglichkeiten, die Ihnen einfallen? Könnten Sie dazu etwas sagen? Danke.

SV **Prof. Dr. Martin Steinebach:** Die Pattern-Analyse würde ich so verstehen, dass man entweder mit maschinellem Lernen oder mit Regeln – das sind die beiden Ansätze, die man heutzutage kennt – versucht, typische Grooming-Muster und Vorgehensweisen abzubilden und dann wiederzuerkennen. Das kann man entweder dadurch machen, dass man typische Anmachsprüche, typische Forderungen nach Nacktfotos oder Ähnliches fest codiert. Oder man kann dem System viele Beispiele zeigen und hoffen, dass das System die Muster, stilistische Eigenschaften und so weiter in der Kommunikation erkennt. Die von Ihnen erwähnten anonymisierten Daten: Das ist die Grundlage dafür, dass wir es mit maschinellem Lernen überhaupt vernünftig hinbekommen können. Die Forschung ist im Cybergrooming deshalb noch nicht so weit, weil es eine sehr geringe Datengrundlage gibt. Diese Datengrundlage ist deshalb so gering, weil es natürlich hochsensibles Material ist, das ganz viele Leute betrifft. Die Entwicklung zur

Anonymisierung von solchen unstrukturierten Textdaten steht wirklich noch ganz am Anfang, und da muss noch viel gemacht werden, um überhaupt diesen ersten Schritt zu erreichen, dass wir hier vernünftig forschen und entwickeln können.

Abg. **Catarina dos Santos-Wintz** (CDU/CSU): Vielen Dank, dann würde ich noch einmal zurückkommen zu Herrn Hartmann. Die Rolle des EU-Zentrums ist laut den Stellungnahmen der verschiedenen Sachverständigen durchaus strittig und nicht ganz so einig. Sie empfehlen in Ihrer Stellungnahme, dass dem EU-Zentrum allein oder zum Beispiel in der Zusammenarbeit mit Europol ein konkreter Auftrag der Koordinierung der Strafverfolgung zugewiesen wird. Sehen Sie beispielsweise je nachdem, wie eine mögliche Kompetenz zugeordnet wird, auch eine Konkurrenz zu bestehenden nationalen Beschwerdestellen, wie zum Beispiel die von „eco“? Wenn ja, was könnte man dagegen tun und wie wäre Ihrer Meinung nach eine gute Ausgestaltung?

SV **Markus Hartmann:** Aus meiner Sicht ist es wichtig, dass das EU-Zentrum einen zusätzlichen Mehrwert zu den schon bestehenden Infrastrukturen liefert. Entscheidend ist aus Sicht der Strafverfolgungsbehörden, dass es Koordinierungsfunktionen übernehmen kann, etwa sicherzustellen, dass europaweit Ermittlungen gegen bestimmte Plattformen, die entsprechendes Material oder Taten fördern, koordiniert werden und die Ressourcen gebündelt werden, die zur Verfügung stehen. Was nicht passieren darf – und da ist der Vorschlag nach meinem Verständnis noch sehr unkonkret, was die konkrete Geschäftsverteilung dieses EU-Zentrums angehen soll – dass bekannte und bewährte Strukturen, die von Ihnen angesprochene Meldestelle „eco“ ist ein verlässlicher Partner, mit dem wir Strafverfolgungsbehörden effektiv zusammenarbeiten, aufgebrochen und ersetzt werden. Wir brauchen nicht den Ersatz erfolgreicher, bestehender Dinge, sondern wir brauchen zusätzliche Mehrwerte und eine europäische Dimension des Ganzen.

Die **Vorsitzende:** Vielen Dank. Für BÜNDNIS 90/DIE GRÜNEN Tobias Bacherle.

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Ich würde mit meinen Fragen an Ella Jakubowska beginnen. Die deutsche Debatte hat auch heute wieder gezeigt, dass sich deutlich positioniert wird, wie auch diese Anhörung zeigt. Wie bewerten Sie die Positionen des Europäischen Parlaments und anderer nationaler Parlamente und Regierungen zum Vorschlag?

SVe **Ella Jakubowska:** Innerhalb des Europäischen Parlaments zeigt sich, dass immer noch versucht wird, herauszuarbeiten, was eigentlich ihre Position ist. Uns liegt jedoch ein vielversprechender Bericht des MdEP Alex Saliba vor, der die Leitung im Namen des Europäischen Parlaments vom Ausschuss für Binnenmarkt innehat, in dem er wesentliche Teile der gefährlichsten Abschnitte dieses Gesetzes gestrichen hat. Um diese Verordnung dem Digital Services Act besser anzupassen oder, besser gesagt, die Verordnung daran zu hindern, den Digital Services Act auszuhöhlen, wofür unserer Meinung nach ein hohes Risiko besteht, hat Herr Saliba empfohlen, einen Großteil des Vorschlags außer Kraft zu setzen, um Grundrechte besser zu schützen.

Wir beobachten eine wachsende Opposition innerhalb des Europäischen Parlaments, zum Beispiel aufgrund des Risikos der Massenüberwachung und den Eingriffen in das Recht junger Menschen auf Privatsphäre und Datenschutz. Meiner Wahrnehmung nach lässt sich auch zunehmend beobachten, dass nationale Parlamente ihre

Kontrollfunktion bei diesem Thema wirklich ernst nehmen. So läuft beispielsweise in Irland gerade ein Kontrollverfahren zu diesem Gesetz. Dabei hat man sich offen gegenüber allen Bedenken unsererseits gezeigt. In Österreich beobachten wir die bisher stärkste Bewegung eines nationalen Parlaments, wo das nationale Parlament eine verbindliche Abstimmung durchgeführt hat, dass ihre Regierung daran hindert, diesem Vorschlag auf EU-Ebene zuzustimmen, wenn es Grundrechte unverhältnismäßig unterwandert, wie es derzeit der Fall ist. Mehrere andere nationale Parlamente haben einen ähnlichen Weg eingeschlagen und ihre Kontrollbefugnisse genutzt.

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Eine schnelle Ja-Nein-Frage: Das hört sich so an, als ob Deutschland mit seinem kritischen Standpunkt nicht allein ist. Würde eine deutliche Position von Deutschland helfen, weitere Unterstützung zur Veränderung von kritischen Teilen des Vorschlags zu bekommen?

SVe **Ella Jakubowska:** Zweifelsohne ja.

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. An dem Vorschlag ist nicht nur das Client Side Scanning problematisch. Welche Konsequenzen hätte eine verpflichtende Altersverifizierung auf die Anonymität im Internet? Und welche Konsequenzen hätte das für die Nutzer, die auf eine anonyme Nutzung angewiesen sind?

SVe **Ella Jakubowska:** Uns ist kein Altersverifizierungsverfahren bekannt, das die Grundrechte beachtet. Wie Sie bereits gesagt haben, ist die Gefahr, die Anonymität im Internet zu beseitigen, immens. Und wir wissen, dass Anonymität im Internet für die Demokratie unerlässlich ist. Sogar so sehr, dass der frühere Sonderberichterstatter der Vereinten Nationen für Meinungsfreiheit, David Kaye, darüber sprach, dass Anonymität und Verschlüsselung die beiden wichtigsten Werkzeuge für Sicherheit im digitalen Zeitalter sind.

Das gilt nicht nur für Nutzer im Allgemeinen, sondern insbesondere auch für die jungen Menschen selbst, wenn man bedenkt, wie schädlich Altersverifizierungsmethoden sein können, da sie oft Methoden wie die systemische Verarbeitung der sensibelsten Daten junger Menschen beinhalten. Manchmal werden dabei KI-Systeme eingesetzt, die nach unseren Kenntnissen stark diskriminierend sein können. Tatsächlich besagt eine Studie aus dem vergangenen Jahr, dass maschinelle Altersbestimmungen sogar noch verzerrter und ungenauer als Altersbestimmungen durch Menschen sind. Es darf auch nicht außer Acht gelassen werden, wer durch diese Verfahren ausgeschlossen wird, denn davon sind die bereits Vulnerabelsten unserer Gesellschaft betroffen: Menschen ohne gültige Papiere, die keinen Zugang zu Ausweisdokumenten haben, Roma- und Sintigemeinschaften, die bereits einen hohen Grad an struktureller Diskriminierung erfahren. Und wie wir bereits von einigen der anderen Sprecher gehört haben, wollen wir diese Menschen nicht von der Möglichkeit ausschließen, über das Internet zu kommunizieren.

Daher glaube ich, dass eine verpflichtende Altersverifizierung gefährlich verfrüht ist und deren Implementierung einen schweren Schaden für uns alle anrichtet, die wir auf Anonymität im Internet bauen, unabhängig davon, ob es sich um Journalisten, Whistleblower oder Personen handelt, die sich bei der Korruptionsbekämpfung engagieren oder um Personen, die auf den Zugang zu unseren demokratischen Rechten, deren Ausübung und auf Privatsphäre angewiesen sind.

Die **Vorsitzende:** Vielen Dank. Dann für die FDP Maximilian Mordhorst.

Abg. **Maximilian Mordhorst** (FDP): Vielen Dank, Frau Vorsitzende. Meine Fragen gehen an Frau Widlok. Vielleicht zuallererst einmal zur grundrechtlichen Perspektive – offensichtlich sind sich die Sachverständigen bei den allermeisten Fragen sehr einig. Wenn man das Thema Belastung der Polizei und andere Dinge betrachtet: Hier haben einige angesprochen, dass es eine Fehlerquote gibt – potenziell – man weiß noch nicht genau, wie die aussehen würde. Wenn Sie alle grundrechtlichen Bedenken am Anfang einmal außen vor lassen – es gibt auch andere Perspektiven, als hier in diesem Ausschuss. Glauben Sie, dass der vorliegende Entwurf für die Polizistinnen und Polizisten oder andere Behörden, die verfolgen, eine wirkliche Entlastung darstellen könnte, und könnten Sie noch einmal etwas zu den Fehlerquoten sagen?

SVe **Teresa Widlok:** Vielen Dank, sehr gerne. Natürlich sind die Fehlerquoten ein Puzzlestein im Rahmen einer Verhältnismäßigkeitsabwägung. Deswegen können wir grundrechtlich nicht ganz davon absehen – oder von der Abwägung im grundrechtlichen Rahmen. Die Fehlerquoten sind ein interessantes Thema; der Entwurf als solcher sagt selbst etwas dazu, von was für Fehlerquoten er ausgeht. In der Begründung hebt er heraus, dass am Markt verfügbare Erkennungstechnologien bereits ein "hohes Maß an Genauigkeit erreicht“ hätten, so zitiere ich das jetzt einmal. Dann wird eine kleine Fußnote daran gesetzt, und man kann weiter nach hinten blättern und sieht: Okay, was meint man mit einem „hohen Maß an Genauigkeit“? Das stimmt etwa mit dem überein, was Prof. Steinebach hier gerade schon gesagt hat. Da wird zitiert, dass Microsoft angibt, für diese Grooming-Software, die man eingesetzt hat, oder Software zur Erkennung von Grooming, bereits eine Erkennungsrate von 88 Prozent zu haben, sodass man eben offensichtlich eine Fehlerrate von 12 Prozent feststellt bei diesem Industriestandard für den Bereich des Groomings. Das heißt – um an das anzuknüpfen, was Herr Hartmann schon gesagt hat: Die Überschwemmung mit Daten der Sicherheitsbehörden, die das alles irgendwie erhalten und sichten müssen, ist absehbar.

Abg. **Maximilian Mordhorst** (FDP): Vielen Dank. Noch einmal zum Recht auf Verschlüsselung. Sie haben sehr eindringlich noch einmal darauf hingewiesen, wie wichtig das ist. Gibt es aus Ihrer Sicht irgendeine Möglichkeit, den vorliegenden Entwurf vereinbar zu machen mit dem Recht auf Verschlüsselung oder halten Sie ihn für unvereinbar mit dem Recht auf Verschlüsselung?

SVe **Teresa Widlok:** Kurze Antwort: Ich glaube, er ist damit unvereinbar. Allerdings ist es so, dass ein Recht auf Verschlüsselung, je nachdem woraus man es herleitet, natürlich grundrechtliche Positionen zusammenfasst, und das sind nicht abwägungsfreie Räume, sondern da kann auch ein Eingriff vielleicht gerechtfertigt sein in ein solches Recht. Ich vermisse aber ein ähnlich starkes Bekenntnis in diesem Verordnungsentwurf, wie wir es in der Interimsverordnung noch gesehen haben. Da ist ein Erwägungsgrund, der ganz deutlich darauf hinweist, dass alle Regelungen in dem Vorschlag nicht so zu verstehen sind, dass Ende-zu-Ende-Verschlüsselung verboten oder abgeschwächt werden soll. Eine solche Provision finden wir weder in den Erwägungsgründen, noch in den Ausführungen in den Artikeln. Da könnte man deutlich stärker noch einmal hervorheben, dass das nicht das Ziel des Verordnungsentwurfes ist.

Abg. **Maximilian Mordhorst** (FDP): Glauben Sie, dass es bewusste Gründe für diese Exegese des Ganzen gibt? Oder halten Sie das eher für einen misslichen Zufall?

SVe **Teresa Widlok:** Ich möchte keine Verschwörungstheorien in den Raum stellen. Aber wenn man sich international umschaut, die Cyber Security Convention auf UN-Ebene ist zum Beispiel auch so ein Projekt, was aktuell angeschoben wird, und überall auf allen Ebenen weltweit ist zu erkennen, dass immer mehr die Pönalisierung von Straftaten im Bereich der Inhalte vorangetrieben werden soll. Um das zu tun, muss man natürlich Inhalte kennen, sodass insgesamt zu erkennen ist, dass dieses mächtige Tool verschlüsselter Kommunikation, womit man sich auch selbst sehr effektiv schützen kann, aktuell überall unter Druck steht. Von daher halte ich es nicht für einen absoluten Zufall, dass das ein Kollateralschaden ist, der von diesem Entwurf ausgeht.

Abg. **Maximilian Mordhorst** (FDP): Vielleicht noch ganz kurz: Es wird immer gesagt, man muss analoge Maßstäbe anlegen können. Gibt es aus Ihrer Sicht in der analogen Welt etwas Vergleichbares zu dem, was in diesem Entwurf steht, beispielsweise das Postgeheimnis oder andere Dinge?

SVe **Teresa Widlok:** Sie erwähnen es gerade: Das Recht auf vertrauliche Kommunikation ist sowohl digital als auch analog anzuwenden. Dieser schöne Satz, der einem immer entgegengehalten wird, ist hier zu 100 Prozent anwendbar. Fairerweise muss meiner Ansicht nach das, was im Analogen gilt, auch im Digitalen gelten. Denn das analoge Briefgeheimnis muss auch ein digitales Briefgeheimnis sein können.

Die **Vorsitzende:** Danke, und dann kommen wir zur AfD, Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine erste Frage geht an Herrn Hartmann. Wie schätzen Sie die Wahrscheinlichkeit ein, dass die möglicherweise kommende anlasslose Chatkontrolle diejenigen, auf die sie eigentlich zielt, nämlich die Täter, ins schwerer zugängliche und zu kontrollierende Darknet treibt, während gleichzeitig Millionen unbescholtene Bürger des Grundrechts einer unverletzlichen, privaten Kommunikation beraubt werden?

SV **Markus Hartmann:** Es wird sicher Verdrängungseffekte geben. Die haben wir in allen Bereichen gesehen. Gesetzliche Verbote bestimmter Technologien führen zu Ausweichstrategien. Wir beobachten allerdings, dass es eine große Gruppe innerhalb der Täterklientel gibt, die zu solchen Ausweichstrategien nicht in der Lage ist, mangels technischer Kompetenz. Insofern ist es schwierig einzuschätzen, wie hoch diese Verdrängungseffekte ausfallen. Fakt ist – da gebe ich Ihnen mit der Frage insofern recht – , dass wir relativ einfache Technologien am Markt haben, die technisch kundige Täter einsetzen können, und damit in der Lage sind, weiter verschlüsselt zu kommunizieren, während die große Masse, die sich auf gängige Technologien verlässt, die am Markt sind, eine stärkere Einschränkung erfahren.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine nächste Frage geht an Frau Eickstädt. Der Text Generator ChatGPT, Ende November 2022 der Öffentlichkeit vorgestellt, demonstriert auf beeindruckende Weise die Kraft auf Sprache ausgerichteter KI-Lösungen. Halten Sie es für möglich, dass eine entsprechend trainierte Software dieser Art als Supervisor privater digitaler Kommunikation im Stande wäre, Annäherungsversuche Erwachsener an Kinder und Jugendliche in Chats zu erkennen?

SVe **Elina Eickstädt:** Ich würde die Frage an

Professor Dr. Steinebach weitergeben, weil ich annehme, dass er sich wesentlich besser mit einer Datenlage und der Trendentwicklung in diesem Bereich auskennt.

Abg. **Steffen Janich** (AfD): Ich bitte darum.

SV **Prof. Dr. Martin Steinebach:** Gerne, gut. ChatGPT ist eine andere Technologie als eine Erkennungstechnologie. Es ist eine Synthesestrategie. Ich glaube, dass wir auch bei ChatGPT immer noch sehr hohe Fehlerraten haben. Das darf man nicht vergessen. Es macht beeindruckende Dinge, aber im Endeffekt würde ich sagen: Jede zehnte Frage wird mit Sicherheit falsch beantwortet, und ich befürchte, man kommt aus dem Problem auch mit der Technologie nicht heraus.

Abg. **Steffen Janich** (AfD): Vielen Dank. Herr Steinebach, die nächste Frage wäre noch: In einer Pressemitteilung zur geplanten Verordnung schreibt die EU-Kommission, im Jahr 2020 seien fast 95 Prozent der Meldungen zu sexuellem Kindesmissbrauch von genau einem Unternehmen gekommen. Sie wissen, dass die ganze Online-Branche betroffen ist. Haben Sie Kenntnis darüber, um welches Unternehmen und um welche seiner Dienste es sich dabei handelt?

SV **Markus Hartmann:** Ich glaube, das war die Facebook-Gruppe. Die sind darin ziemlich stark. Die machen das auch öffentlich. Es gibt genug Dokumente, die es recht genau aufzeigen – und das muss man hier auch der Vollständigkeit halber sagen: Da geht es aber auch um das Wiedererkennen bekannter Inhalte. Die sagen, ca. 75-80 Prozent ist Wiedererkennen, und der Rest sind Detektoren, auf die sie reagieren und diese händisch sperren.

Abg. **Steffen Janich** (AfD): Vielen Dank, meine nächste Frage geht wieder an Herrn Hartmann. Die Bundesregierung hat sich – namentlich die Ressorts des Innern, der Justiz und des Digitalen – sehr kritisch gegenüber dem vorliegenden Entwurf der EU-Verordnung geäußert. Halten Sie die Verordnung in der jetzigen Fassung insgesamt für zustimmungsfähig beziehungsweise zustimmungswürdig? Überwiegen Ihrer Auffassung nach die begrüßenswerten Anteile die bedenklichen Meldungen?

SV **Markus Hartmann:** Wenn ich aus Sicht der Strafverfolgung einen Wunsch äußern könnte, dann wäre es, das man über den Entwurf nicht im Ganzen zu befinden hätte, sondern einzelne Komponenten auseinander nimmt. Ich kann mit dem EU-Zentrum einiges anfangen. Ich kann auch in Übereinstimmung mit dem, was Herr Türk gesagt hatte, mit der Frage der Wiedererkennung – hashbasiert bei serverseitigem Scannen – einiges anfangen und halte das für eine praktikable Technologie. Sollte der Entwurf in Gänze zur Abstimmung stehen, ist das Paket insgesamt meiner Bewertung nach nicht verhältnismäßig und aus Praktikabilitätsgründen für die Strafverfolgung nicht zuträglich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Ich verzichte auf weitere Fragen.

Die **Vorsitzende:** Vielen Dank und für DIE LINKE. Anke Domscheit-Berg.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Herzlichen Dank an alle Sachverständigen für Ihre Beiträge. Meine Frage geht an Felix Reda von der Gesellschaft für Freiheitsrechte. Die Bundesregierung hatte bis jetzt gesagt, dass sie grundsätzlich die EU-Verordnung unterstützt, weil sie sonst gar keinen Einfluss mehr nehmen kann auf die Ausgestaltung. Sie waren selber einmal Berichterstatter in der EU. Können Sie das auf Basis Ihrer eigenen Erfahrung so bestätigen, dass eine

grundsätzliche Ablehnung, wie sie zum Beispiel Österreich gemacht hat, weniger Wirkung hätte?

SV **Felix Reda:** Ich glaube, dass eigentlich eher das Gegenteil richtig ist. Wenn man nicht von Anfang an in den Diskussionen deutlich macht, dass die Ablehnung des Entwurfs in seiner jetzigen Form bevorsteht, dann gibt es keinen großen Anreiz für die EU-Kommission, erhebliche Zugeständnisse zu machen. Die meisten Entwürfe werden, zumindest in ähnlicher Form, am Ende verabschiedet. Es ist selten, dass neue Elemente, die im Kommissionsentwurf nicht vorhanden sind, hinzukommen, und es wird auch selten ein Aspekt eines Vorschlags ersatzlos gestrichen. Das heißt, das Schlechteste, was man machen kann, um die Verhandlungen zu beeinflussen, ist, sich mit der Positionierung sehr lange Zeit zu lassen, weil dann die Diskussionen und die Verhandlungen vorangeschritten sind. Das Beste, was der Bundestag an dieser Stelle machen könnte, wäre eine Artikel 23-Stellungnahme. Das würde Deutschlands Verhandlungsposition eher stärken, denn dadurch würde eine Sperrminorität im Rat in greifbare Nähe rücken. Wenn die beiden anderen Länder, die solche Positionen bereits verabschiedet haben oder kurz davor stehen, das mit Österreich und den Niederlanden tun und Deutschland hinzukommt, dann würde eigentlich nur noch ein großer oder mittelgroßer Staat für eine Sperrminorität fehlen. Und das kann die EU-Kommission nicht einfach ignorieren.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Vielen Dank. Ich hätte dann noch einige Fragen, die sich rund um das Thema Altersverifikation drehen. Die soll ja für alles Mögliche mit dieser Verordnung vorgeschrieben werden. Diese Dienste werden, das haben wir gehört, aber auch von Minderjährigen benutzt. Also unabhängig davon, wie blöd man einen Ausweisnachweis findet: Manche haben noch gar keinen Ausweis. Wie soll denn da überhaupt eine Altersverifikation für Minderjährige erfolgen?

SV **Felix Reda:** Das würde im Grunde genommen nur gehen, wenn man sagt, man verifiziert alle Erwachsenen und behandelt alle, die sich nicht als Erwachsene ausweisen können, als Kinder. Das Problem bei dem Entwurf ist, dass er aber eigentlich beides verlangt. Es müssen alle Erwachsenen erkannt werden, um zu verhindern, dass die sich zum Zwecke des Groomings Kindern nähern können. Es müssen aber auch alle Minderjährigen erkannt werden, weil die App-Stores diese von dem Download bestimmter Apps aussperren sollen. Das heißt, im Grunde genommen kann das nur funktionieren, wenn jede einzelne Person altersverifiziert wird. Da ist ganz klar das Problem: Nicht nur Kinder, die teilweise keine Identifikationsdokumente haben, sondern auch Menschen ohne Papiere würde das betreffen. Die alternativen Verfahren, die es gibt, sind nicht nur sehr invasiv – wie zum Beispiel biometrische Erfassung vom Gesicht und so weiter –, sondern sie sind auch sehr fehleranfällig. Da wird es dazu kommen, dass Leute falsch eingestuft werden.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Herzlichen Dank. In Ihrem Eingangsstatement haben Sie kurz in einem Nebensatz erwähnt, dass die Auswirkungen auch auf das Open Source-Ökosystem durch die Altersverifikation schwierig werden. Was sind denn das genau für Auswirkungen? Was ist da das Problem?

SV **Felix Reda:** Da muss man unterscheiden: Einerseits die App selber, da hat man zum Beispiel eine App wie "Signal", die dadurch besonders sicher ist, dass der Source Code für jeden nachprüfbar ist. Wenn man dort eine Altersverifikation implementieren würde,

dann könnte jeder, der sich den Source Code anschaut, nachvollziehen, wie der funktioniert, könnte den entsprechend verändern und die Altersverifikation herausnehmen. Insofern nicht besonders effektiv, aber es wäre auch für die Open Source-Projekte nicht zu leisten, weil die oft gar nicht die zentralisierte Stelle haben, die dafür sorgen könnte, diese Altersverifikation durchzuführen. Der andere Aspekt sind die App-Stores. Um ein modernes Smartphone oder Tablet zu benutzen, braucht man einen App Store. Die EU hat in der Vergangenheit viel gemacht, um die dominante Position von Google und Apple auf diesem App Store-Markt zu dämpfen, durch den Digital Markets Act, damit alternative Open Source-basierte App-Stores wie F-Droid eine Chance haben. Die können aber eine solche Altersverifikation nicht anbieten. Das sind dezentrale Strukturen, die im Grunde genommen nur sicherstellen, dass die Apps, die dort angeboten werden, Open Source sind. Die können nicht eine Altersverifikation implementieren, und dementsprechend würde man dadurch im Grunde genommen sagen: Eine Nutzung von alternativen App Stores zu Apple und Google ist nicht möglich.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Vielen Dank.

Die **Vorsitzende:** Vielen Dank, wir kommen in die zweite Runde und haben weiterhin fünf Minuten pro Fraktion. Ich gebe das Wort an Carmen Wegge für die SPD-Fraktion, die heute zu Gast als Mitglied des Innenausschusses ist.

Abg. **Carmen Wegge** (SPD): Vielen Dank, Frau Vorsitzende. Meine erste Frage geht an Frau Eickstädt. Es wurde schon viel gefragt und gesagt zu der Altersverifikation. Sie haben es in Ihrem Statement auch angedeutet. Ich würde trotzdem noch einmal kurz und knapp fragen wollen: Gibt es aktuell technische Möglichkeiten der Altersverifikation, die gleichzeitig eine anonyme und pseudonyme Nutzung des Netzes gewährleisten würden?

SVe **Elina Eickstädt:** Nein.

Abg. **Carmen Wegge** (SPD): Vielen Dank für die Antwort. Nun habe ich etwas mehr Zeit, das ist gut. Meine nächste Frage geht an Herrn Schabhüser vom BSI. Es wird bei dem Vorschlag immer von einer technologieoffenen Lösung gesprochen und es stimmt natürlich auch: Artikel 7 in Verbindung mit Artikel 10 des Verordnungsvorschlags legen keine explizite Technologie fest. Nichtsdestotrotz: Sehen Sie eine Möglichkeit, die Anforderungen der Verordnung zu wahren, ohne die Verschlüsselung aufzuheben und Schwachstellen auf dem Gerät zu schaffen? Gibt es das überhaupt trotz technologieoffener Lösung? Wenn nicht: Welche Sicherheitsvorkehrungen bräuchte der Vorschlag, um beides sicherzustellen?

**Dr. Gerhard Schabhüser** (BSI): Man muss differenzieren zwischen unverschlüsselter und verschlüsselter Kommunikation. Bei verschlüsselter Kommunikation sehe ich ohne das Thema Aufbrechen der Privatheit keine Methoden. Bei unverschlüsselter Kommunikation ist natürlich ein ganzer Teil an Technologien durchsetzbar – die sind heute angesprochen worden, wie Hashing gegen bekanntes Material. Technologieneutral finde ich immer gut. Aber es gibt ein paar Grundsätze, die funktionieren nicht. Das Thema ist: Wenn man Verschlüsselung richtig implementiert und keine Fehler macht, dann ist sie nicht aufzubrechen. Also bleibt dann nur, links oder rechts vorher etwas zu tun. Wir hatten eben schon in den Stellungnahmen gehört, dass das schwierig ist.

Abg. **Carmen Wegge** (SPD): Vielen Dank.

Dann geht meine nächste Frage an Herrn Türk vom Deutschen Kinderschutzbund. Sie hatten ja schon anklingen lassen, dass der Vorschlag auch die Bedürfnisse von Opfern sexualisierter Gewalt möglicherweise nicht ausreichend berücksichtigt. Deswegen würde ich Sie gerne fragen, inwieweit zum Beispiel verschlüsselte und vertrauliche Kommunikation auch für Opfer von sexualisierter Gewalt wichtig ist – zum Beispiel, wenn sie sich an eine Beratungsstelle wenden. Wie könnte das durch den Vorschlag bedroht werden?

SV **Joachim Türk:** Vielen Dank. Wir könnten das Thema aufbohren. Es gilt für alle, die einen speziellen Schutz brauchen in ihrer Kommunikation. Es geht überhaupt nicht darum, dass man eine Beratungsstelle aufsucht, sondern dass man mit vertrauten Personen über bestimmte Dinge vertraulich reden kann. Der Vorschlag der EU-Kommission lässt zu, dass massenhaft mitgetrackt wird und dass bestimmte Schlüsselbegriffe dann ausgeleitet werden. Man kann sich vorstellen, dass vielfach bei Minderheiten, die sich nur untereinander austauschen, solche Begriffe auftauchen und dann die entsprechende Kommunikation ausgeleitet wird. Das ist extrem schädlich.

Abg. **Carmen Wegge** (SPD): Vielen lieben Dank. Meine letzte Frage geht an Professor Ulrich Kelber. Wie beurteilen Sie die Rolle der Datenschutzaufsichtsbehörden in diesem Vorschlag der Verordnung? Ist sie stark genug, um das Recht auf informationelle Selbstbestimmung ausreichend zu beachten?

**Prof. Ulrich Kelber** (BfDI): In den vorgeschlagenen Wegen selber sind eigentlich schon Widersprüche zu Grundprinzipien, die sich die Europäische Union mit der Datenschutzgrundverordnung gegeben hat – Datenminimierung, die Frage der Zweckmäßigkeit, der Verhältnismäßigkeit – angelegt. Bei der Frage der Aufsicht über dann eingesetzte Technologien wird eine Einbindung bei der Auswahl der Technologie vorgesehen, danach allerdings keine Beteiligung mehr im laufenden Verfahren. Das widerspricht jeglicher Erfahrung, wo die Probleme auftreten. Das war das, warum ich vorhin diesen einen Satz gesagt habe: Selbst bei den Nachrichtendiensten, also bei der höchsten Geheimhaltungsstufe, haben wir als Datenschutzaufsichtsbehörden im nationalen Recht mehr Möglichkeiten vorgesehen, auch im laufenden Betrieb hinein zu sehen, als was in dem Verordnungsentwurf für diese eingesetzten Technologien dann den Datenschutzbehörden als Mittel zur Verfügung stände.

Die **Vorsitzende:** Vielen Dank. Für die CDU/CSU-Fraktion ist in der zweiten Runde Dr. Reichel dran.

Abg. **Dr. Markus Reichel** (CDU/CSU): Frau Vorsitzende, vielen Dank. Meine erste Frage geht an Herrn Dr. Gerhard Schabhüser. Wäre eine Technik wie das Client Side Scanning auch ein mögliches Einfallstor für böswillige Dritte, um in dieser Form den Zugang zu Endgeräten – also Mobiltelefonen, Laptops und so weiter – zu erhalten?

**Dr. Gerhard Schabhüser** (BSI): In der Tat, wir würden die entsprechende Komplexität der Systeme erhöhen und damit eine zusätzliche Angriffsfläche stellen. Heute kann ich zu den Technologien nicht sagen, wie groß sie ist. Aber zunächst einmal erhöhen wir die Angriffsfläche, aber auch nicht nur zu der Fragestellung Eingriff in das System, sondern ich kann mir noch weitere Eingriffe vorstellen, die die Auswertung selbst noch verändern – also eine noch etwas weiter gehende Angriffsfläche darstellen.

Abg. **Dr. Markus Reichel** (CDU/CSU): Vielen Dank. Eine weitere Frage an Herrn Hartmann. In Ihrer Stellungnahme haben Sie die Frage

einer Folgeregelung für die Vorratsdatenspeicherung angesprochen und sind dort auf das Thema der Zuordnung von IP-Adressen zu Anschlüssen und zu Geräten eingegangen. Könnten Sie uns erläutern, wie dieses Konzept funktionieren sollte, das Sie auch für Ihre konkrete Arbeit benötigen würden?

SV **Markus Hartmann:** Das ist natürlich eine hochkomplexe Frage, die ich nur grob skizzieren kann mit Blick auf die zur Verfügung stehende Zeit. Wichtig ist, dass es Fallgestaltungen gibt, in denen die Zuordnung einer IP-Adresse zu einem Endgerät oder zu einem Anschluss zur Identifikation von Tatverdächtigen wichtig ist. Das gilt gerade für den Bereich, in dem wir – wie bei der Bekämpfung von Kinderpornografiedarstellungen und ähnlichem – auf internetbasierte Spuren angewiesen sind. Mir ist allerdings wichtig zu betonen, dass aus Sicht der Strafverfolgung nicht erforderlich ist, ein umfassendes Konzept einer Vorratsdatenspeicherung, sondern ein zielgenaues, abgestimmtes Modell zu entwickeln, das sowohl die grundrechtlichen wie die Strafverfolgungspositionen berücksichtigt.

Dazu gehören aus meiner Sicht: Dass wir das gesamte System der Abfrage solcher Zuordnungsdaten so modernisieren und durchdigitalisieren, dass wir eine Schnelligkeit erreichen, die im Ergebnis dazu führt, dass wir für die weit überwiegende Zahl Account-gebundener Straftaten sozusagen auf das nächste Login – das ist unter dem Begriff der Login-Falle von NGOs entwickelt und vorgetragen worden – dass wir dieses Konzept umsetzen und im Ergebnis damit live auf Daten zugreifen können. Für den relativ überschaubaren Bereich verbleibender Situationen, die nicht Account-gebunden sind und wo ich nicht auf Live-Daten zugreifen kann, kommen wir mit einer sehr beschränkten Speicherfrist aus. Auch in der Größenordnung der jetzt zur Netzstörungsbeseitigung vorgesehenen Frist von circa einer Woche werden wir einen wesentlichen Prozentsatz der infrage stehenden Fallkonstellation bearbeiten können. Wir müssen aus dem Bereich der ideologischen Gräben in der Vorratsdatenspeicherung aus Sicht der Strafverfolgung raus und ein sachorientiertes Konzept entwickeln.

Abg. **Dr. Markus Reichel** (CDU/CSU): Vielen Dank, sehr aufschlussreich. Eine weitere Frage an Herrn Türk vom Kinderschutzbund. Sie hatten es auch in Ihrem Beitrag genannt: Das umstrittene Thema der Altersverifikation. Ließe sich vielleicht ein etwas anderer Weg finden, der auf der Verantwortung der Eltern für ihre Kinder aufbaut, zum Beispiel über Familien-Accounts, wo dann über die Eltern eine entsprechende Altersfreigabe gesucht wird.

SV **Joachim Türk:** Schönen Dank. Auch wir sehen eine ausweisbezogene Identifikation als rote Linie. Wir glauben aber, dass es durchaus Anreize gibt, im Netz zumindest das Alter mitzuteilen, etwa bei Familien-Accounts, wo Familien ein Benefit haben, wenn Eltern gemeinsam mit ihren Kindern das Alter einrichten. Wenn das Alter dann allein ausgelesen werden kann und automatisch beim Download von Apps ausgelesen wird, halten wir das für sinnvoll. Wir müssen immer von der Position ausgehen, dass wir Kinder schützen wollen. Cyber Grooming ist ein Akt der Gewalt und um diese zu bekämpfen, braucht es Instrumente. Wir wollen aber keine rote Linie überschreiten. Deswegen denke ich, dass solche Dinge geeignet sind, dass man Eltern sagt, es lohnt sich aus verschiedenen Gründen – Kinderschutz aber auch aus finanziellen Gründen – das Alter der Kinder

gemeinsam mit ihnen freiwillig anzugeben. Das wäre schon ein wesentlicher Schritt.

Abg. **Dr. Markus Reichel** (CDU/CSU): Vielen Dank, und eine allerletzte Frage an Prof. Steinebach. Sie haben das Problem der Datengrundlage genannt. Wäre es auch denkbar, dass man über die Nutzung von Künstlicher Intelligenz eine Datengrundlage schafft, die dann später an anderer Stelle zum Training genutzt wird?

Die **Vorsitzende:** Ganz kurz bitte nur.

SV **Prof. Dr. Martin Steinebach:** Wahrscheinlich nicht, denn das Problem ist, dass die Trainingsdaten auch wieder vorhanden sein müssen, um überhaupt der KI beizubringen, für was sie sich interessieren soll.

Die **Vorsitzende:** Vielen Dank. Für BÜNDNIS 90/DIE GRÜNEN noch einmal Tobias Bacherle.

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Meine erste Frage geht noch einmal an Professor Kelber. Sie schreiben in Ihrer Stellungnahme auf Seite 14 zu Frage 7, nach der Altersverifikation, dass es ein Risiko der Überidentifikation bei Online-Diensten und für Softwareanwendungen in Folge der Verordnung geben könnte und, dass es auch eine Gefahr für Whistleblower und Oppositionelle in Drittländern darstellen könnte. Könnten Sie das noch etwas ausführen?

**Prof. Ulrich Kelber** (BfDI): Wir müssen angesichts der Tatsache, dass es keine allgemein gültigen Technologien für diese Aufgabenstellung gibt – und zwar für beide Varianten: Ausschluss von Erwachsenen, die sich als Kinder ausgeben, und von Kindern, die noch nicht volljährig sind – davon ausgehen, dass natürlich Marktmacht zum Einsatz kommen würde an dieser Stelle. Dementsprechend würden die Unternehmen – auch übrigens zum Ausschluss von möglichem Risiko, das sie eingehen müssen, und Rechtsverletzungen, wenn sie anstelle einer Altersverifikation eine Personen-Identifikation vornehmen würden, wo es nicht notwendig ist – natürlich auch ein Interesse daran haben, noch mehr Menschen als heute bei der Nutzung ihrer Dienste zu identifizieren. Das wäre der eine Aspekt. Der zweite Aspekt wäre: Viele Dienste würden natürlich nicht mit einer spezifischen deutschen oder europäischen Variante zur Verfügung gestellt, sondern sie würden weltweit von vornherein so ausgelegt werden, dass auch diese europäischen Dinge möglich sind. Das heißt, alle autoritären Staaten würden ein Surveillance Ready-Produkt hingelegt bekommen, mit dem sie sagen „das setzen so auch die Europäer ein, was ist denn eigentlich falsch?“ Die würden nicht nur nach Grooming oder anderen Dingen suchen, sondern auch nach anderen Inhalten ihre Suche durchführen können.

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Vielen herzlichen Dank. Nun haben Sie auch schon meine nächste Frage mit beantwortet, dass das eine Blaupause sein könnte. Deswegen würde ich weitergehen zu der Frage an Frau Eickstädt. Sie haben gesagt, dass es ein komplexes Problem ist, das mit dem einfachen Holzhammer an technischen Mitteln versucht wird, zu lösen. Welche technischen Hilfsmittel sehen Sie denn, um Kinder und Jugendliche im digitalen Raum besser schützen zu können, ohne deren Persönlichkeitsrechte zu gefährden?

SVe **Elina Eickstädt:** Ich glaube, Herr Türk hat das sehr schön in seiner Stellungnahme formuliert und auch der Digital Services Act sieht sehr viele ähnliche Maßnahmen vor. Wir müssen es sehr niedrigschwellig gestalten, dass Kinder Möglichkeiten haben, sich an Vertrauenspersonen zu wenden, um komische Dinge zu melden. Das ist etwas,

was wir nicht nur mit technischen Mitteln gestalten können, sondern was auch ein Wahrnehmungsaspekt ist. Ich nenne an dieser Stelle immer gerne das Projekt des Familienministeriums: „Schiebe den Gedanken nicht weg." Denn wir müssen Kindern und Jugendlichen klarmachen: Was im echten Leben, in der realen Welt nicht in Ordnung ist, ist auch im Digitalen nicht in Ordnung. Es muss sehr einfach sein, sich Hilfe zu holen oder zu sagen: Hier kommt mir etwas komisch vor. Das kann man natürlich entsprechend technisch begleiten. Ich betone hier das Begleiten.

Abg. **Tobias Bacherle** (BÜNDNIS 90/DIE GRÜNEN): Ich habe eine weitere Frage an Ella Jakubowska, da wir über die Machbarkeit durch Polizisten gesprochen haben, hauptsächlich jedoch durch die deutschen Polizisten. Wie würden Sie das bewerten? Ist die Polizei in Europa dazu in der Lage? Haben sie die Ressourcen, die zahlreichen neuen Fälle zu bearbeiten, die sich infolge eines der vorgeschlagenen Mechanismen in dem Vorschlag ergeben würden?

SVe **Ella Jakubowska:** Leider glaube ich nicht, dass sie dazu in der Lage wäre. In ganz Europa zeigt sich, dass Strafverfolgungsbehörden systematisch unterbesetzt sind und ihnen nicht nur das Geld und das Personal fehlen, um die Kindesmissbrauchsfälle zu bearbeiten, denen sie bereits gewahr sind, sondern auch die Ausbildung und das Verständnis für eine kinderfreundliche und opferinformierte Umsetzung. Das heißt, dass Urteile verloren gehen und junge Menschen an diesen systemischen Problemen der Justizsysteme in ganz Europa scheitern. Ebenso wie es von den Kinderschutzexperten der Berliner Polizei heißt, dass sie im Rahmen dieses Vorschlags nicht mehr Straftäter, sondern mehr Fehlalarme erwarten, hört man auch von der niederländischen Polizei, dass sie kategorisch ausschließt, der Anzahl an Grooming-Berichten im Rahmen dieses Vorschlags Herr werden zu können.

Die **Vorsitzende:** Vielen Dank. Für die FDP-Fraktion Maximilian Funke-Kaiser.

Abg. **Maximilian Funke-Kaiser** (FDP): Vielen herzlichen Dank. Zunächst einmal finde ich es sehr bemerkenswert, dass ausnahmslos keiner sich für diesen Verordnungsentwurf ausgesprochen hat. Das habe ich so – auch wenn ich noch nicht so lange im Deutschen Bundestag bin – noch nicht gehört bei einer öffentlichen Anhörung. Meine erste Frage geht an Teresa Widlok und auch an Prof. Ulrich Kelber. Wie bewerten Sie den Vorschlag, eine Unterscheidung vorzunehmen in Bezug auf Server Side Scanning und Client Side Scanning, also eine Unterscheidung zu vollziehen, inwieweit man unverschlüsselte respektive verschlüsselte Kommunikation scannt.

SVe **Teresa Widlok:** Der technische Ansatzpunkt ist die eine Frage, und da bin ich immer noch an der Stelle, dass ich ein anlassloses Ausrollen solcher Technologien immer noch für nicht richtig halte. Aber ich finde, die viel wichtigere Unterscheidung – egal ob das jetzt sozusagen Client Side Scanning oder Server Side Scanning wäre –, ist die Frage, welche Materialien wir suchen oder finden wollen. Ob das bereits bekannte Materialien sind. Dieses EU-Center zum Beispiel: Das soll ja auch Indikatoren zur Verfügung stellen von bekanntem Material. Oder ob das ganz neues Material ist, das noch überhaupt nicht existiert. Die Fehlerraten sind nicht niedriger, nur weil man serverseitig scannt.

**Prof. Ulrich Kelber** (BfDI): Es gibt natürlich Unterschiede, zum Beispiel die Nicht-Notwendigkeit des Durchbrechens zum Beispiel von verschlüsselter Kommunikation, die dann möglich wäre. Viele andere

Fragestellungen, also die Unverhältnismäßigkeit des Eingriffs, die vollständige Durchleuchtung von Kommunikation und Daten, die im Fall von False-Positives dazu führen kann, dass solche Daten von Dritten eingesehen werden können, dass auch repressive Maßnahmen ergriffen werden, dass man ausgeschlossen wird von Diensten. Die Problematik ist bei beiden Ansätzen gleich. Das heißt, eine ganze Menge der Bedenken bleiben auch bei einem Client Side Scanning übrig.

Abg. **Maximilian Funke-Kaiser** (FDP): Also keine Unterscheidung, ob verschlüsselt oder unverschlüsselt. Wir haben gerade eben schon gehört: Es gibt eine sehr hohe Fehlerquote. Die nächste Frage richte ich wieder an Frau Widlok. Durch diese hohe Fehlerquote, die auch schon beschrieben wurde, müssen sehr viele Nutzer – auch von Messenger-Diensten – damit rechnen, dass ihre Inhalte überprüft werden, von den Moderatoren und den Strafverfolgungsbehörden. Was bedeutet das denn am Ende aus Ihrer Perspektive für Personengruppen wie beispielsweise Anwälte, die einem Berufsgeheimnis unterliegen, oder auch für Whistleblower?

SVe **Teresa Widlok:** Ganz genau kann ich es Ihnen natürlich nicht sagen, weil ich nicht den Berufsgruppen angehöre. Aber von allen Äußerungen zu diesem Entwurf, die jetzt von Journalistinnen, von Verbänden, von Patientinnen, Informanten und sonstigen Berufsgruppen gemacht wurden, die sich eben alle damit auseinandersetzen, habe ich keine positive Äußerung zu diesem Entwurf gehört, muss ich ehrlich sagen.

Abg. **Maximilian Funke-Kaiser** (FDP): Ich würde noch einen neuen Aspekt in die Anhörung einbringen und noch einmal an Sie, Frau Widlok, die Frage stellen: Was glauben Sie, welche angemessenen Maßnahmen es gäbe, um das eigentliche Ziel der Chatkontrolle zu erfüllen, und die verhältnismäßig wären sowie die Grundrechte nicht unverhältnismäßig einschränken würden?

SVe **Teresa Widlok:** Einen Punkt würde ich gerne aufgreifen an der Stelle, der vorhin schon einmal Erwähnung fand, und zwar diese Interimsverordnung, die auf freiwilliger Basis den Einsatz von Technologien zum Durchleuchten von Strukturen ermöglicht. Darüber könnte man ja theoretisch einmal nachdenken, ob man gegebenenfalls da behutsam herangeht und überlegt und evaluiert, inwiefern das ein sinnvolles Instrument ist. Es ist auch insofern spannend, weil der Scope – also der Anwendungsbereich dessen – viel enger war, als es jetzt dieser CSA-Verordnungsentwurf ist. Zum Beispiel waren Audiokommunikation, andere Kommunikationsinhalte sowie Seitenkommunikation, alle explizit ausgeschlossen, und dann will ich noch darauf hinweisen, dass der Entwurf selbst eine Abschätzung vorgenommen hat in seiner Begründung. Das ist eine Abstufung. Es gab fünf Optionen, die überlegt wurden. Von der Option A – gar keine legislativen Maßnahmen zu ergreifen, sondern eher praktische Unterstützung der Strafverfolgungsbehörden, bessere Ausstattung und so weiter – bis hin zur Option E, wie wir sie jetzt vor uns liegen haben, die dann ausgewählt wurde, die dann auch noch Grooming, neues Material und quasi die volle Bandbreite enthielt.

Das heißt, theoretisch war sich der Gesetzgeber auf europäischer Ebene da selber schon darüber im Klaren, dass es noch eine große Bandbreite an Themen gibt, die man vielleicht einmal angehen könnte. Dass es jetzt die Option E geworden ist, liegt vielleicht auch daran, dass die Fragen, wie Strafverfolgungsbehörden ausgestattet sind

und solche Dinge, eben nicht in der Zuständigkeit der Europäischen Kommission liegen, sondern das sind dezidierte Dinge, die auf mitgliedstaatlicher Ebene geregelt werden müssen. Wenn man als Europäische Kommission mitmachen will, braucht man eben den Ansatz E.

Die **Vorsitzende:** Vielen Dank. Ich muss ein bisschen die Zeit im Auge behalten. Als nächstes für die AfD-Fraktion Herr Janich.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine nächste Frage geht an Herrn Professor Kelber. Der Verordnungsentwurf der Kommission spricht vor allem über technische Möglichkeiten zur Überwachung der privaten digitalen Kommunikation. Die Frage nach dem notwendigen Personal zur Überprüfung der von einem Algorithmus inkriminierten Dateien spart er aus. Sollte der Entwurf in der vorliegenden Form realisiert werden – wie viele zusätzliche Personen in den Behörden der Strafverfolgung wären Ihrer Einschätzung nach mit dem Sichten des als kinderpornografisch identifizierten Materials beschäftigt?

**Prof. Ulrich Kelber** (BfDI): Da kann ich Ihnen keine Einschätzung geben. Weder zur Zahl noch zur Tiefe, da habe ich keine Erkenntnisse.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine nächste Frage an Herrn Reda. Der vorliegende Entwurf der Kommission sieht eine Altersverifizierung der Nutzer der Dienste durch deren Anbieter vor. Eine Selbstauskunft ist nicht sicher zu überprüfen. Ein biometrisches Scannen des Gesichtes etwa wäre das Ende der Anonymität im Netz. Einen elektronisch lesbaren Personalausweis gibt es in Deutschland erst ab 16 Jahren. Diese Methoden sind unvollständig und überdies fälschungsanfällig. Gibt es Ihres Wissens nach zuverlässige Methoden zur Altersfeststellungen im Netz, die zugleich die Privatsphäre der Nutzer respektieren?

SV **Felix Reda:** Nein, solche Methoden sind mir nicht bekannt.

Abg. **Steffen Janich** (AfD): Vielen Dank. Meine nächste Frage geht an Herrn Hartmann. Sind Ihnen die konkreten Umstände bekannt, unter denen Algorithmen des maschinellen Lernens darauf trainiert werden, Darstellungen des sexuellen Missbrauchs an Kindern zu erkennen? In welchen Ländern geschieht das? Anhand welcher Kriterien und Indikatoren, angeleitet durch welche Firmen, Organisationen und durch welches vorgebildetes Personal?

SV **Markus Hartmann:** Ich kann Ihnen dazu keinen europaweiten Überblick geben. Aus unseren eigenen Forschungsprojekten – wir engagieren uns auch im Bereich der Entwicklung solcher Detektionsmechanismen, allerdings nicht mit dem Fokus auf die Kontrolle der Kommunikation, sondern mit dem Fokus, bereits gesicherte Beweismittel, etwa nach Durchsuchungsmaßnahmen, schneller auswerten zu können – nehmen wir wahr, dass an unseren Entwicklungen in Deutschland ein hohes fachliches Interesse besteht und auch Wirtschaftsunternehmen und Wissenschaftsvertreter aktiv in die Kommunikation eintreten.

Daraus leite ich für mich ab, dass in diesem Technologiefeld noch sehr viel Bewegung ist, dass es auch noch einen hohen wissenschaftlichen Begleitungsbedarf gibt. Jetzt bitte ich um Verständnis. Ich bin qualifizierter Hobby-Informatiker, und insofern kann ich jetzt nicht die gesamte Wissenschaftsseite beurteilen, aber das Feedback, was wir quer durch die Bank bekommen, ist, dass wir doch an einer Bleeding Edge Technology in vielen Bereichen noch arbeiten, deren Zuverlässigkeit sich im weiteren Prozess

noch erweisen muss.

Abg. **Steffen Janich** (AfD): Vielen Dank. Die nächste Frage geht an Herrn Türk. Im Vorschlag der Verordnung auf Seite 47 wird definiert, dass als Kind jede natürliche Person unter 18 Jahren zu gelten habe. Ist es Ihrer Auffassung nach sinnvoll, beim Kampf gegen die Verbreitung kinderpornografischen Materials im Internet zwischen Kindern unter 14 Jahren und Jugendlichen unter 18 Jahren zu unterscheiden?

SV **Joachim Türk:** Ich halte das nicht für sinnvoll. Wir folgen da den Einstufungen der EU. Nationale Unterscheidungen sind am Ende juristische Festlegungen.

Abg. **Steffen Janich** (AfD): Vielen Dank. Ich verzichte auf den Rest.

Die **Vorsitzende:** Vielen Dank. Für DIE LINKE. Anke Domscheit-Berg.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Vielen Dank. Ich möchte Felix Reda von der Gesellschaft für Freiheitsrechte fragen, was denn eigentlich die Rechtsgrundlage für diese europäische Verordnung ist und welche Konsequenzen die Wahl dieser Rechtsgrundlage hat?

SV **Felix Reda:** Danke. Die Rechtsgrundlage ist Artikel 114 des Vertrages über die Arbeitsweise der EU. Das ist die Harmonisierung des Binnenmarktes. Es handelt sich hier um eine Form der Wirtschaftsregulierung, die es der EU erlaubt, auch Verordnungen zu erlassen, die direkt in der gesamten EU Gültigkeit erlangen. Es wird zwar in der öffentlichen Debatte über die Chatkontrolle-Verordnung vor allen Dingen das Ziel des Kinderschutzes in den Vordergrund gestellt. Aber wenn man sich den Vorschlag durchliest und die Ausführungen zur Rechtsgrundlage, dann sagt die EU-Kommission klar: Der Grund für diese Verordnung sei, dass einige Mitgliedstaaten unterschiedliche nationale Vorschriften zur Bekämpfung sexueller Gewalt gegen Kinder erlassen hätten und dass das zu einer Zersplitterung des Binnenmarkts führe und den Unternehmen bei der grenzübergreifenden Bereitstellung von Diensten im Weg stehen würde.

Mir hat noch niemand sagen können, was für nationale Vorschriften das sein sollen. Denn die EU hat ja gerade erst mit dem Digital Services Act den Umgang von Online-Intermediären mit illegalen Inhalten voll harmonisiert. Das heißt, Mitgliedstaaten dürfen solche Maßnahmen gar nicht verabschieden. Frau Widlok hat gerade das Problem der Kompetenzen angesprochen. Gegen diese Verordnung zu sein auf der Grundlage Artikel 114 bedeutet nicht, dass man gegen Maßnahmen zum Schutz von Kindern ist, sondern diese Verordnung grenzt einfach von vornherein die verfügbaren Maßnahmen auf Wirtschaftsregulierung ein. Wenn wir uns anhören, was die verschiedenen Expertinnen und Experten hier gesagt haben, sind ganz viele sinnvolle Maßnahmen im Bereich der Prävention, im Bereich der Ausstattung der Strafverfolgungsbehörden eben nicht Teil dieser Wirtschaftsregulierung und nur relativ wenige unter dieser Rechtsgrundlage machbar. Auch zum Beispiel das EU-Zentrum, das von einigen begrüßt wird. Es gibt auch Zweifel, ob alles das, was dieses EU-Zentrum machen soll, überhaupt auf der Rechtsgrundlage Artikel 114 möglich ist.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Vielen Dank. Mich würde – die Frage geht erneut an Felix Reda – noch interessieren, ob die mit der EU-Verordnung geschaffenen technischen Grundlagen nicht auch zur Durchsuchung von privater Kommunikation und von bei Hostern gespeicherten Inhalten nach ganz anderen Kriterien eingesetzt werden könnten – und damit auch anderen

Zwecken dienen könnten, als dem Schutz von Kindern. Wie wahrscheinlich sind solche Begehrlichkeiten? In dem Zusammenhang möchte ich noch einmal darauf hinweisen, dass die Hashwerte, von den heute schon die Rede war, ja auch nicht rückwärts gerechnet werden können. Ich kann durch niemanden – nicht durch Wissenschaftler, Journalisten, auch nicht durch Abgeordnete – kontrollieren, welcher Inhalt eigentlich in so einer Datenbank ist.

SV **Felix Reda:** Die Gefahr sehe ich in vielerlei Hinsicht gegeben. Am eklatantesten ist sie bei der Durchbrechung oder Schwächung der Ende-zu-Ende-Verschlüsselung. Denn es gibt keine Verschlüsselung nur für die Guten. In dem Moment, wo solche Hintertüren oder Client Side Scanning vorgesehen sind, können sie auch von Kriminellen für andere Zwecke missbraucht werden, auch von Geheimdiensten.

Ein anderer Punkt ist die Frage der Überwachung. Um welche Hashwerte geht es da? Herr Kelber hat einerseits die mangelnde Einbindung der Datenschutzbehörden erwähnt. Ich sehe aber darüber hinaus auch noch ein größeres Problem bei den Hosting-Anbietern, also den Anbietern von Cloud-Diensten zum Beispiel, denn es ist vorgesehen, dass die Dienste erst einmal eigene Risikominderungsmaßnahmen vornehmen müssen. Nur wenn diese nicht ausreichen, gibt es danach eine Aufdeckungsanordnung. Anders als die Chat-Programme, die unter die Privacy-Richtlinie fallen, sind diese Hosting-Dienste nicht grundsätzlich daran gehindert, private Inhalte zu scannen. Das bedeutet, wenn man sagt: Okay, ihr müsst jetzt erst einmal freiwillige Maßnahmen machen, dann werden die Anbieter gehalten sein, bei den Hosting-Diensten sehr viel weitreichendere Maßnahmen zu installieren, um so einer Aufdeckungsanordnung zu entgehen. Da gibt es dann überhaupt keine Aufsicht mehr. Das heißt, es gibt überhaupt keine Kontrolle darüber, wonach genau gefiltert wird, unter welchen Schutzvorkehrungen die Inhalte beispielsweise dann Mitarbeiterinnen und Mitarbeitern der Dienste vorgelegt werden und so weiter.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Herzlichen Dank. Vielleicht passend zur E-Privacy-Verordnung: Wie bewerten Sie, dass laut Artikel 1 Absatz 4 des Verordnungsentwurfs die E-Privacy-Richtlinie nicht wieder voll hergestellt werden soll?

SV **Felix Reda:** Das ist wahrscheinlich, wenn man die Chatkontrolle möchte, in dieser Form notwendig. Die E-Privacy-Richtlinie sagt ganz klar, dass interpersonelle Kommunikation mit elektronischen Mitteln nicht ausgelesen werden darf, und ohne diesen Aspekt außer Kraft zu setzen, kann man diese Aufdeckungsanordnung gegen interpersonelle Kommunikationsdienste nicht machen. Das verkennt, dass diese Regelungen der E-Privacy-Richtlinie aus den Grundrechten direkt abgeleitet sind. Das heißt, durch die Abschaffung der E-Privacy-Richtlinie kann man hier nicht die Grundrechte außer Kraft setzen.

Die **Vorsitzende:** Vielen Dank. Wir sind am Ende der zwei Fragerunden und damit am Ende unserer öffentlichen Anhörung. Ich möchte allen ganz, ganz herzlich danken, einmal den Sachverständigen für ihre wertvollen Hinweise, die wir in die weiteren Beratungen mitnehmen werden. Ich möchte auch den Vertreterinnen und Vertretern der Ministerien danken, dass Sie hier waren und zugehört haben. Ich möchte in diesem Zuge ganz herzlich Herrn Koenen noch zum Geburtstag gratulieren, der seinen Geburtstag heute mit uns verbringen wollte, bei dieser

wichtigen Anhörung. Also alles, alles Gute Ihnen! Genau, da kann man einmal klatschen und klopfen. Den Zuhörerinnen und Zuhörern einen ganz herzlichen Dank, sowohl im Saal, als auch an den Endgeräten, für das gezeigte Interesse. Ich danke den Leuten, die hinter der Technik standen und uns unterstützt haben. Das hat ja wieder alles gut funktioniert. Vielen Dank dafür. Ich danke auch vor allem dem Sekretariat des Ausschusses ganz herzlich für die Vorbereitungen und möchte noch den Hinweis auf die nächste Sitzung geben. Die nichtöffentliche Sitzung des Ausschusses findet direkt im Anschluss statt. Wir starten allerdings mit einem öffentlichen Tagesordnungspunkt. Dieser kann dann auch gerne von den Zuschauerinnen und Zuschauern weiterhin besucht werden. Wir benötigen allerdings jetzt eine fünfminütige Pause für den technischen Wechsel. Wir bleiben aber zunächst in der Zoom-Konferenz und starten dann erst zum nichtöffentlichen Teil mit Webex. Draußen steht ein Catering-Wagen für alle diejenigen, die sich zwischendurch stärken wollen. Dann bleibt mir nur noch, allen einen angenehmen Tag zu wünschen. Ich freue mich auf die nächste öffentliche Anhörung. Die Sitzung ist geschlossen. Vielen Dank.

Schluss der Sitzung: 15:56 Uhr

Tabea Rößner, MdB
**Vorsitzende**

# Anlagenkonvolut
# zum Wortprotokoll der 30. Sitzung am 1. März 2023

## Öffentliche Anhörung „Chatkontrolle“

**Stellungnahmen der eingeladenen Sachverständigen:**

**Elina Eickstädt**
Informatikerin und Sprecherin des Chaos Computer Clubs
A-Drs. 20(23)134
Englische Übersetzung zu 20(23)134

**Markus Hartmann**
Leitender Oberstaatsanwalt,
Leiter der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW)
A-Drs. 20(23)131
Englische Übersetzung zu 20(23)131

**Ella Jakubowska**
European Digital Rights (EDRi), Senior Policy Advisor
A-Drs. 20(23)137
Deutsche Übersetzung zu 20(23)137

**Felix Reda**
Gesellschaft für Freiheitsrechte (GFF), Projektleiter
A-Drs. 20(23)132
Englische Übersetzung zu 20(23)132

**Prof. Dr.-Ing. Martin Steinebach**
Fraunhofer-Institut für Sichere Informationstechnologie SIT,
Leiter Abteilung Media Security und IT Forensics
A-Drs. 20(23)133
Englische Übersetzung zu 20(23)133

**Joachim Türk**
Der Kinderschutzbund Bundesverband e.V.,
Mitglied des Bundesvorstandes und stv. Landesvorsitzender
A-Drs. 20(23)136
Englische Übersetzung zu 20(23)136

**Weitere Stellungnahmen:**

**Prof. Ulrich Kelber**
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)
A-Drs. 20(23)138