Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (2022/0155 (COD))[1]

Am 1. März 2023 führte der Ausschuss für Digitales des Deutschen Bundestages eine Anhörung unter dem Titel “Chatkontrolle” durch. Wir begrüßen, dass der Ausschuss sich dieses Themas angenommen hat, um eine Position gegenüber dem Verordnungsvorschlag zu entwickeln. Gleichwohl nehmen wir bedauernd zur Kenntnis, dass es seitens der Fraktionen offenbar kaum Interesse an einer ausgewogenen Betrachtung des Regulierungsvorhabens gibt. Dafür sprechen aus unserer Sicht die Auswahl der geladenen Sachverständigen, unter denen Akteur:innen, die eine konstruktive Haltung gegenüber dem Vorhaben einnehmen[2], leider fehlten, sowie die Bezeichnung der Anhörung mit einem alarmistischen Terminus, der den dem EU-Regulierungsvorschlag zugrundeliegenden Sachverhalten nicht gerecht wird. Der im Verordnungsentwurf nicht verwendete Begriff der Chatkontrolle wurde von Akteur:innen in eine Debatte eingeführt, welche das Anliegen des Kinderschutzes als im Widerspruch zu Privatsphäre- und Datenschutz stehend beschreibt und mit dem Ziel geführt wird, das Regulierungsvorhaben zu diskreditieren. Auch die Formulierungen des Fragenkatalogs, welcher den geladenen Sachverständigen zur Beantwortung übermittelt wurde, geben den Regulierungsvorschlag teilweise nicht korrekt wieder, sondern sind vielmehr suggestiv formuliert und spiegeln eine gewisse Voreingenommenheit der Verfassenden.[3]

Vor diesem Hintergrund nehmen wir anhand des Fragenkatalogs des Ausschusses für Digitales des Deutschen Bundestages aus zivilgesellschaftlicher und kinderrechtlicher Perspektive Stellung zu dem Verordnungsentwurf und möchten damit einen Beitrag zur Beratung und Meinungsbildung leisten.

1) Der Vorschlag der EU-Kommission zur CSA-Verordnung, auch bekannt als Chatkontrolle, hat seit seiner Veröffentlichung im Mai 2022 für viele Diskussionen gesorgt. Bitte erläutern Sie die technischen, juristischen, grundrechtlichen, datenschutzrechtlichen, sozialen und/oder gesellschaftlichen Implikationen des Vorschlags.

Die Europäische Kommission hat am 11. Mai 2022 ihre Strategie für ein Better Internet for Kids (BIK+) veröffentlicht. In dieser Strategie bündelt sie Zielstellungen und Maßnahmen, um Kindern eine selbständige und sichere Nutzung digitaler Umgebungen zu ermöglichen. Mittels altersgerechter Angebote sollen Kinder vor schädlichen und illegalen Inhalten geschützt, durch Medienkompetenzförderung zu einem eigenständigen und sicheren Agieren in digitalen Räumen befähigt sowie durch Partizipation an der Gestaltung kindgerechter Online-Angebote beteiligt werden. [4] Am selben Tag stellte die Europäische Kommission den hier zu diskutierenden Verordnungsentwurf vor. Beide Vorhaben sind zusammen zu betrachten und sollen gemeinsam dazu beitragen, dass junge Menschen an digitalen Erfahrungen teilhaben können, ohne dabei Schaden zu nehmen.
Der Verordnungsentwurf adressiert ein spezielles und gravierendes Risiko, dem sich viele junge Menschen online ausgesetzt sehen. Laut der JIM-Studie 2022[5] berichtet ein Viertel der Jungen und Mädchen im Alter von zwölf bis 19 Jahren in Deutschland von Kontaktaufnahmen durch Fremde im

[1] abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0209
[2] Übersicht von Akteuer:innen, die eine europäische Regulierung begrüßen abrufbar unter https://kinderrechte.digital/transfer/assets/9039.pdf
[3] Weiterführende Informationen abrufbar unter https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/932296-932296
[4] Weiterführende Informationen abrufbar unter https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids
[5] abrufbar unter https://www.mpfs.de/fileadmin/files/Studien/JIM/2022/JIM_2022_Web_final.pdf

digitalen Umfeld innerhalb der vergangenen zwölf Monate. Nicht in jedem Fall muss daraus ein Risiko erwachsen. Gleichwohl sind die Anbahnung und Ausübung sexualisierter Gewalt gegen Kinder eine reale Gefahr. Täter:innen nutzen dabei in hohem Maße digitale Umgebungen, um Kinder anzusprechen und kennenzulernen, untereinander zu kommunizieren sowie Materialien, die sexualisierte Gewalt abbilden und darlegen, zu verbreiten. Im Jahr 2021 wurden weltweit 85 Millionen Bildern und Videos entsprechender Straftaten von Internet-Unternehmen identifiziert und gemeldet.[6] Für die Bundesrepublik wurde im selben Jahr ein Anstieg um rund 110 Prozent bei Verbreitung, Erwerb, Besitz und Herstellung von Darstellungen sexualisierter Gewalt an Kindern und Jugendlichen durch die Polizeiliche Kriminalstatistik belegt.[7] [8] Dabei handelt es sich nur um die polizeibekannten Fälle (sog. Hellfeld). Nach Auskunft der Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs (UBSKM) Kerstin Claus hat sich Europa zum Drehkreuz für die Verbreitung entsprechender Missbrauchsabbildungen entwickelt.[9] Vor diesem Hintergrund ist es naheliegend, dass die Europäische Kommission einen Vorschlag zur Prävention und Bekämpfung solcher Straftaten vorgelegt hat. Unterstützung findet sie bei einer Mehrheit der Bevölkerung. So sprachen sich in einer Befragung von 9.410 Erwachsenen in acht europäischen Ländern[10] etwas mehr als drei Viertel (76 Prozent) für die automatische Erkennung, Meldung und Entfernung von Material aus, welches sexualisierte Gewalt an Kindern darstellt.[11]

Mit ihrem Regulierungsentwurf beabsichtigt die Europäische Kommission, Online-Diensteanbieter zu verpflichten, ihre Angebote auf entsprechende Risiken zu untersuchen (vgl. Art. 3 des Entwurfes) und diesen durch geeignete Vorsorge- und Sicherheitsmaßnahmen zu begegnen (vgl. Art. 4 des Entwurfes), sexualisierte Gewalt gegen Kinder aufzudecken und zu melden sowie entsprechende Darstellungen zu löschen bzw. den Zugang dazu zu verwehren (vgl. Art. 1 des Entwurfes). Sollte dabei die Erkenntnis gewonnen werden, dass die ergriffenen Maßnahmen potenzielle Risiken nicht hinreichend mindern, besteht die Möglichkeit, eine so genannte Aufdeckungsanordnung zu erlassen (vgl. Art. 7 des Entwurfes). Die in Umsetzung der Aufdeckungsanordnung zur Anwendung kommenden Technologien müssen wirksam zur Erkennung und Verhinderung der Verbreitung von bekannten oder neuen Darstellungen sexualisierter Gewalt gegen Kinder oder zur Verhinderung der Kontaktaufnahme zu Kindern beitragen und hinreichend zuverlässig in Bezug auf potenzielle Fehlmeldungen sein. Das Recht der Nutzenden auf Privatsphäre sowie auf Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten soll dabei so weitgehend wie möglich respektiert werden (vgl. Art. 10 des Entwurfes); dementsprechend sind die zuständigen Datenschutzbehörden in das Verfahren einzubeziehen. Gegen den Erlass einer Aufdeckungsanordnung kann mit Rechtsbehelf vorgegangen werden (vgl. Art. 9 des Entwurfes).

Mit der Better Internet for Kids Strategie (BIK+) adressiert die Europäische Kommission das bedeutende gesellschaftliche Anliegen der Befähigung junger Menschen, sich eigenständig und sicher im digitalen Umfeld zu bewegen und daran teilzuhaben. Dieses Anliegen wird durch den hier diskutierten Verordnungsentwurf, der ein relevantes Risiko adressiert, unterstützt. Im Sinne und Interesse der Mehrheit der Bevölkerung der Europäischen Union zeigt der Entwurf Maßnahmen auf, um sexualisierter Gewalt gegen Kinder vorzubeugen und strafrechtlich relevante Handlungen zu verfolgen. Die vorgeschlagenen Maßnahmen erscheinen nach Rechtsgüterabwägung vertretbar und praktikabel, um das formulierte Ziel zu erreichen.

---

[6] Weiterführende Informationen abrufbar unter https://home-affairs.ec.europa.eu/whats-new/campaigns/legislation-prevent-and-combat-child-sexual-abuse_de

[7] Laut PKS sind die Fälle von sexuellem Kindesmissbrauch im Jahr 2021 um 6,3 % auf über 15.500 Fälle gestiegen. Bei den Missbrauchsdarstellungen gab es einen Anstieg um 108,8 % auf über 39.000 Fälle.

[8] Weiterführende Informationen abrufbar unter https://beauftragte-missbrauch.de/presse/artikel?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=652&cHash=2f4ccb3e6f0591c91abbf74a7f194c8d

[9] Ebd.

[10] Frankreich, Deutschland, Italien, Niederlande, Polen, Schweden, Ungarn und Spanien

[11] Weiterführende Informationen abrufbar unter https://ecpat.de/wp-content/uploads/2021/11/PM-Childprotect_On-ECPAT-DE.pdf

*2) Der Vorschlag der Kommission sieht vor, dass Aufdeckungsanordnungen ergehen sollen, die dazu führen, dass Anbieter*innen von Kommunikationsdiensten oder Geräten verdeckt Informationen ausleiten müssen, sofern der Verdacht besteht, dass über diese Dienste oder Geräte Missbrauchsmaterial ausgetauscht wird oder auf diesen Grooming stattfindet. Welche Dienste und Geräte sind aus Ihrer Sicht davon potenziell und in welcher Reichweite betroffen und welche Auswirkungen hat dies auf deren Nutzer*innen?*

Zunächst weisen wir darauf hin, dass eine Aufdeckungsanordnung nicht aufgrund des Verdachts des Austauschs von inkriminiertem Material ergehen soll, vielmehr stehen am Beginn des Prozesses eine Risikobewertung des Dienstes durch den Anbieter sowie Maßnahmen zur Minderung eines ermittelten Risikos. Erst wenn im folgenden Verfahren festgestellt wird, dass die Maßnahmen zur Risikominderung nicht die erforderliche Wirkung erzielen, kommt eine Aufdeckungsanordnung in Betracht. Des Weiteren ist es unzutreffend, dass im Falle einer Aufdeckungsanordnung eine "verdeckte" Ausleitung erfolgt; vielmehr sind Informationspflichten der Anbieter gegenüber den Nutzer:innen in Art. 10, Abs. 5 zwingend vorgeschrieben.
Die Frage, welche Dienste und Geräte potenziell in welcher Reichweite betroffen sein könnten, kann pauschal nicht beantwortet werden. Theoretisch kommen jeder Kommunikationsdienst sowie jedes Angebot in Betracht, das einen Austausch unter den Nutzenden ermöglicht, um bekanntes und unbekanntes Material sexualisierter Gewalt gegen Kinder zu verbreiten bzw. um Kontakt zu Kindern aufzunehmen in der Absicht, sexualisierte Gewalt auszuüben. Infolgedessen ist ebenso grundsätzlich jedes Endgerät, welches den Zugang zu vorgenannten Angeboten eröffnet, potenziell von dem Verordnungsentwurf der Europäischen Kommission erfasst. Gerade vor diesem Hintergrund ergibt sich die Notwendigkeit einer Risikobewertung der Angebote, um genau die zu identifizieren, welche Vorsorgemaßnahmen und Sicherungskonzepte für ihre Nutzenden ergreifen müssen. Sollten von den betreffenden Anbietenden keine hinreichenden Maßnahmen zur Risikominderung sexualisierter Gewalt gegen Kinder ergriffen werden, kommt eine Aufdeckungsanordnung in Betracht. Wenn in diesem Fall, das Interesse an der Verhütung und Bekämpfung sexualisierter Gewalt schwerer wiegt als die potentiell negativen Eingriffe in die (Grund-)Rechte der Nutzenden des Angebotes (vgl. Art. 7 Abs. 4 a und b des Entwurfes), kommt es zur Umsetzung einer Aufdeckungsanordnung. Dann werden die Nutzenden des Angebotes darüber informiert, dass innerhalb des Angebotes entsprechende Maßnahmen zur Prävention und Bekämpfung sexualisierter Gewalt gegen Kinder ergriffen und infolgedessen ggf. Meldungen von Kommunikation und Inhalten an das EU-Zentrum erfolgen können (vgl. Art. 10 Abs. 5 des Entwurfes). Die Ausleitung von entsprechendem Material oder Informationen erfolgt insofern immer in Kenntnis der Nutzenden, von einer verdeckten und/oder anlasslosen Kontrolle kann daher keine Rede sein. Vielmehr verfolgt die EU-Kommission mit diesem transparenten Ansatz das Ziel, entsprechende Aktivitäten zu verhindern und Nutzende des Angebotes darüber zu informieren, dass sie an einem digitalen Umfeld teilhaben, welches Risiken und Gefahren für sie bergen kann.

3) Wieso ist der Kommissionsvorschlag Ihrer Meinung nach geeignet oder nicht geeignet, Kinder effektiv vor (sexuellen) Übergriffen und der Verbreitung von Missbrauchsmaterial zu schützen und wo sehen Sie konkreten Handlungsbedarf?

Sexualisierte Gewalt ist ein gravierendes Problem unserer Gesellschaft. Diesem muss mit einem umfassenden Ansatz begegnet werden. Dabei ist den meisten Akteur:innen bewusst, dass sie gemeinsam in einer Verantwortungsgemeinschaft aus Anbietenden, Regulierenden, Bildenden und Erziehenden agieren müssen, um nachhaltige und effiziente Ergebnisse erzielen zu können. Vor diesem Hintergrund gehören Vorsorge- und Schutzmaßnahmen, wie sie das 2021 reformierte Jugendschutzgesetz[12] vorsieht, und wie sie im Rahmen von *safety-by-design-Konzepten* mitunter

[12] s. Paragraph 24a JuSchG

bereits praktiziert werden, ebenso dazu wie Politik- und Regulierungsansätze, die Anbietende dazu verpflichten, in die Sicherheit ihrer Angebote zu investieren, sowie Einrichtungen der Bildung, die Kinder- und Jugendhilfe und zivilgesellschaftliche Akteur:innen in die Lage versetzen, Kinder, Erziehungsberechtigte und Fachkräfte für einen sicherheitsbewussten Umgang mit digitalen Angeboten zu befähigen.
Mit der Allgemeinen Bemerkung Nr. 25[13] [14] hat der Kinderrechteausschuss der Vereinten Nationen 2021 den Vertragsstaaten wegweisende Hinweise und Anregungen gegeben, wie die Konvention über die Rechte des Kindes der Vereinten Nationen im digitalen Umfeld anzuwenden ist, um die Rechte auf Schutz, Befähigung und Teilhabe für alle Kinder zu verwirklichen. Für den europäischen Raum weisen sowohl die Strategie des Europarates für die Rechte des Kindes [15] als auch die EU-Kinderrechtsstrategie[16] zentral auf Schutz- wie Teilhabebedürfnisse von jungen Menschen im und am digitalen Umfeld hin.
Der Verordnungsentwurf unterstützt die Umsetzung dieser Richtlinien durch Maßnahmen der Prävention und Bekämpfung sexualisierter Gewalt gegen Kinder. So ist es naheliegend und bestenfalls intrinsisch motiviert, dass Anbietende ihre Angebote auf mögliche Risiken und Gefährdungen hin analysieren und dann geeignete Maßnahmen ergreifen, um jungen Nutzenden eine sichere Online-Erfahrung zu ermöglichen, da sichere Angebote für Kinder die Attraktivität eines Dienstes steigern und hinsichtlich der Verantwortungsübernahme in der Gemeinschaft positiv wahrgenommen werden. Sofern Anbietenden dazu jedoch nicht Willens oder in der Lage sind, greift die staatliche Gemeinschaft zeitlich befristet ein, um bei der Realisierung einer sicheren Online-Umgebung zu unterstützen und die Verpflichtung zur Gewährleistung der Sicherheit junger Menschen durchzusetzen.
Mit Auslaufen der Ausnahme zum Schutz von Kindern im Internet zur ePrivacy-Richtlinie im Sommer 2023 besteht konkreter Handlungsbedarf in Bezug auf die Regelung einer risikobewertungsbasierten Verpflichtung zum Monitoring hinsichtlich bereits bekannter und bis dahin unbekannter Darstellungen sexualisierter Gewalt gegen Kinder sowie von Kommunikation in der Absicht des Cybergroomings. Diesen Bedarf soll der Verordnungsentwurf der Europäischen Kommission decken.

*4) Wie schätzen Sie die Gefahr ein, dass unbescholtene Bürger*innen, durch falsch positive automatisierte Erkennung unter Verdacht geraten und was würden solche Falsch-Positiv-Meldungen für Auswirkungen sowohl auf die Verdächtigten als auch die Ermittlungsbehörden haben?*

Kein Ermittlungsverfahren – unabhängig davon, ob human oder technisch basiert – ist frei von Fehlern und Falscheinschätzungen. Daher gilt es potenziell strafrechtlich relevantes Verhalten oder Material möglichst objektiv und im Kontext zu bewerten. Die Unschuldsvermutung gilt bis das Gegenteil bewiesen ist. Entsprechend müssen Prüfvorgänge sensibel, nachvollziehbar und entlang der Rechtsordnung bearbeitet werden. Eine Vorverurteilung darf nicht stattfinden.
Ebenso sollte jedoch auch selbstverständlich sein, dass illegales Verhalten aufgedeckt, die Täterschaft aufgeklärt und strafrechtliche Konsequenzen gezogen werden. Dafür ist es im konkreten Kontext geboten, technische Mittel unterstützend einzusetzen, um der Vielzahl von bekannt illegal sowie unbekannt illegal zirkulierenden Materialien sowie der Alter und Unerfahrenheit ausnutzenden Anbahnung von Kontakten Älterer mit dem Ziel der Ausübung sexualisierter Gewalt gegen Kinder

[13] Originaldokument in englischer Sprache abrufbar unter https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
[14] Deutsche Sprachversion abrufbar unter https://www.dkhw.de/fileadmin/Redaktion/1_Unsere_Arbeit/1_Schwerpunkte/2_Kinderrechte/2.14_Koordinierungsstelle_Kinderrechte/2.14.1_Kinderrechte_in_der_digitalen_Welt/Allgemeine_Bemerkung_25_final_09_11_2021_so6.pdf
[15] Abrufbar unter https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a5a064
[16] Abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021DC0142&from=en#footnoteref70

begegnen zu können. Sowohl quantitativ wie auch qualitativ kann Technologie eine wertvolle Unterstützung und Ergänzung menschlicher Aufklärungs- und Strafverfolgungsarbeit sein. Dabei soll darauf Wert gelegt werden, dass den Technologien nicht die abschließende Bewertung zukommt, sondern diese in jedem Fall einem Menschen vorbehalten bleibt.
Der Verordnungsentwurf der Europäischen Kommission sieht vor, dass entsprechend ausgeleitete Kommunikation oder Materialien (vgl. Art. 12 des Entwurfes) zunächst von Beschäftigten des EU-Zentrums begutachtet werden (vgl. Art. 48 des Entwurfes). Damit leistet die Europäische Kommission einen wesentlichen Beitrag einerseits zur Entlastung der nationalen Strafverfolgungsbehörden, welche sich in der Folge auf Vorgänge konzentrieren können, die von unabhängigen Expert:innen als relevant für die Strafverfolgung bewertet wurden. Andererseits wirkt sie so auch potentiellen Vorverurteilungen entgegen, da nicht jede Meldung eines prüfungsrelevanten Vorganges überhaupt strafverfolgungsrelevant wird. Das EU-Zentrum kann demnach auch als eine weitere Sicherheitsgarantie dahingehend betrachtet werden, dass Expert:innen sexualisierter Gewalt gegen Kinder Sachverhalte bearbeiten und sortieren, bevor diese bei den Strafverfolgungsbehörden bekannt und dort weiterverfolgt werden. Insgesamt ist daher von positiven Auswirkungen dieses Verfahrens auf mögliche Verdächtigte und die Ermittlungsbehörden auszugehen, da durch die Begutachtung unabhängiger Expert:innen eine Reduktion der Verdachtsfälle und somit eine Konzentration der Ermittlungsarbeit auf relevante Vorgänge zu erwarten ist.
Die Europäische Kommission unterstreicht mit diesem Ansatz sowie der Bereitschaft zum Aufbau und zur Ausstattung des EU-Zentrums ihre Verantwortung sowohl für den Schutz von Kindern als auch für den Schutz der Rechte der Nutzenden von risikobehafteten Online-Angeboten.

5) Anbieter von Hostingdiensten und Anbieter interpersoneller Kommunikationsdienste, die eine Aufdeckungsanordnung erhalten haben, sollen laut Artikel 10 CSAM-E Technologien installieren und betreiben, die die Kontaktaufnahme zu Kindern mit Missbrauchsabsicht ("Grooming") erkennen. Sind Ihnen Technologien bekannt, die verlässlich zwischen unbedenklicher, sexuell oder romantisch aufgeladener, Kommunikation und Grooming unterscheiden können?

Es existiert keine Technologie die verlässlich im Sinne einer einhundertprozentig sicheren Entscheidung in der Lage ist die Kontaktaufnahme zu Kindern durch Ältere mit Absicht der Ausübung sexualisierter Gewalt zu erkennen. Gerade deshalb ist es so wichtig, dass nicht jede Meldung einer Technologie ungeprüft durch einen Menschen den Strafverfolgungsbehörden zugeleitet wird und dort für Überlastungen sorgt sowie Beteiligte des Vorgangs möglicher Vorverurteilung aussetzt.
Gleichwohl existieren Verfahren, welche unter Wahrung von Verschlüsselungsmechanismen in der Lage sind anhand von Metadaten und/oder Mustern mit einer hohen Wahrscheinlichkeit zu erkennen, ob es sich bspw. um SPAM-Nachrichten oder Malware handelt. Diese Technologien kommen grundsätzlich auch zur Erkennung von Grooming-Absichten in Betracht. Um mögliche Belastungen aus Fehlmeldungen zu reduzieren können Meldeschwellen implementiert werden, die erst ab einer gewissen Anzahl erfasster potentieller Verdachtsfälle in einem zu definierenden Zeitraum zu einer entsprechenden Reaktion des Systems führen.
Im Übrigen verweisen wir auf unsere Ausführungen in der Antwort zur Frage 4.

6) Welche technischen Ansätze halten Sie für effektive und grundrechtlich unbedenkliche Alternativen zu den im Verordnungsentwurf vorgesehenen Maßnahmen?

Der Verordnungsentwurf schlägt mit seiner Kombination aus Technikeinsatz und menschlicher Prüfung nach heutigem Stand die bestmögliche Vorgehensweise vor, um sexualisierter Gewalt gegen Kinder online vorzubeugen und diese nachzuverfolgen. Dabei berücksichtigt die Europäische Kommission den umfassenden Stellenwert der Grundrechte der Nutzenden von Online-Angeboten und wägt diese mit den Schutz- und Teilhaberechten von Kindern und Jugendlichen an und in digitaler Umgebung ab. Auch

sieht die Europäische Kommission ein mehrstufiges Verfahren aus Risikoanalyse, der Implementierung von Vorsorge- und Schutzmaßnahmen sowie einer ggf. notwendigen Aufdeckung illegaler Praktiken vor. Gerade weil eine Aufdeckungsanordnung grundrechtssensibel ist und alle Nutzenden eines Angebotes betrifft definiert sie hohe Anforderungen an die Umsetzung einer Aufdeckungsanordnung (vgl. Art. 7 und 10 des Entwurfes). Auch unterliegt der Erlass einer solchen Anordnung der kritischen Betrachtung verschiedener Akteur:innen und trägt somit zu einer ausgewogenen, zielgerichteten und effektiven Entscheidung bei (vgl. Art. 7 des Entwurfes), welche der betroffene Anbietende rechtlich überprüfen lassen kann (vgl. Art. 9 des Entwurfes).

*7) Der Vorschlag der Kommission enthält u.a. die Forderung nach einer verpflichtenden Altersverifikation. Wo genau und unter welchen Voraussetzungen müssten Internetnutzer*innen nach diesem Vorschlag ihr Alter verifizieren und welche technischen Ansatzpunkte gibt es oder werden gerade erforscht, um eine Altersverifikation grundrechtskonform unter Wahrung der Anonymität der Nutzer*innen im Internet umzusetzen?*

Ziel des Verordnungsvorschlags ist es Kinder und Jugendliche vor sexualisierter Gewalt zu schützen bzw. diese nachzuverfolgen. Im Nachgang der erforderlichen Risikoanalyse sollen Anbieter demnach zielführende Maßnahmen ergreifen, um Minderjährige in ihren Angeboten sinnvoll schützen zu können. Dafür kann es sinnvoll oder notwendig sein, dass Alter der Nutzenden zu kennen (vgl. Art. 3 des Entwurfes). Daher ermächtigt der Verordnungsentwurf die Anbietenden nach erfolgter Risikofeststellung dazu Altersüberprüfungen der Nutzenden vorzunehmen, um die Gefährdung zu minimieren (vgl. Art. 4 des Entwurfes). Entsprechendes soll für die Anbietenden von App-Stores gelten sofern diese Angebote mit nachgewiesenen Risiken bereithalten (vgl. Art. 6 des Entwurfes). Die Altersverifizierung würde insofern jede:n Nutzenden erfassen, wenn diese ein risikobehaftetes Angebot in Anspruch nehmen.
Bestehende Altersverifizierungsverfahren basieren auf dem Nachweis höchstpersönlicher Daten, bspw. durch die Vorlage oder das Übertragen der Informationen des Personalausweises und/oder nutzen biometrische Daten in Live-Nachweisverfahren, welche ebenso sehr sensibel sind.[17] In keinem der bestehenden Verfahren wird die Anonymität der Nutzenden gewahrt, da regelmäßig mehr Daten erhoben und verarbeitet werden als zur Feststellung des Alters notwendig sind. Im Sinne des Ziels dieses Verordnungsvorschlags erscheint es ausreichend, nicht das präzise Alter der Nutzenden zu kennen, sondern zielgerichtete Unterscheidungen zwischen Altersgruppen vorzunehmen, um effektive Vorsorge- und Sicherheitsmaßnahmen für diese Gruppen vorhalten zu können. Ein grundrechtskonformes, datensparsames und Anonymität wahrendes Altersverifizierungsverfahren wird derzeit innerhalb der Bundesregierung beraten.

*8) Der Vorschlag der Kommission würde es ermöglichen, private Kommunikationsdienste zu Aufdeckungsanordnungen zu verpflichten, u.a. um Inhalte aus privaten und verschlüsselten Chats zu erlangen (u.a. Client Side Scanning), um Grooming zu erkennen oder das Alter zu verifizieren; als Folge des technologieneutralen Ansatzes sind potenziell auch Netzsperren denkbar. Welche internationalen Konsequenzen würden solche Möglichkeiten, das Nutzer*innenverhalten zu analysieren, oder den Zugang zu Online-Inhalten und sicheren Räumen zu beschränken, zeitigen – insbesondere im Hinblick auf eine höhere Gefahr rechtswidriger Eingriffe (Hacking) in die Privatsphäre europäischer Bürger*innen aus dem Ausland und im Hinblick darauf, dass autoritäre Staaten die EU-Regeln als Blaupause für illegitime Überwachungsmaßnahmen ohne rechtsstaatliche Einhegung nutzen?*

[17] Erläuterungen zu entsprechenden Verfahren im Rahmen des PostIdent-Angebotes abrufbar unter https://www.deutschepost.de/de/p/postident.html

Die Frage adressiert potenzielle (Neben-)Wirkungen des Verordnungsentwurfes, die außerhalb der Europäischen Union liegen (könnten) und unbekannte Dritte in den Blick nehmen. Sofern darauf abgestellt wird, dass entsprechende Technologien in anderen Staaten und ggf. anderen (inhaltlichen) Kontexten zur Anwendung kommen könnten, ist darauf zu verweisen, dass nicht die Technologie und die damit erhobenen Daten ein etwaiges Problem darstellen, sondern deren Verwendung in Zusammenhängen, welche nach hiesigen Maßstäben als nicht demokratisch und/oder nicht rechtsstaatlich betrachtet würden.
Der Verordnungsentwurf der Europäischen Kommission setzt hohe Standards an die in Umsetzung einer Aufdeckungsanordnung zur Anwendung kommenden Technologien. Diese müssen wirksam sein zur Erkennung der Verbreitung von bekannten oder neuen Darstellungen sexualisierter Gewalt gegen Kinder oder der Kontaktaufnahme zu Kindern und hinreichend zuverlässig in Bezug auf Fehlmeldungen. In das Recht der Nutzenden auf Privatsphäre sowie auf Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten sollen sie geringstmöglich eingreifen (vgl. Art. 10 des Entwurfes). Dieser technologieoffene Ansatz ist als Anreiz für die Diensteanbietenden zur Entwicklung entsprechend leistungsfähiger Systeme gesetzt, um den Schutz von Kindern in digitalen Umfeldern sowie den Schutz der Privatsphäre aller Nutzenden in ihren Angeboten zu gewährleisten. Systeme, welche nicht in der Lage sind, diesen Anforderungen zu genügen dürfen entsprechend der Vorgaben des Verordnungsentwurfes nicht zur Anwendung kommen. Wir erachten das Risiko, dass wirksame Systeme zur Aufdeckung von inkriminiertem Material unter außereuropäischen Jurisdiktionen zu anderen, potenziell nicht-demokratischen Zwecken zum Einsatz kommen als gering. Wir verweisen dazu auch auf die in Folge des Inkrafttretens des Netzwerkdurchsetzungsgesetzes in Deutschland entsprechend geäußerten Befürchtungen, die sich jedoch nicht bewahrheitet haben; das Gesetz wurde bisher nicht in anderen Ländern nachgeahmt oder zu undemokratischen Zwecken instrumentalisiert.

9) Zuletzt hat das „Child Rights International Network“ in einer Studie die Bedeutung unterstrichen, „das Framing von Privatsphäre versus Kinderschutz hinter uns [zu] lassen, um die Rechte aller Kinder zu schützen“ (Berichterstattung bei netzpolitik.org vom 02.02.2023). Wie verhält sich der aktuelle EU-Kommissionsvorschlag zu dem Recht von Kindern und Jugendlichen auf Privatsphäre und sichere IT-Systeme und welche kurzfristigen und langfristigen Konsequenzen hätte der Kommissionsvorschlag im Hinblick darauf?

Mit der Studie “Privacy and Protection: A children’s rights approach to encryption”[18] leistet das Child Rights International Network (CRIN) einen Beitrag für die holistische Betrachtung der Kinderrechte, wie sie in der 1989 durch die Vereinten Nationen verabschiedeten Konvention über die Rechte des Kindes[19] verbrieft wurden. Demnach sind alle Kinderrechte gleichwertig zu betrachten und nur im Zusammenwirken zu realisieren. Daraus folgt, dass die Rechte des Kindes auf Schutz vor Gewalt (Art. 19 UN-KRK) oder vor sexuellem Missbrauch (Art. 34 UN-KRK) und auf den Schutz der Privatsphäre (Art. 16 UN-KRK) gleichermaßen wirksam sind und sich in keinem Über- oder Unterordnungsverhältnis zueinander befinden. Auch bedingen sich die Rechte und tragen wechselseitig zu ihrer Realisierung bei. Das CRIN hat mit der Studie untersucht, wie sich Verschlüsselung(stechnologien) auf das Aufwachsen und Leben von Kindern auswirken. Dabei stellt die Untersuchung Bezüge der Kinderrechtskonvention unter Berücksichtigung der Allgemeinen Bemerkung Nr. 25 und konkreten Situationen her, in denen Kinder von Verschlüsselung profitieren oder durch diese nachteilig betroffen sind. Dabei werden Vorteile und Risiken aufgezeigt, die für Verwirklichung der Kinderrechte mit der Verschlüsselung einhergehen. CRIN plädiert dafür anzuerkennen, dass Kinder Individuen und keine einfältige Gruppe sind und wirbt dafür zu berücksichtigen, dass die Auswirkungen von Verschlüsselung je nach Herkunft,

[18] Abrufbar unter https://static1.squarespace.com/static/5afadb22e17ba3eddf90c02f/t/63c9173dc9ac2348a1d9eac7/1674123078909/Privacy+and+Protection+-+CRIN+defenddigitalme+encryption+report.pdf
[19] Abrufbar unter https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

Bedürfnissen und Identität des Kindes sehr unterschiedlich sein können. Mit dem Bericht schlägt das Netzwerk daher verschiedene Szenarien vor, um die Diskussion über das Paradigma von Privatsphäre versus Schutz hinaus zu öffnen, und gibt Beispiele für die Vielfalt und Komplexität der ethischen, rechtlichen und praktischen Fragen. Insgesamt gehen die Beteiligten des Netzwerkes davon aus, dass Privatsphäre und Schutz zusammengedacht werden sollten und alle Maßnahmen, die zum Schutz junger Menschen ergriffen werden auf ihre Wirkung hin überprüft werden mögen. Darüber hinaus weisen sie darauf hin, dass sich Debatten um den Schutz von Kindern und Jugendlichen im digitalen Umfeld nicht allein auf technische Ansätze reduzieren dürfen und werben dafür bestehende Schutzsysteme für diese ganzheitlich in den Blick zu nehmen. Nicht zuletzt machen sie darauf aufmerksam, dass Kinder mit ihren Ansichten und Perspektiven in entsprechende Debatten einzubeziehen sind. Im Ergebnis sollten Anbietende in die Verantwortung genommen und dazu angehalten werden transparent darzulegen, wie sie Kinderrechtsverletzungen in ihren Angeboten und Diensten begegnen sowie Hinweise und Unterstützung dazu bekommen, wie sie ihre Produkte sicher für Kinder gestalten können. Als ein zentrales Instrument erachtet CRIN dabei kindgerechte Meldeverfahren. Der Umgang mit entsprechenden Meldungen sollte zeitnah und nachvollziehbar gestaltet werden. Auf den übermäßigen Einsatz von Technologien sollte dabei verzichtet werden.
Da sich der hier diskutierte Verordnungsentwurf wie zuvor bereits dargelegt in eine umfassendere Strategie für die sichere Teilhabe von Kindern in und am digitalen Umfeld einordnet und gerade nicht allein auf technische Möglichkeiten des Schutzes vor sexualisierter Gewalt abstellt folgt der Ansatz der Europäischen Kommission dem empfohlenen Vorgehen des CRIN zum Schutz von Kindern vor sexualisierter Gewalt online. In ihrem Bericht warnen die Verfassenden die Diskussion um den Schutz junger Menschen auf die Dimension der Überwachung zu verengen und werben für eben solch einen vielseitigen Ansatz: *No single law, policy or technological development can protect children online or secure their human rights more broadly. Encryption cannot be addressed in isolation, but only as part of a wider ecosystem with a range of actors that can meaningfully interact, each with its own role that it can effectively and legitimately play* (vgl. S. 104).

10) Welches politische Maßnahmenpaket ist aus Ihrer Sicht ganzheitlich erfolgsversprechend, um wirksam, effektiv und grundrechtskonform gegen sexualisierte Gewalt an Kindern vorzugehen – wo besteht Nachsteuerungs- und Verbesserungspotenzial im Bereich der Prävention und bei der Bekämpfung von sexualisierter Gewalt und deren Darstellung im Internet?

Das Maßnahmenpaket der Europäischen Kommission bestehend aus der Better Internet for Kids Strategie (BIK+) sowie dem hier diskutierten Verordnungsentwurf zeigt sowohl umfassende wie auch zielführende Wege auf, um sexualisierte Gewalt gegen Kinder vorzubeugen und zu verfolgen. Im Übrigen verweisen wir auf unsere Ausführungen in der Antwort zur Frage 3, in welcher zu entsprechend vielgestaltigen Maßnahmen bereits verwiesen wurden.

11) Erfasst der Vorschlag der EU-Kommission alle Plattformen im Internet, auf denen kinderpornographisches Material verbreitet werden kann, zielgerecht oder in welcher Form besteht möglicherweise Nachbesserungsbedarf mit Blick auf den Geltungsbereich?

Sofern die Frage darauf abzielt, dass der Verordnungsentwurf der Europäischen Kommission nicht das Darknet erfasst, möchten wir darauf aufmerksam machen, dass Kriminalität nicht ausschließlich im Verborgen stattfindet. Auch, wenn sich die Erkenntnisse aus nachvollziehbaren Gründen nur auf das sog. Hellfeld beziehen können, wird deutlich, dass der Austausch strafrechtlich relevanten Materials in erheblichem Umfang im Internet stattfindet.[20] Und auch hinsichtlich der Kontaktanbahnung von

[20] vgl. https://home-affairs.ec.europa.eu/whats-new/campaigns/legislation-prevent-and-combat-child-sexual-abuse_de

erwachsenen Fremden gegenüber Kindern mit dem Ziel der Ausübung sexualisierter Gewalt ist davon auszugehen, dass diese vorrangig im offen zugänglichen Internet stattfindet, da sich Kindern in der Regel nicht im Darknet aufhalten und somit dort auch nicht für Täter:innen ansprechbar sind.
Hinweisen möchten wir in diesem Zusammenhang ebenso darauf, dass jedes neu als inkriminiert identifizierte Foto oder Video zu einem zusätzlichen Hash-Wert führt und somit dazu beiträgt, die Datenbank bekannten Materials zu erweitern und so die Verbreitung von (dann) bekanntem Material sexualisierter Gewalt gegen Kinder einzudämmen. Dies ist von besonderer Bedeutung, da jede Weiterleitung, Neueinstellung oder anderweitige Zurverfügungstellung dieses Materials die Fortsetzung eines Verbrechens darstellt, was bei den abgebildeten Kindern zu einer erneuten Viktimisierung führt sowie Heilungs- und Verarbeitungsprozesse beeinträchtigen oder gar zu weiteren Verletzungen führen kann. Auch leistet jedes bekannt gewordene Foto oder Video, welches bereits eindeutig als strafrechtlich relevant und illegal eingestuft wurde, einen Beitrag zur Entlastung der Ermittlungs- und Strafverfolgungsbehörden, da entsprechende Bewertungsprozesse nicht erneut durchgeführt werden müssen.
Ungeachtet dessen zielt die Europäische Kommission mit ihrem Verordnungsentwurf darauf ab sexualisierter Gewalt gegen Kinder vorzubeugen, insofern ist die Fokussierung auf das Internet folgerichtig und naheliegend. Die vorgeschlagenen Maßnahmen erscheinen in der Zusammenschau mit den Vorhaben der Better Internet for Kids Strategie (BIK+) geeignet einen wirkungsvollen Beitrag zum Schutz von Kindern im digitalen Umfeld zu leisten.

12) Sind Instrumente zur besseren Strafverfolgung und Rechtsdurchsetzung hinreichend im Vorschlag der EU-Kommission gewürdigt worden, wo besteht möglicherweise Verbesserungsbedarf und welche Instrumente wären dazu notwendig?

Die Verordnung zielt darauf, die Menge der verbreiteten Darstellungen sexualisierter Gewalt gegen Kinder sowie die Fallzahlen des Groomings durch Prävention und Abschreckung zu reduzieren. Täter:innen müssen derzeit weder im offenen Internet noch im Darknet mit einer hohen Wahrscheinlichkeit der Aufdeckung ihrer Straftaten rechnen. Darauf reagiert der Entwurf mit der Androhung der Aufdeckungsanordnung, wenn die Risikobewertung für den Dienst eine hohe Wahrscheinlichkeit für die Ausübung derartiger Straftaten ergibt. Dadurch aufgedeckte Fälle resultieren aus einem fundierten Monitoring und dürfen daher zu einem hohen Prozentsatz als valide gelten, so dass sie einen entsprechenden Ermittlungsaufwand der zuständigen Strafverfolgungsbehörden mit dem Ziel der Rechtsdurchsetzung nach sich ziehen werden. Wie hoch dieser Aufwand sein wird und welche personellen Ressourcen dafür benötigt werden, hängt entscheidend davon ab, in welchem Maße eine abschreckende Wirkung durch die drohende Aufdeckung der Straftaten erzielt werden kann – ein hoher strafrechtlich bewirkter Abschreckungsgrad führt generell zu einer Reduzierung der Fallzahlen. Dennoch ist eine bessere Ausstattung der Ermittlungsbehörden grundsätzlich wünschenswert; diese fällt jedoch in die Zuständigkeit der nationalen Ebene und kann nicht per Verordnung seitens der Europäischen Kommission angeordnet werden.

13) Wird das neue EU-Zentrum die nationalen Strafverfolgungsbehörden und Europol, laut der aktuellen Planungen, angemessen unterstützen können und welche Ausstattung würde es dazu benötigen?

Das geplante Zentrum wird als eigenständige Rechtseinheit der Europäischen Union errichtet (vgl. Art. 41 des Entwurfes) und soll dem Ziel der Vorbeugung und Bekämpfung sexualisierter Gewalt gegen Kinder dienen. Dafür ist laut dem Verordnungsentwurf vorgesehen, dass es Informationen und Fachkenntnisse sammelt und zur Verfügung stellt, bei der Aufdeckung, Meldung und Entfernung sowie Sperrung entsprechender Materialien unterstützt sowie die Arbeit weiterer Behörden und auch mit

Privaten durch Kooperationen unterstützt (vgl. Art. 40, 43ff des Entwurfes). Zu den aufzubauenden Datenbanken mit Indikatoren sowie Meldungen werden Europol als auch die nationalen Strafverfolgungsbehörden in Zusammenarbeit mit dem EU-Zentrum auf Antrag Zugang erhalten sofern dies für deren Arbeit erforderlich und dienlich ist (vgl. Art. 46 des Entwurfes). Darüber hinaus soll das EU-Zentrum über die Kompetenz verfügen eigenständig Hinweise und Informationen zu etwaigen Straftaten direkt an Europol und die zuständigen Strafverfolgungsbehörden weiterleiten zu können (vgl. Art. 48 des Entwurfes). Die vorgesehenen Prozesse zum Zusammenwirken und der Unterstützung erscheinen geeignet, um das Ziel der Vorbeugung und Bekämpfung sexualisierter Gewalt gegen Kinder effektiv erreichen zu können.
Die Aufstellung und Ausführung des Haushaltsplans inklusive des Stellenplans obliegt dem Exekutivdirektor des EU-Zentrums. Dieser legt jährlich dem Exekutivausschuss einen Voranschlag vor. Dieser fertigt auf Grundlage des Voranschlags einen endgültigen Entwurf und leitet diesen dem Europäischen Parlament, dem Rat und der Europäischen Kommission zu. Unter Berücksichtigung der seitens der Europäischen Kommission für erforderlich erachteten Mittel für Haushalt und Personal bewilligen Europäisches Parlament und Rat die Mittel für das EU-Zentrum (vgl. Art. 67 des Entwurfes). Es obliegt mithin der Entscheidung des Europäischen Parlaments und des Rates das EU-Zentrum mit einer auskömmlichen Ausstattung zu unterstützen.

14) Umfasst der Vorschlag der EU-Kommission aus Ihrer Sicht alle technischen Ansätze, mit denen das Ziel, dem Schutz von Kindern gerecht zu werden, erreicht werden kann und welche weiteren technischen Ansätze wären aus Ihrer Sicht erforderlich?

Mit ihrem Entwurf für die Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern hat sich die Europäische Kommission für einen technologieoffenen Ansatz entschieden. Insbesondere vor dem Hintergrund der fortlaufend voranschreitenden (Weiter-) Entwicklung von Technologien ist es ausdrücklich zu begrüßen, dass in dem Regulierungsdokument nicht der Einsatz spezifischer Technologien festgeschrieben wird. Dies hätte zur Folge, dass die Verordnung regelmäßig hinsichtlich neu zur Verfügung stehender Mittel aktualisiert werden müsste. Da technologische Entwicklungen oftmals schneller vonstattengehen als ein formales Novellierungs- oder neues Rechtssetzungsverfahren, wäre die Gefahr sehr groß, dass der Verordnungstext regelmäßig hinter dem technischen Möglichen zurückbleiben würde und infolgedessen Kindern nicht der jeweils bestmögliche Schutz vor sexualisierter Gewalt zukommen könnte. Darüber hinaus eröffnet die ausbleibende Benennung konkreter Technologien den Anbietenden einen Freiraum, den sie unter Berücksichtigung der durch die Verordnung zu setzenden Vorgaben nutzen können, um geeignete Verfahren zur Vorbeugung und Bekämpfung sexualisierter Gewalt gegen Kinder einzusetzen und/oder (weiter-) zu entwickeln.
Da der Technologie offene Ansatz zukunftsweisend und vorausschauend ist, wird dieser auch durch den deutschen Gesetzgeber angewandt. So definiert bspw. dass 2021 reformierte Jugendschutzgesetz in den neu erlassenen Regelungen Ziele zur sicheren Teilhabe von Kindern und Jugendlichen am digitalen Umfeld und beschreibt nicht abschließend, welche Maßnahmen durch die Anbietenden für deren Erreichung sinnvoll und effektiv eingesetzt und ergriffen werden könnten. Damit verfolgt der hiesige Gesetzgeber denselben Ansatz, wie die Europäische Kommission
im hier zu diskutierenden Verordnungsentwurf.

15) Der Verordnungsentwurf sieht auch die Möglichkeit von Netzsperren einzelner URLs vor, die im Zuge der bisherigen Entwurfsänderungen während der tschechischen Ratspräsidentschaft sogar noch ausgeweitet werden sollen. Halten Sie es angesichts der weit verbreiteten https Verschlüsselung von URL-Abrufen für technisch möglich, einzelne URLs gezielt zu sperren, ohne auf die Sperrung ganzer Domains zurückzugreifen, wenn ja, auf welche Weise soll dies möglich sein und wenn nein, können

Netzsperren auf diese Weise den Anforderungen des europäischen Gerichtshofs an die Zielgerichtetheit von Netzsperren genügen?

Der Verordnungsentwurf gibt nach unserer Einschätzung der Löschung von inkriminiertem Material eindeutige Priorität gegenüber der Sperrung. Angesichts der für sichere Onlinetransaktionen erforderlichen https-Transportverschlüsselung bedürfte die Feststellung, dass inkriminierte Inhalte übermittelt werden, einer Deep Package Inspection, wie sie beispielsweise auch zur Bekämpfung von Viren, Spam und Protokollverstößen eingesetzt wird.
Für das mit dem Verordnungsentwurf zu bekämpfende Material ist, aufgrund der mit dessen Herstellung und Verbreitung für die Betroffenen einhergehenden schwerwiegenden und traumatisierenden Folgen, der Löschung grundsätzlich Vorrang zu geben, denn nicht gelöschtes Material kann jederzeit erneut auffindbar gemacht und weiterverbreitet werden.

16) Wie bewerten Sie die Rolle und den Charakter des laut EU-Verordnungsentwurf geplanten EU-Zentrums einerseits mit Blick auf die Wahrnehmung primär präventiver Aufgaben und andererseits mit Blick auf Aufgaben, die die Entwicklung und den Einsatz technischer Überwachungswerkzeuge betreffen?

Ein Zentrum, das auf europäischer Ebene präventive Maßnahmen wahrnimmt und koordiniert, ist aus unserer Sicht zu begrüßen. Wie zu Frage zwölf ausgeführt, tragen Prävention und Abschreckung dazu bei, Fallzahlen zu reduzieren und so Ermittlungsarbeit auf die relevanten Fälle zu konzentrieren. Prävention besteht jedoch nicht allein aus aufklärenden und pädagogischen Maßnahmen gegenüber Kindern und Erziehungsverantwortlichen, sie muss vielmehr auch den Einsatz technischer Instrumente der Prävention, d. h. der Verhinderung sexualisierter Gewalt gegen Kinder umfassen. Die Entwicklung derartiger technischer Instrumente ist nach unserer Ansicht Aufgabe der Anbieter von Diensten und Plattformen, bei denen erhebliche Risiken festgestellt wurden.
Für das EU-Zentrum sehen wir die Aufgabe, den Austausch von Wissen und Erkenntnissen im Hinblick auf den Einsatz und die Wirksamkeit technischer Instrumente zu ermöglichen. Darüber hinaus ist für das EU-Zentrum die Aufgabe der Unterstützung Betroffener von sexualisierter Gewalt – ungeachtet der Herkunft der Betroffenen und der Täter:innen – vorgesehen; dies ist ein Ansatz, der aus zivilgesellschaftlicher und kinderrechtlicher Perspektive unbedingt zu begrüßen ist.

17) Wenn nicht die Endgeräte, sondern die mit ihnen mögliche Kommunikationen („Chats“) durchsucht würden, gälte das auch für eine Ende-zu-Ende-Verschlüsselung etwa von Messenger-Diensten. Auch hier gerieten ungezählte gesetzestreue Bürger ins Visier der Behörden, nur weil sie einen bestimmten Dienst mit entsprechender Software nutzen. Sind Ihnen Software Lösungen bekannt, die das Echtzeit-Mitlesen oder zumindest das Knacken Ende-zu-Ende-verschlüsselter Kommunikation erlauben? Halten Sie es für vertretbar, die grundgesetzlich garantierte vertrauliche private Kommunikation durch Algorithmen aufzuheben?

Der Verordnungsentwurf sieht eine Aufdeckungsanordnung dann vor, wenn von einem Angebot erhebliche Risiken der sexualisierten Gewalt gegen Kinder ausgehen sowie die Verhütung und Bekämpfung dieses Missbrauchs schwerer wiegt als die potentiell negativen Eingriffe in die (Grund-)Rechte der Nutzenden des Angebotes (vgl. Art. 7 Abs. 4 a und b des Entwurfes). Kommt es zur Umsetzung einer Aufdeckungsanordnung, werden alle Nutzenden des Angebotes zuvor darüber informiert, dass innerhalb des Angebotes entsprechende Maßnahmen zur Prävention und Bekämpfung sexualisierter Gewalt gegen Kinder ergriffen und infolgedessen ggf. Meldungen an das EU-Zentrum erfolgen werden (vgl. Art. 10 Abs. 5 des Entwurfes). Insofern erfolgt die Prüfung von Materialien und Kommunikationen durch Technologien in Kenntnis der Nutzenden und es ist davon auszugehen, dass damit eine hohe abschreckende Wirkung auf Täter:innen einhergeht. Kommt es auf

der Basis des eingesetzten Algorithmus zur Ausleitung entsprechender Materialien und Kommunikationen, ist eine Prüfung durch Expert:innen des EU-Zentrums auf mögliche Strafbarkeit vorgesehen. Das Ergreifen von weiteren Maßnahmen basiert daher nicht allein auf dem eingesetzten Algorithmus. Für die Aufdeckung potenziell strafrechtlich relevanter Handlungen innerhalb von Kommunikationen bedarf es nicht zwingend der Kenntnis der Kommunikationsinhalte. Vielmehr kommen bereits heute in anderen Kontexten Instrumente zur Erkennung von Mustern zum Einsatz. So analysieren zum Beispiel Finanzdienstleister Finanzströme dahingehend, ob Micro-Payments zeitgleich aus verschiedenen Regionen der Welt auf bestimmten Konten eingehen und können so zur Aufdeckung von live gestreamter sexualisierter Gewalt gegen Kinder beitragen. Entsprechende Muster, bspw. eine Vielzahl von Kontaktanfragen an bis dahin nicht mit dem Profil der anfragenden Person verbundene Nutzer:innen, können ein Hinweis auf einen breit angelegten Grooming-Prozess sein. Hier würde es sich bei einer weitergehenden Analyse der interpersonellen Kommunikation gerade nicht um eine anlasslose Überwachungsmaßnahme, sondern vielmehr um eine durch einen Anfangsverdacht begründete Ermittlung handeln.
Das Recht auf Privatsphäre und vertrauliche Kommunikation ist wesentlich für unser Zusammenleben und stellt ein hohes Gut dar. Nicht weniger von Bedeutung ist der Schutz von Kindern vor sexualisierter Gewalt und ihr Recht auf ein gesundes Aufwachsen. Vor diesem Hintergrund setzt die Europäische Kommission mit ihrem Verordnungsentwurf hohe Anforderungen an eine Aufdeckungsanordnung sowie die dabei zur Anwendung kommenden Technologien. Diese müssen wirksam sein zur Erkennung der Verbreitung von bekannten oder neuen Darstellungen sexualisierter Gewalt gegen Kinder oder zur Verhinderung der Kontaktaufnahme zu Kindern in sexueller Absicht und hinreichend zuverlässig in Bezug auf potenzielle Fehlmeldungen funktionieren. In das Recht der Nutzenden auf Privatsphäre sowie auf Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten sollen sie geringstmöglich eingreifen (vgl. Art. 10 des Entwurfes).

18) Im Verordnungsentwurf heißt es, das zu gründende Zentrum für Fragen des sexuellen Kindesmissbrauchs in Den Haag solle verbindliche Indikatoren für Abbildungen sexuellen Missbrauchs liefern, die von den scannenden Unternehmen anzuwenden seien. Nun wissen erfahrene Ermittler, dass es keineswegs eindeutig zu definieren und im Einzelfall zu belegen ist, aufgrund welcher Kriterien was als Familienfoto, als selbstdokumentiertes Spiel unter Kindern und Jugendlichen, als Zufallsschnappschuss einer Sportveranstaltung oder eben als Kinderpornografie zu gelten hat. Gibt es bereits Erkenntnisse über das methodische Vorgehen des genannten EU-Zentrums? Und falls ja, kann dieses Vorgehen gegebenenfalls als verlässlich und geeignet eingeschätzt werden?

Da das EU-Zentrum noch nicht existiert besteht keine Grundlage um seriöse Aussagen über ein potentielles methodisches Vorgehen der Behörde treffen zu können und dieses fachlich zu bewerten. Absehbar erscheint, dass Kenntnisse, Indikatoren und Technologien sich in Umsetzung der Verordnung sukzessive weiterentwickeln werden und infolgedessen die Ermittlungssicherheit steigen sowie die Fehlerquoten sinken werden. Gleichwohl ist nicht davon auszugehen, dass Technologien in absehbarer Zukunft allein ohne menschliche Mitwirkung, die Aufgaben zur Verhütung und Bekämpfung der sexuellen Gewalt bewältigen können.