Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)131

22.02.2023

Generalstaatsanwaltschaft Köln
Zentral- und Ansprechstelle Cybercrime
Nordrhein-Westfalen - ZAC NRW

Stellungnahme zu der öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestags zur „Chatkontrolle“ am 1. März 2023

I. Vorbemerkung

Die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) ist als hybride Einrichtung bei der Staatsanwaltschaft und bei der Generalstaatsanwaltschaft Köln eingerichtet. Gemäß Abschnitt 3 der AV d. JM vom 15. März 2016 in der Fassung vom 17. Dezember 2021 (4100 - III. 274, ZAC-AV) führt die Zentralstelle in ihrem staatsanwaltschaftlichen Teil Verfahren von herausgehobener Bedeutung bei Straftaten des Cybercrime im engeren Sinne und – bei bestimmten besonderen digitalen Kriminalitätsphänomenen – im weiteren Sinne in Nordrhein-Westfalen. Zu den besonderen Deliktsphänomenen gehören unter anderem die internet-konnexen Straftaten gegen die sexuelle Selbstbestimmung von Kindern und Jugendlichen, namentlich die sogenannten Mantelverfahren als Ermittlungsverfahren gegen Unbekannt zur Auswertung einer Vielzahl gebündelter digitaler Spuren mit dem Ziel der Identifizierung beschuldigter Personen und die landesweite Verfahrensführung von aus der Meldepflicht nach § 3a Absatz 2 Nummer 3 b) NetzDG und aus Meldungen des US-National Centers for Missing and Exploited Children (NCMEC) sowie vergleichbarer Organisationen resultierenden Vorgängen. Neben diesem Deliktsbereich bearbeitet die Zentralstelle in besonderem Maße Verfahren wegen Angriffen gegen kritische Infrastrukturen, Behörden, staatliche Einrichtungen und Unternehmen und ist in diesem Zusammenhang mit vielfältigen Fragen der Informationssicherheit befasst.

Bei der Generalstaatsanwaltschaft Köln ist die ZAC NRW als landesweite Ansprechstelle Cybercrime eingerichtet. Zu deren Aufgabenkreis gehören u. a. gemäß Abschnitt 4.1 der ZAC-AV die Zuständigkeit für grundsätzliche, verfahrensunabhängige Fragestellungen aus dem Bereich des Cybercrime und gemäß Abschnitt 4.3 der ZAC-AV eine Forschungszuständigkeit mit dem Ziel der (Fort-) Entwicklung praxisrelevanter Methoden und Techniken für die Strafverfolgung. Dazu arbeitet die Zentralstelle mit nationalen und internationalen Partnern aus Wissenschaft und Wirtschaft zusammen. Zentrale wissenschaftliche Projekte sind derzeit im Bereich des Einsatzes künstlicher Intelligenz zur automatischen Beurteilung kinder- und jugendpornografischer[1] Bild- und Videoinhalte angesiedelt. Daneben befasst sich die Zentralstelle als Ansprechstelle auch mit Fragen des Einsatzes und der Auswirkungen von Kryptographie im Ermittlungskontext.

[1] Für die Ausarbeitung wird im Wesentlichen die gesetzliche Terminologie des 13. Abschnitts des Besonderen Teils des Strafgesetzbuchs zugrunde gelegt.

Die ZAC NRW ist damit im Kern eine operative Strafverfolgungseinrichtung, deren Forschungs- und Entwicklungsarbeit auf die Unterstützung in Ermittlungs- und Strafverfahren und die Nutzbarmachung moderner technischer Entwicklungen für die Strafverfolgungspraxis gerichtet ist. Die Beurteilung der Vorschläge der EU-Kommission zur sogenannten Chatkontrolle erfolgt daher in dieser Stellungnahme vornehmlich unter dem Gesichtspunkt der staatsanwaltschaftlichen und der allgemeinen Strafverfolgungspraxis. Die Perspektiven der Prävention, der verbesserten Compliance und sonstige Auswirkungen auf gesellschaftliche, politische sowie technische Aspekte werden mit Blick auf die hier vorhandene Expertise nur in ihrer jeweiligen Interaktion mit der Strafverfolgung beleuchtet.

II. Einzelfragen

Dies vorausgeschickt merke ich zu den Einzelfragen in der mit Blick auf den engen Zeitrahmen der Anhörung gebotenen Komprimierung an:

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.

Der Verordnungsvorschlag der Europäischen Kommission zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (CSAM-E), der die aktuell geltende Übergangsverordnung (EU) 2021/1232 vom 14. Juli 2021 ablösen soll, hat – soweit er die Harmonisierung des Binnenmarkts durch einheitliche EU-Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern zum Ziel hat – Auswirkungen auch auf die Tätigkeit der mit dem Deliktsphänomen des Kindesmissbrauchs im digitalen Raum befassten nationalen Strafverfolgungsbehörden. Sind die Scanning-Aktivitäten der großen Internetkonzerne (u. a. Facebook/Meta, Microsoft, Google/Alphabet) von unverschlüsselten Messenger- und E-Mail-Nachrichten sowie gehosteten Dateien und gepostetem Content auf Kindesmissbrauchsdarstellungen bislang freiwillig erfolgt, sollen diese nun verpflichtend sein, indem für „alle Anbieter von Hosting- oder interpersonellen Kommunikationsdiensten auf dem digitalen Binnenmarkt der EU“ (im Folgenden: Diensteanbieter) – das heißt unter anderem für Hostprovider, interpersonelle Kommunikationsdienste (Messenger und E-Mail) und Appstores sowie Zugangsprovider – einheitliche, sich nach der Art des Dienstes richtende Verpflichtungen festgelegt werden, um künftig die

Nutzung von Hosting- und Kommunikationsdiensten für die Verbreitung von Darstellungen des sexuellen Kindesmissbrauchs und die Kontaktaufnahme zu Kindern, das so genannte „Grooming", zu verhindern.

Dabei kommt insbesondere den folgenden fünf Ausprägungen des Vorschlags eine besondere Bedeutung für die Strafverfolgungspraxis zu, wobei hier datenschutzrechtliche, soziale, gesellschaftliche und/oder technische Aspekte nur aus spezifischer Sicht der Strafverfolgungsbehörden eine Betrachtung erfahren:

1. **Pflicht zur präventiven Bewertung und Minderung von Risiken**
   Diensteanbieter sollen künftig zur Durchführung einer Risikobewertung, das heißt zur Feststellung verpflichtet sein, ob und inwieweit ihre Dienste für die Verbreitung von Material über sexuellen Kindesmissbrauch oder für die Kontaktanbahnung missbraucht werden können und Maßnahmen zur Risikominderung vorsehen. Soweit hier auch die Einführung einer Altersverifizierung in Betracht gezogen wird, dürfte damit jede anonyme Nutzung von Kommunikationsdiensten faktisch unmöglich werden, da ein wirksamer Ausschluss Minderjähriger von der Nutzung der Dienste nur durch ein die persönliche Identifizierung ermöglichendes Verfahren, nicht aber schon durch die bloße Altersbestätigung zu erreichen sein dürfte. Wegen der Folgewirkungen für den Bereich des Open-Source-Ökosystems wird auf die Antwort zu Frage 7 verwiesen.

2. **Gezielte Aufdeckungspflichten auf der Basis von sog. *detection orders* (Aufdeckungsanordnungen)**
   Ergibt die durch eine seitens der Mitgliedstaaten noch zu benennende nationale Koordinationsbehörde vorzunehmende Prüfung, dass trotz etwaig ergriffener Risikominimierungsmaßnahmen weiterhin ein erhebliches Risiko für die Nutzung des Dienstes im Kontext von Kindesmissbrauch besteht (zu vgl. Artikel 7 CSAM-E), sollen auf Antrag der national einzurichtenden Koordinierungsbehörden von einem Gericht oder einer unabhängigen Verwaltungsbehörde zeitlich befristete und der Aufdeckung einer bestimmten Art von Inhalt in einem bestimmten Dienst dienende Anordnungen erlassen werden können, durch welche die Diensteanbieter verpflichtet werden sollen, am Maßstab und unter Nutzung seitens eines noch einzurichtenden EU-Zentrums bereitgestellter Indikatoren bekanntes oder unbekanntes Material zu sexuellem Kindesmissbrauch oder Kontaktanbahnungen ausfindig zu machen. Im Ergebnis sind die Diensteanbieter damit gezwungen, auf Anordnung eine Einsicht in die Inhalte ihrer Dienste vorzunehmen. Werden die Diensteanbieter zum Adressaten einer solchen Überprüfungsanordnung, sind sie gehalten, Technolo-

gien einzusetzen, die den in Artikel 10 Abs. 3 CSAM-E zur Umsetzung einer Aufdeckungsanordnung bestimmten Anforderungen entsprechen. Dabei obliegt dem Anbieter die Entscheidung, ob er sich hierzu einer eigenen Software oder der Softwareentwicklung des EU-Zentrums gegen Kindesmissbrauch bedient (zu vgl. Artikel 10 Abs. 2; Artikel 40 bis 42 CSAM-E). Die eingesetzten Technologien sollen dabei einerseits effektiv zur Erkennung der Verbreitung von bekannten und neuen Darstellungen sexuellen Kindesmissbrauchs oder der Kontaktaufnahme zu Kindern beitragen und zum anderen über einen zuverlässig geringen Fehlerquotienten bei der Extraktion einschlägiger Informationen verfügen, um so die Betroffenheit anderer Informationen weitgehend zu vermeiden. Zudem sollen die Technologien dem neuesten Stand der Technik entsprechen und den mit ihrem Einsatz einhergehenden Grundrechtseingriff möglichst geringhalten. Vor diesem Hintergrund und in Ansehung der zu überprüfenden Datenmengen werden die Kommunikationsdienste und Interprovider ihrer Verpflichtung im Ergebnis nur durch eine vollumfassende automatisierte, weitgehend KI-basierte Prüfung der Kommunikationsinhalte – und damit letztlich auch nur vermeintlich technikoffen – nachkommen können. Soweit sich die Überprüfungsmechanismen in Anbetracht der im Vorschlag klar definierten Anforderungen und der zu erwartenden Menge an Daten und Inhalte realistisch betrachtet nur in Gestalt der vollständigen Kenntnisnahme und automatisierten Scannung aller Inhalte eines Dienstes umsetzen lassen, stellen sich diese als Eingriff in europäische (und nationale) Grundrechte dar, der in seiner Intensität und Ausprägung von der konkreten Umsetzung sowie der Art des jeweils betroffenen Dienstes und Inhaltes abhängt. Insoweit wird auf die Antwort zu Frage 3 Bezug genommen.

Hinsichtlich der zum Einsatz gebrachten Technologien dürfte dabei zu differenzieren sein: Bei den Anbietern unverschlüsselter bzw. lediglich transportverschlüsselter Kommunikationsdienste (z. B. E-Mails, Messenger sozialer Netzwerke wie Facebook, Instagram, Twitter) steht aufgrund der Regelungsinhalte zu erwarten, dass serverseitig Algorithmen zum Einsatz kommen, um eine automatisierte Erkennung von Abbildungen von Kindesmissbrauch und Grooming-Nachrichten zu gewährleisten. Anders verhält es sich bei den Anbietern von Ende-zu-Ende-verschlüsselter Kommunikation (etwa WhatsApp, Threema, Signal). Hier ist eine Prüfung der Kommunikationsinhalte aufgrund ihrer Verschlüsselung bereits technisch ausgeschlossen. Zwar lässt der Verordnungsvorschlag insoweit offen, wie die Anbieter entsprechender Kommunikationsdienste ihre Verpflichtung künftig technisch umzusetzen haben. Da verschlüsselnde Anbieter jedoch von der Verordnung nicht ausgenommen und damit gleichermaßen zu einer Inhaltsprüfung nach Maßgabe der Verordnung verpflichtet sind, werden diese gehalten sein, eine Prüfung der Inhalte bereits vor der Verschlüsselung vorzunehmen, das heißt in der App oder dem Dienst selbst

einen Mechanismus einzubauen, der die Nachricht überprüft, bevor diese versendet – und damit verschlüsselt – wird. Im Ergebnis bedeutet dies für die Überprüfung der Ende-zu-Ende-verschlüsselten Inhalte, dass diese – will man Verschlüsselung nicht gänzlich abschaffen oder technologisch schwächen – auf den Endgeräten der Nutzer, sog. Client-Side-Scanning, zu prüfen sein werden. Kommunikationsdienste und Interprovider sollen die Kommunikationsinhalte dabei direkt auf dem Endgerät – vor deren Versand – untersuchen und bewerten sowie im Verdachtsfall ausleiten. Die Implementierung von Aufdeckungsanordnungen berührt damit in erheblichem Maße auch Fragen der Informationssicherheit, denn sie führt im Ergebnis eine Sollbruchstelle für Verschlüsselungstechnologie ein, deren Risiko- und Missbrauchspotentiale evident sind.

Durch die in Aussicht genommene Implementierung von Aufdeckungsanordnungen dürften in Anbetracht der hohen Fehlerrate der eingesetzten Technologien bei Milliarden überprüfter und jedenfalls Millionen gemeldeter Kommunikationsinhalte (auch) private Unterhaltungen und – zu einem wohl erheblichen Teil der absoluten Intimsphäre zuzurechnende – private Bild- und Videodateien zahlreicher Unionsbürgerinnen und Unionsbürger von einer Vielzahl von Prüfenden zur Kenntnis zu nehmen und zu prüfen sein, auch wenn der Vorschlag vorab eine zunächst automatisierte und sodann erst menschliche Prüfung im EU-Zentrum vorsieht.

3. Meldepflichten und Entfernung inkriminierten Materials

Diensteanbieter sollen verpflichtet werden, als relevant eingestufte Inhalte einem neu einzurichtenden EU-Zentrum zu melden und umgehend die Entfernung des Materials über sexuellen Kindesmissbrauch zu bewirken. Ist eine Entfernung nicht möglich, sollen die Diensteanbieter verpflichtet sein, den Zugang zu Bildern und Videos zu sperren (zu vgl. Artikel 16 bis 18 CSAM-E). Kommen die Diensteanbieter ihrer Verpflichtung zur Entfernung bzw. Sperrung nicht nach, sollen die nationalen Behörden befugt sein, eine Entfernungsanordnung erlassen. Hinsichtlich der Wirksamkeit von Sperrmechanismen wird auf die Antwort zu Frage 15 Bezug genommen.

4. Kontrollmechanismen und Rechtsbehelfe

Mit dem Ziel, die Gefahr von Falscherkennungen und -meldungen so gering wie möglich zu halten, soll vor einer Weiterleitung der auf diese Weise generierten Meldungen von mutmaßlich sexuellem Kindesmissbrauch eine vorherige Prüfung durch das EU-Zentrum erfolgen. Zudem sollen „verschiedene Maßnahmen ergriffen (werden), damit sowohl die Anbieter als auch die Nutzer über einen wirksamen Rechtsbehelf verfügen“ (zu vgl. die Regelungen in Artikel 9, 15, 18 CSAM-E). So

soll etwa den Anbietern von Hostingdiensten und Anbietern interpersoneller Kommunikationsdienste, die eine Aufdeckungsanordnung erhalten haben, sowie Nutzerinnen und Nutzer, die von den zu deren Ausführung ergriffenen Maßnahmen betroffen sind, ein Recht auf einen wirksamen Rechtsbehelf zukommen, der das Recht umfasst, die Aufdeckungsanordnung vor den Gerichten des Mitgliedstaats der zuständigen Justizbehörde oder der unabhängigen Verwaltungsbehörde, die sie erlassen hat, anzufechten (zu vgl. Artikel 9 CSAM-E). Mit Blick auf die Komplexität der Rechtswahrnehmung für einzelne Nutzerinnen und Nutzer – zumal im europäischen Rechtskontext – bleibt zweifelhaft, ob individuelle Rechtsbehelfe ein hinreichend geeignetes Korrektiv für etwaigen Fehlgebrauch von Aufdeckungsanordnungen sein können. Damit kommt den Anbietern eine Rechtsgarantiefunktion für ihre Nutzerinnen und Nutzer zu, die sie im Hinblick auf ihre vornehmlich wirtschaftlichen Interessen kaum in geeigneter Weise ausfüllen können. Hier dürfte sich dringend die Einführung eines starken und unabhängigen Kontrollmechanismus empfehlen.

5. Einrichtung eines EU-Zentrums

Der Vorschlag sieht die Schaffung eines sog. Europäischen Zentrums zur Prävention und Bekämpfung des sexuellen Missbrauchs (EU-Zentrum) vor, dem insbesondere die Funktion einer Kompetenz- und Koordinierungsstelle zukommen soll. So sollen dem EU-Zentrum unter anderem die Aufgaben der Bereitstellung von Indikatoren für die Aufdeckung sexuellen Kindesmissbrauchs und der Einrichtung der hierfür erforderlichen Datenbanken, der Entgegennahme entsprechender Meldungen der Diensteanbieter sowie die Prüfung von (Falsch-) Meldungen zugedacht sein. Daneben soll das EU-Zentrum die nationalen Behörden bei der Wahrnehmung der ihnen zugedachten Aufgaben und die Opfer bei der Entfernung sie betreffender Inhalte unterstützen. Ferner sollen Inhalte – sofern sich der Verdacht eines missbrauchsrelevanten Inhaltes bestätigt – an Europol oder nationale Sicherheitsbehörden weitergeleitet werden (zu vgl. Artikel 48 CSAM-E).

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?

Voraussetzung für die Aufdeckungsanordnungen ist nicht die in erheblichem Maße tatsächlich festzustellende *Verwendung* des Dienstes für Kindesmissbrauch. Vielmehr

reicht bereits ein erhebliches *Risiko* – unabhängig vom Umfang – einer einschlägigen Nutzung für die Anordnung von Überprüfungsmechanismen aus (zu vgl. Artikel 7 Abs. 4 CSAM-E), sodass künftig alle Dienste und Geräte digitaler Kommunikation von den Regelungen des Verordnungsentwurfs erfasst sein dürften. Eine Eingrenzung auf einzelne Dienste erscheint auch mit Blick auf die Weite der Anbieterdefinition (zu vgl. Artikel 2 CSAM-E) nicht intendiert; insbesondere sind bestimmte Reichweiten- oder Nutzungsschwellenwerte nicht vorgesehen.

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?

Strafrecht ist in besonderem Maße angewandte Verhältnismäßigkeit. Strafverfolgung um jeden Preis ist – ungeachtet des betroffenen Deliktsbereichs – unter der Geltung deutschen und europäischen Verfassungsrechts keine tragfähige Alternative. Aus der spezifischen Perspektive einer Strafverfolgungsbehörde muss der Kommissionsvorschlag im Sinne der klassischen Verhältnismäßigkeitstrias daher geeignet, erforderlich und verhältnismäßig im engeren Sinne sein, das Ziel der Bekämpfung von Straftaten im Bereich des sexuellen Kindesmissbrauchs (zu vgl. Erwägungsgrund 1) zu erreichen. Die reine (technische) Eignung ist stets in den Kontext einer konkreten Verhältnismäßigkeitsabwägung zu stellen. Daraufhin zu prüfen sind wegen ihrer Strafverfolgungsbezüge vor allem die Aufdeckungsanordnung, nachgeordnet aber auch das EU-Zentrum und die Meldepflicht für inkriminierte Inhalte.

Hierzu im Einzelnen:

1. <u>Aufdeckungsanordnung</u>

Die Aufdeckungsanordnung als Kern der Kommissionsvorschläge mit Bezügen zur Strafverfolgungspraxis erweist sich als nicht uneingeschränkt erforderlich, um das Ziel einer verbesserten und wirksamen Bekämpfung des netzkonnexen Kindesmissbrauchs zu erreichen. Sie begegnet darüber hinaus – teilweise durchgreifenden – Bedenken in Bezug auf ihre Angemessenheit.

a) An der grundsätzlichen Legitimität des Zwecks der Bekämpfung sehr schwerer Straftaten aus dem Gesamtdeliktsfeld des internetkonnexen sexuellen Kindesmissbrauchs (zu vgl. Erwägungsgrund 13) und des Mittels einer staatlichen Regulierung für bestimmte netzbezogene Anwendungsfälle bestehen keine Bedenken.

b) Das durch den Kommissionsvorschlag vorgesehene Mittel der Aufdeckungsanordnung dürfte auch geeignet, das heißt in Bezug auf den angestrebten Zweck zumindest förderlich sein. Denn es steht zu erwarten, dass sowohl die Zahl der erkannten Straftaten des internetkonnexen sexuellen Kindesmissbrauchs durch die vorgeschlagene Maßnahme erhöht als auch die Identifikation einzelner tatverdächtiger Personen gefördert werden wird. Zu berücksichtigen sein dürften bei der Frage der Eignung auch Verdrängungseffekte hin zu Technologien und Anbietern, die durch die ausschließlich nutzerseitige Herrschaft über das Schlüsselmaterial bzw. den Verschlüsselungsprozess Aufdeckungsanordnungen leerlaufen lassen oder sich schlicht der EU-Jurisdiktion entziehen. Solche Effekte stehen zu erwarten, dürften in Bezug auf das Volumen der Gesamtkommunikation jedoch lediglich untergeordnete Bedeutung erlangen. Jedenfalls ist auf Basis der Praxiserfahrungen der ZAC NRW die vorgeschlagene Maßnahme nicht als schlechthin ungeeignet zu qualifizieren.

c) Erhebliche und im Ergebnis durchgreifende Bedenken bestehen jedoch bereits in Bezug auf die Erforderlichkeit jedenfalls eines Teils der mit der Aufdeckungsanordnung verbundenen Maßnahmen, insbesondere soweit sie sich gegen Ende-zu-Ende-verschlüsselte Kommunikation richten. Erforderlich ist ein Mittel zur Zweckerreichung dann, wenn kein milderes Mittel in Frage kommt oder ein milderes Mittel zur Zweckerreichung nicht gleich geeignet erscheint.

   Der Kommissionsvorschlag sieht mit der sogenannten Aufdeckungsanordnung in Artikel 7 ff. CSAM-E einen Mechanismus vor, nach dem auf Antrag der national einzurichtenden Koordinierungsbehörden von einem Gericht oder einer unabhängigen Verwaltungsbehörde – zeitlich befristete und der Aufdeckung einer bestimmten Art von Inhalt in einem bestimmten Dienst dienende – Anordnungen erlassen werden können, bekanntes oder unbekanntes Material zu sexuellem Kindesmissbrauch oder Kontaktanbahnungen verpflichtend aufzuspüren, sodass Diensteanbieter auf Anordnung Einsicht in die Inhalte ihrer Dienste vornehmen müssen. Die Aufdeckungsanordnung stellt dabei gemäß Artikel 7 Abs. 4 CSAM-E auf einen risikobasierten Ansatz ab.

   Der Kommissionsvorschlag scheint damit in Bezug auf die Strafverfolgung von einem Erkenntnis- und Informationsdefizit auszugehen, infolgedessen die Strafverfolgungsbehörden nicht in gebotenem und deliktswirksamem Umfang tätig werden können. Dem ist zuzugeben, dass die derzeitige Strafverfolgungspraxis (zu vgl. sogleich 3.) in erheblichem Umfang von Meldungen US-amerikanischer Unternehmen an das dortige National Center for Missing and Exploited Children (NCMEC)

abhängt. Soweit für ein funktionsfähiges und umfassend rechtssicheres europäisches Äquivalent technische Instrumente wie das serverseitige Scannen unverschlüsselter (bzw. lediglich transportverschlüsselter) Nutzungsinhalte und wirksame Meldemechanismen für Endnutzer erforderlich sind, sind ähnlich wirksame, dabei aber weniger invasive Instrumente nicht ersichtlich. Dabei ist auch zu berücksichtigen, dass der serverseitige Zugriff auf unverschlüsselte Nutzungsinhalte erfolgt, bei denen die Nutzerinnen und Nutzer Dritten – den Anbietern – bewusst Zugriff auf ihre Daten einräumen und diese insoweit aus dem Kernbereich der Privat- und Intimsphäre entlassen.

Auch wenn der Kommissionsvorschlag den Begriff der „Ende-zu-Ende-Verschlüsselung“ bemerkenswert weitgehend vermeidet, ist mit Blick auf die konkrete Ausgestaltung von Artikel 10 CSAM-E auch davon auszugehen, dass die Kommission (vor allem) den vor- oder nachgelagerten Zugriff auf verschlüsselte Kommunikation durch geräteseitigen Zugriff auf die Inhalte als Mittel zur Mitigation eines besorgten Zugriffsausschlusses für die Strafverfolgungsbehörden in den Blick genommen hat.

Ende-zu-Ende-verschlüsselte Kommunikation stellt für die Strafverfolgungsbehörden prinzipienbedingt eine besondere Erschwernis dar, da sie – lege artis implementiert – den Zugriff auf die für die Ermittlungen erforderlichen Informationen im Sinne von Klarkommunikationsdaten wirksam einschränkt. Gleichwohl erweist sich Ende-zu-Ende-Verschlüsselung von Täterkommunikation im hier betrachteten Deliktsfeld des netzkonnexen Kindesmissbrauchs nur in einer deutlich untergeordneten Zahl von Fällen als durchgreifendes Ermittlungshemmnis. Es muss dabei dahinstehen, ob dies vornehmlich wirksamen Ermittlungsmethoden, mangelnder technischer Affinität der Täterklientel oder sonstigen technischen Ursachen wie der Bandbreitenlimitation verschlüsselter Kommunikationswege für Multimediadaten geschuldet ist. Dabei muss auch die Erkenntnisbreite in den Blick genommen werden, die durch eine Kombination der Feststellungen aus serverseitiger Überwachung, aus den Ermittlungsverfahren selbst und aus Hinweisen Dritter (s. o.) erlangt werden kann.

In ihrer Akzentuierung entfernt sich die Kommission zumindest in Bezug auf Ende-zu-Ende-verschlüsselte Kommunikation in erheblichem Maße von der Realität der Strafverfolgungspraxis. Deren zentrales Hemmnis ist nicht ein Mangel an verschlüsselungsbedingt nicht erkannten Straftaten, tatrelevanten Plattformen oder deliktsspezifischen konkreten Verbreitungswegen.

Vielmehr besteht ein strukturelles Handlungsdefizit durch eine unzureichende technische und personelle Ausstattung der Strafverfolgungsbehörden. Diese Mängel

zeigen sich auf fast allen Ebenen des strafrechtlichen Ermittlungsverfahrens. Überlange Auswertedauern digitaler Beweismittel von teils mehrjähriger Länge verhindern den zeitgerechten Ermittlungsfortschritt. Die unzureichende Verfügbarkeit spezialisierter polizeilicher Ermittlungsteams führt zu einer lediglich konsekutiven Bearbeitung aktueller Erkenntnisse. Technisch und fachlich hochqualitative, im Einzelfall auch Verschlüsselung neutralisierende und parallelisierte Ermittlungsarbeit wird durch die Ressourcenlimitation so eingegrenzt, dass Quantität und Qualität der strafprozessualen Ermittlungsarbeit deutlich hinter dem bei adäquater Ausstattung Machbaren zurückbleiben müssen. Der gesetzlich zulässige Handlungsrahmen der Strafprozessordnung kann aus Gründen der Ausstattungsknappheit nicht in jedem Fall sachgerecht ausgeschöpft werden. Aus den Kontakten der ZAC NRW auf bundes- sowie auf internationaler Ebene ergibt sich überdies, dass diese Zustandsbeschreibung nicht auf den Zuständigkeitsbereich der Zentralstelle begrenzt ist, sondern eine grundlegende Problemstellung darstellt.

In spiegelbildlicher Betrachtung ist die Ertüchtigung der Strafverfolgungspraxis ein mindestens ebenso gut geeignetes, jedoch im Vergleich jedenfalls zum *client side scanning* erheblich weniger invasives Mittel zur Erreichung der angestrebten Verbesserung der Strafverfolgung netzkonnexer Straftaten des Kindesmissbrauchs im weiteren Sinne. Im Zuge der Bearbeitung des bedeutsamen Missbrauchskomplexes „Bergisch Gladbach“ hat sich die mit seiner Bewältigung beauftragte ZAC NRW seit 2020 organisatorisch neu aufgestellt. Sie wurde personell deutlich verstärkt und hat mit der „Task Force zur Bekämpfung des Kindesmissbrauchs und der Verbreitung von Kinderpornografie in digitalen Medien“ eine spezialisierte Abteilung eingerichtet. Mittlerweile werden in Zusammenarbeit mit dem Landeskriminalamt Nordrhein-Westfalen sämtliche Meldungen ausländischer Meldepartner wie des US-NCMEC landeseinheitlich durch die ZAC NRW gesichtet und erstbearbeitet. Daneben sind Sonderdezernate für Ermittlungen gegen Plattformen und Infrastrukturen, die Kindesmissbrauch im Netz ermöglichen und fördern, eingerichtet worden. Auch durch diese Maßnahmen ist es – neben anderen Faktoren wie dem grundsätzlich gestiegenen Meldeaufkommen – gelungen, die Zahl der Verfahren der Zentralstelle im gesamten Deliktsfeld des dreizehnten Abschnitts des Besonderen Teils des Strafgesetzbuchs gegen bekannte Täter im Jahresvergleich 2021 zu 2022 mehr als zu verdoppeln und die gegen unbekannte Täter sogar zu versechsfachen. Dabei ist davon auszugehen, dass sich das zugrundeliegende Deliktsphänomen nicht wesentlich gewandelt hat, die Strafverfolgungsbehörden jedoch durch ihre verbesserte Aufstellung einen deutlich gestiegenen Anteil des sogenannten Dunkelfelds haben erhellen können. Diesen Weg auch europäisch konsequent weiterzugehen, würde mit Blick auf die Belange der Strafrechtspflege ei-

nen mindestens ebenso wirksamen Beitrag wie eine uneingeschränkte Aufdeckungsanordnung leisten, ohne dass jedoch mit einem lediglich risikobasierten Instrument wie der genannten Anordnung der Grundpfeiler der Strafverfolgung (nur) bei zureichenden tatsächlichen Anhaltspunkten für eine konkrete Straftat („Anfangsverdacht“, zu vgl. § 152 Abs. 2 StPO) verlassen werden müsste. Konkrete, wirksame, jedoch stets anlassbezogene Strafverfolgung dürfte im Vergleich zu einer risikobasierten Generalintervention auch in Ende-zu-Ende-verschlüsselte Kommunikationsinfrastrukturen ein deutlich milderes, jedoch (mindestens) ebenso geeignetes Mittel zur verbesserten Bekämpfung des netzkonnexen Kindesmissbrauchs darstellen.

d) Soweit in Bezug auf serverseitiges Scannen unverschlüsselter Nutzungsinhalte die Erforderlichkeit von Aufdeckungsanordnungen mit gut vertretbaren Argumenten bejaht werden kann, müsste sich eine solche Maßnahme auch als verhältnismäßig im engeren Sinne erweisen. Dazu müssten die relevanten Grundrechtseingriffe nicht außer Verhältnis zum verfolgten Zweck stehen. Zu Recht weist der Wissenschaftliche Dienst des Deutschen Bundestags in seiner Ausarbeitung vom 7. Oktober 2022 (WD 10 - 3000 - 026/22), auf die zur Vermeidung von Wiederholungen Bezug genommen wird, darauf hin, es erscheine unwahrscheinlich, „dass eine grundsätzliche Überwachung von Individualkommunikation der Überprüfung der (europäischen) Grundrechte standhalten würde. […] Ausgehend von den genannten Aspekten und Problemen, sieht der aktuelle Verordnungsentwurf unverhältnismäßige Eingriffe in die geprüften Grundrechte der GRCh vor“ (zu vgl. Abschnitt 6 der Ausarbeitung).

   Dabei hebt die Ausarbeitung indes vornehmlich auf Schwächen KI-basierter Lösungen ab und stellt deren Fehleranfälligkeit heraus. Es dürfte sich jedoch empfehlen, in Bezug auf das serverseitige Scannen unverschlüsselter Nutzungsinhalte auf das präzise Detektionsverfahren digitaler Fingerabdrücke, sogenannter Hashes, abzustellen. Über diese lässt sich prinzipienbedingt nur bereits bekanntes und als solches klassifiziertes Missbrauchsmaterial erkennen, da Hashverfahren anders als KI-Lösungen auf die Wiedererkennung bekannten Materials setzen, während die Künstliche Intelligenz auch unbekanntes Missbrauchsmaterial detektieren soll. Mit Hash-Lösungen werden die Schwächen KI-basierter Lösungen vermieden, um den Preis, unbekannte, da neu generierte Inhalte auszublenden. In grundrechtlicher Hinsicht dürfte durch ein solches rein automatisiert vergleichendes und nicht bewertendes Verfahren eine deutlich minimierte und im Ergebnis angemessene Eingriffsintensität erreicht werden. Das aus Sicht der Strafverfolgungsbehörden zwangsläufig entstehende Entdeckungsdelta in Bezug auf unbekanntes Missbrauchsmaterial kann dabei auf Grundlage der zu c) ausgeführten Ertüchtigung der

Strafverfolgungsbehörden wirksam geschlossen werden, da im weit überwiegenden deliktstypischen Regelfall – zumindest komplementär – Tatverdächtige auch bekannte Kindesmissbrauchsinhalte verbreiten und besitzen. Effektive Ermittlungsarbeit der Strafverfolgungsbehörden auf Basis der durch ein serverseitiges Scannen anhand von Hashwerten gewonnenen Erkenntnisse dürfte sich als hinreichend wirksame Maßnahme erweisen, im Zuge der Ermittlungen selbst auch denjenigen auf die Spur zu kommen, die unbekanntes Missbrauchsmaterial herstellen und/oder verbreiten, ohne dass es dafür der weit invasiveren Methode eines bewertenden KI-Einsatzes und der Durchbrechung von Verschlüsselung bedarf. Sofern es dem EU-Zentrum gelingt, einen wirksamen, unbürokratischen und zeiteffektiven Weg der Pflege entsprechender Hashdatenbanken einzurichten, dürfte darüber hinaus in Wechselwirkung mit den aufgrund von Meldungen pp. geführten Ermittlungsverfahren die Hashfilterqualität laufend zunehmen.

Aus Sicht einer Cybercrime-Zentralstelle ist schließlich und vorsorglich in Bezug auf die Abwägungskriterien der Angemessenheitsprüfung mit Blick auf die Ende-zu-Ende-Verschlüsselung deren überragende Bedeutung für die Informationssicherheit zu betonen. Ende-zu-Ende-Verschlüsselung ist für die digitale Kommunikation das einzige wirksame Mittel, deren Vertraulichkeit zu schützen. Sie stellt damit nicht nur für Privatpersonen, sondern auch für Unternehmen, Behörden und nicht zuletzt die Strafverfolgung – besonders geschützte Berufsgruppen wie Strafverteidiger eingeschlossen – die wichtigste digitale Schutzmaßnahme dar. Verschlüsselung ist aus technischer Sicht entweder wirksam oder kompromittiert. Geschwächte oder durch ein Instrument wie die Aufdeckungsanordnung strukturell unterminierte Verschlüsselung ist faktisch keine Verschlüsselung. Die Vorschläge der Kommission implementieren eine grundsätzliche Sollbruchstelle und sind in Bezug auf inhaltsverschlüsselte Kommunikation auch aus diesem Gesichtspunkt unverhältnismäßig.

2. <u>EU-Zentrum</u>

Zu begrüßen ist aus Sicht der Strafverfolgungspraxis eine verbesserte europäische Zusammenarbeit der Ermittlungsbehörden. Ein EU-Zentrum kann hierbei einen wesentlichen Beitrag bilden. Dies gilt zunächst für die Gewährleistung einer vereinheitlichten europäischen Erkenntnispraxis. Wünschenswert wäre darüber hinaus ein stärkerer operativer Akzent der Aufgaben des Zentrums aus Artikel 43 des Vorschlags. Dabei soll nicht verkannt werden, dass der Kommissionsvorschlag an verschiedenen Stellen auf die Zusammenarbeit des EU-Zentrums mit Europol abstellt. Gleichwohl bedarf die europäische Strafverfolgungspraxis eines deutlich gesteigerten Anteils an europäischer Koordinierung und originärer Initiative.

Zudem wäre zu befürworten, wenn auch die justizielle Seite der Strafverfolgung durch eine geeignete Einbindung – etwa über Eurojust – stärkere Berücksichtigung erführe. Denn es dürfte davon auszugehen sein, dass nur durch einen Strafverfolgungsverbund jenseits einer rein polizeilichen Aufstellung ein wirksamer europäischer Strafverfolgungsimpuls gesetzt werden kann.

Ferner könnte es sich empfehlen, dem EU-Zentrum allein oder in Zusammenarbeit mit Europol den konkreten Auftrag einer europäischen Koordinierung der Strafverfolgung bei internetkonnexer Kindesmissbrauchskriminalität zuzuweisen. Die derzeitigen Mechanismen erweisen sich in der Strafverfolgungspraxis als unzureichend. So ist etwa kaum sichergestellt, dass bei staatenübergreifend relevanten Plattformen, über die inkriminiertes Material ausgetauscht und Taten initiiert oder kommuniziert werden, die Strafverfolgungsbemühungen der europäischen Mitgliedsstaaten sachgerecht abgestimmt und die relevanten Erkenntnisse in einem einfachen und zugänglichen Verfahren untereinander ausgetauscht werden. Multinationale sogenannte Joint Investigation Teams werden nur verfahrens- nicht aber phänomenbezogen perpetuiert aufgestellt, obschon es sich bei als besonders relevant erkannten Kriminalitätsbildern wie dem internetkonnexen Kindesmissbrauch empfehlen könnte, „stehende“ multinationale Ermittlungseinheiten zu etablieren. Wenngleich dem EU-Zentrum nach dem Kommissionsvorschlag eine eher beratende, unterstützende und verwaltungsexekutive Funktion zufallen soll, ist die Gesetzgebungsinitiative – auch unter Berücksichtigung der europäischen Gesetzgebungszuständigkeiten – aus Sicht der Strafverfolgungspraxis ohne konkrete Strafverfolgungsbezüge unzureichend.

3. Meldepflicht

Anbieter, die Online-Inhalte mit sexuellem Kindesmissbrauch aufgespürt haben oder denen solche Inhalte sonst bekannt geworden sind, sollen verpflichtet werden, diese an das EU-Zentrum zu melden. Eine solche Meldepflicht ist aus Sicht der Strafverfolgung uneingeschränkt zu begrüßen. Nach der derzeitigen Praxis sind Meldungen des US-NCMEC von herausragender Bedeutung und machen den weit überwiegenden Teil der zur Einleitung von Ermittlungsverfahren Anlass gebenden Sachverhalte aus. Hier ein europäisches Institut einzurichten, dürfte sowohl die Meldegrundlagen erheblich verbreitern als auch den meldenden Anbietern über den Geltungsbereich der US-Gesetzgebung hinaus eine tragfähige Rechtsgrundlage verschaffen.

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?

Die ZAC NRW erforscht mit Partnern aus Wissenschaft und Wirtschaft seit 2017 Möglichkeiten des Einsatzes künstlicher Intelligenz zur automatisierten Detektion kinder- und jugendpornografischer Inhalte in digitalen Beweismitteln. Diese Erfahrungen dürften auch auf den Bereich der automatisierten Erkennung bei internetgestützter Kommunikation zu übertragen sein. Die Herausforderung des Einsatzes automatisierter Erkennung bestehen insbesondere in einem sorgsamen Austarieren des jeweiligen Detektionsfokus. Das eingesetzte Tool soll möglichst wenige inkriminierte Inhalte verpassen („false negative“) und dabei möglichst wenige strafrechtlich unbedenkliche Inhalte zu Unrecht erfassen („false positive“). Beide Erkennungsziele widersprechen einander. Wollte man den Fokus besonders auf möglichst wenige falsch-positive Fehlerkennungen richten, liefe man Gefahr, signifikante Anteile inkriminierter Kommunikation nicht zu erkennen. Umgekehrt würde eine möglichst hohe Detektionsrate tatsächlich inkriminierter Inhalte zwangsläufig mit einer erhöhten „false positive“-Rate einhergehen. Daher ist die Gefahr, dass unbescholtene Bürgerinnen und Bürger durch falsch-positive automatisierte Erkennung unter Verdacht geraten, nicht statisch zu quantifizieren. In dem von der ZAC NRW mit Partnern entwickelten KI-Tool AIRA („AI-enabled rapid assessment“) werden derzeit mehr als 90% der relevanten inkriminierten Inhalte bei einer „false positive“-Rate im mittleren bis unteren einstelligen Prozentbereich erkannt. Übertragen auf den Prozess der Aufdeckungsanordnung und die Vielzahl der insoweit prozessierten Inhalte ist die Gefahr, dass unbescholtene Bürgerinnen und Bürger von behördlichen Ermittlungen betroffen werden, signifikant. Dies gilt insbesondere auch mit Blick auf KI-basierte Falscheinstufungen von Sachverhalten, bei denen das reine Bildmaterial zutreffend erkannt, der strafrechtliche Gehalt aber verkannt wird. Zu nennen sind etwa Fälle von Eigenpostings von Kindern als nicht strafmündige Personen oder Kommunikation Jugendlicher in einvernehmlichen Zusammenhängen (zu vgl. § 184c Abs. 4 StGB).

Falsch-positive Meldungen sind für die Ermittlungsbehörden im Ergebnis eine Ressourcenfehlallokation, da tatsächlich ein Anfangsverdacht nicht gegeben ist. Der CSAM-E sieht für eine Vorfilterung indes das EU-Zentrum vor, so dass davon auszugehen ist, dass der Ressourcenmehraufwand dort zu tragen sein wird. Eine Verlagerung der Vorfilterung auf das EU-Zentrum ist jedoch aus Sicht der Strafverfolgung gegebenenfalls mit weiteren Risiken verbunden. Denn wenn dort für sich genommen straflose Inhalte, die bei wertender Betrachtung unter Berücksichtigung einer krimina-

listischen Beurteilung indikatives sogenanntes Präferenzmaterial darstellen, ausgefiltert werden sollten, dürften für die Strafverfolgung relevante Erkenntnisse verloren gehen.

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?

Solche Technologien sind im Bereich der Forschungszuständigkeit der ZAC NRW nicht bekannt geworden. Soweit die Zentralstelle bislang Technologien zum semantischen Textverständnis erprobt hat, haben diese Tests zwar interessante und durchaus vertiefbare Ansätze erbracht, deren Praxiseinsatz in vertretbarer Qualität jedoch nicht kurz- oder mittelfristig zu erwarten steht.

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

Auf die Ausführungen zu Frage 3 Abschnitt 1 wird Bezug genommen. Anstelle einer weitreichenden und lediglich risikobasierten Intervention in Ende-zu-Ende-verschlüsselte Kommunikationsinfrastrukturen sollten vor allem anlassbezogene, das heißt von einem konkreten Anfangsverdacht getragene und zielgerichtete Ermittlungsmaßnahmen in den Blick genommen werden. Daneben empfiehlt sich ein hashbasiertes, serverseitiges Scanverfahren für unverschlüsselte Nutzungsinhalte.

Ergänzend dürfte etwa die Implementierung einer tragfähigen Rechtsgrundlage für die effektive und vollständige Entfernung und Löschung inkriminierter Inhalte – und nicht lediglich deren Sperrung – in Erwägung zu ziehen sein, soweit die nationalen Rechtsordnungen eine solche Grundlage im Strafverfahrensrecht nicht vorsehen.

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?

Zur Frage der Ausgestaltung der Altersverifikation und diesbezüglicher technischer Ansätze besteht hier keine besondere Sachkunde. Aus Sicht einer in weitem Umfang Open-Source-Software einsetzenden technischen Dienststelle ist auf die Implikationen der verpflichtenden Altersverifikation für das Open-Source-Ökosystem hinzuweisen. Eine verpflichtende Altersverifikation bei weitem Verständnis des Begriffs des „Appstores“ dürfte etwa von Linux-Distributionen kaum rechtssicher zu bewältigen sein. Insoweit droht über den Eingriff in das Distributionssystem auch deutlicher Kollateralschaden für die Strafverfolgungspraxis selbst.

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?

Die für die Umsetzung der Aufdeckungsanordnungen zu implementierenden Techniken bergen das Risiko des Missbrauchs. Dies gilt zunächst für den nach kriminalistischer Erfahrung nicht aus dem Blick zu verlierenden „Innentäter“, der – kriminell oder drittstaatlich induziert – den Zugang zu Inhalten der Nutzer missbräuchlich nutzt. In technologischer Hinsicht unterminiert jegliches Client Side Scanning den Schutz durch Ende-zu-Ende-Verschlüsselung. Die dafür erforderlichen Schnittstellen auf den Endgeräten der Nutzer bzw. in der dort installierten Software können missbraucht werden. Zwar kann nicht verkannt werden, dass der Kommissionsvorschlag technologieoffen formuliert worden ist und daher eine auch nur grob konkretisierte Abschätzung der Risiken derzeit kaum möglich ist. Die Praxis der Strafverfolgung bestätigt indes die These, dass geschaffene technische Risiken mit Sicherheit bei unsicherer Zeitkomponente in Kompromittierung münden: Was gehackt werden kann, wird auch gehackt werden. Es ist daher aus Sicht der Informationssicherheit von einem gesteigerten Risiko auszugehen.

Hinsichtlich der Signalwirkung für autoritäre Staaten besteht hier eine besondere Sachkunde nicht.

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?

Hierzu besteht keine besondere Expertise, so dass von einer dezidierten Stellungnahme abgesehen wird. Dass „Privatsphäre“ den „Kinderschutz“ nicht hindern muss, ist bereits in den Ausführungen zu Frage 3 Abschnitt 1 deutlich gemacht worden. Wegen der Auswirkungen auf die IT-Sicherheit der durch Kinder genutzten Systeme wird ergänzend auf die Beantwortung zu Frage 8 Bezug genommen.

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?

An politische Maßnahmen ist zunächst im Bereich der Ertüchtigung und Stärkung der Strafverfolgungsbehörden zu denken. Die Effektivität der Bekämpfung des Kindesmissbrauchs und der Verbreitung von Missbrauchsdarstellungen im Netz bestimmt sich nicht zuletzt durch den tatsächlichen Einsatz finanzieller, technischer und personeller Ressourcen. Auf die Beantwortung zu Frage 3 Abschnitt 1 wird insoweit Bezug genommen. Gleichzeitig zeigen die Verbesserungen der Handlungsfähigkeit der Strafverfolgungsbehörden – etwa im Bereich der ZAC NRW – die Wirksamkeit der insoweit eingesetzten Ressourcen.

In nationaler gesetzgeberischer Hinsicht dürfte als ein bedeutsames Problem die Nachfolgeregelung der sogenannten Vorratsdatenspeicherung anzusehen sein. Die Möglichkeit einer Zuordnung von IP-Adressen zu Anschlüssen oder Geräten ist bei der Bekämpfung des Kindesmissbrauchs im Netz ein wichtiges Ermittlungsinstrument. Ohne mit Blick auf die hohe gesellschaftliche und rechtspolitische Relevanz des Themas den Rahmen der Fragestellung überspannen zu wollen, dürfte es sich empfehlen, ein intelligentes und grundrechtsschonendes Konzept jenseits der überkommenen und durch den EuGH verworfenen „Vorratsdatenspeicherung“ hin zu einer begrenzten IP-Zuordnung umzusetzen. Der Zugriff auf die ermittlungsrelevanten Daten sollte über entsprechende Schnittstellen bei den Anbietern und Providern rein digital abgebildet und dabei so beschleunigt werden, dass für den häufigen Fall accountgebundener

Missbrauchskriminalität auf die Live-Ausleitung aktueller IP-Daten ohne eine retrograde Speicherung zurückgegriffen werden kann. Für den verbleibenden Kriminalitätsbereich dürfte das vorstehende Konzept der „Login-Falle“ um eine zeitlich sehr begrenzte und damit grundrechtsschonende Speicherdauer für IP-Zuordnungsdaten etwa in der zeitlichen Ausdehnung der derzeitigen Speicherung für Zwecke der Netzsicherheit und der Störungsbeseitigung von einer Woche zu erweitern sein. Eine solche Neuregelung einer begrenzten IP-Zuordnung wäre ein grundrechtssensibler, jedoch weitgehend praxistauglicher Beitrag für verbesserte Ermittlungsmöglichkeiten bei Kindesmissbrauch und der Verbreitung entsprechender Darstellungen im Internet.

Auf europäischer Ebene ist eine Verbesserung der internationalen Zusammenarbeit dringend empfohlen. Die entsprechenden Potentiale und Synergien werden derzeit nicht in dem erforderlichen Ausmaß gehoben. Auf die Beantwortung zu Frage 3 Abschnitt 2 wird ergänzend Bezug genommen.

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?

Auf die Antwort zu Fragen 2 und 3 wird Bezug genommen. Dabei erscheint eine zielgerichtete Erfassung nur spezifischer Plattformen – ungeachtet der Schwierigkeit bei der Festlegung geeigneter Abgrenzungskriterien und der Praxiserfahrung, dass nahezu alle Plattformen auch im Deliktskontext genutzt werden – aufgrund der insbesondere unter dem Gesichtspunkt der Erforderlichkeit und Angemessenheit der Aufdeckungsanordnung dargestellten Bedenken weder geeignet noch ausreichend, um die verfassungsrechtlichen Mängel des Kommissionsvorschlags aufzuwiegen.

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?

Auf die Antwort zu Fragen 3, 6 und 10 wird Bezug genommen.

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?

Eine Verbesserung der internationalen Zusammenarbeit auf europäischer Ebene wird ausdrücklich befürwortet. Die aktuellen Planungen einer umfassenden und anlasslosen Überwachung digitaler Kommunikation stellen sich aus Sicht der Strafverfolgungsbehörden im Ergebnis nicht als uneingeschränkt rechtskonformes Instrument zur besseren Strafverfolgung und Rechtsdurchsetzung dar. Vorzugswürdig erscheint, dem EU-Zentrum die Aufgabe eines Kompetenz- und Koordinierungszentrums zuzuweisen. Auf die Beantwortung zu Frage 3 Abschnitt 2 wird insoweit Bezug genommen.

Dies macht aus Sicht der Strafverfolgungsbehörden – mit Blick auf die bereits derzeit unzureichende Ausstattung – eine personelle Verstärkung auch national unabdingbar, da andernfalls zweifelhaft erscheint, dass die Strafverfolgungsbehörden der Mitgliedstaaten über ausreichend Ressourcen, insbesondere hinreichend geeignetes Personal, verfügen, das sie für eine Tätigkeit im EU-Zentrum abordnen könnten. Auf die Antwort zu Frage 3 Abschnitt 1 lit. c) wird Bezug genommen.

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?

Auf die Antwort zu Fragen 3 und 6 wird Bezug genommen.

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?

Die bisherigen Erfahrungen der Strafverfolgungspraxis mit Netzsperren sind begrenzt. Die Strafprozessordnung sieht ein solches Instrument nicht vor. Aus technischer Sicht sind solche Maßnahmen leicht zu umgehen. Soweit die Frage auf die Sperrung auf Ebene deutscher bzw. nationaler Zugangsprovider abstellt, ist hier kein wirksamer Mechanismus „unter“ dem Domain-Level bekannt. Aus Sicht der Strafverfolgung ist eine Sperrung ohnehin unzureichend, da nicht der Zugang zu inkriminierten Inhalten begrenzt, sondern diese selbst gelöscht und die solches Material verbreitenden Personen strafrechtlich verfolgt werden sollten. Es gilt „verfolgen statt nur sperren“.

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?

Hinsichtlich der wünschenswerten Rolle des EU-Zentrums wird auf die Antwort zu Frage 3 Abschnitt 2 Bezug genommen. Soweit die Frage auf ein mögliches Glaubwürdigkeitsproblem des EU-Zentrums im Bereich seiner präventiven Aufgaben abstellt, dürften die präventiven Aufgaben durch die Zuständigkeiten im Rahmen der Entwicklung und des Einsatzes von „technischen Überwachungswerkzeugen“ nicht gehindert sein. Das Beispiel der Polizei zeigt, dass Repression neben Prävention möglich ist. Entscheidend ist vielmehr, dass beide Aufgaben in verhältnismäßiger und gesellschaftlich akzeptierter Weise ausgeübt werden. Im Übrigen dürfte davon auszugehen sein, dass angesichts der Größe des EU-Zentrums geeignete betriebsorganisatorische Maßnahmen ergriffen werden können.

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?

Im Einklang mit §§ 100a ff. StPO sind bestimmte technische Ermittlungsinstrumente zulässig. Ihnen gemein ist der anlassbezogene Einsatz bei bestimmten hohen rechtlichen Hürden. Eine anlasslose, „algorithmische“ Überwachung und Durchbrechung von Ende-zu-Ende-verschlüsselter Kommunikation dürfte unverhältnismäßig sein. Auf die Antwort zur Frage 3 Abschnitt 1 wird Bezug genommen.

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 Jugendli-

chen, 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?

Über das methodische Vorgehen des EU-Zentrums gibt es hier – zumal vor seiner Einrichtung – keine Erkenntnisse. Zu unterscheiden sein dürfte hinsichtlich bekannten und bereits klassifizierten Missbrauchsmaterials und der Detektion unbekannter und gleichwohl relevanter Inhalte. Hinsichtlich der ersten Fallgruppe sind (etablierte) Techniken wie scharfe und unscharfe Hashverfahren relevant, deren Datenbankpflege gemäß Artikel 43 Abs. 2 lit. b) CSAM-E ebenfalls zu den Aufgaben des EU-Zentrums gehören soll. In Bezug auf unbekanntes Material erscheint es technisch möglich, verbindliche Indikatoren im Sinne bestimmter KI-Klassifikatoren und deren jeweiliger Wahrscheinlichkeitswerte zu entwickeln, ab wann ein Inhalt als mutmaßlich inkriminiert zu gelten hat. Ohne eine menschliche, wertende und juristisch wie kriminalistisch kompetente Nachschau der als relevant identifizierten Fälle dürfte eine verlässliche Identifikation strafrechtlich relevanter Fälle allein auf KI-Basis nicht möglich sein.

22. Februar 2023

[elektronisch ohne Unterschrift übermittelt]
(Hartmann)
Leitender Oberstaatsanwalt
Leiter der ZAC NRW