Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)138

28.02.2023

Bonn, den 28.02.2023

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestages
am Mittwoch, 1. März 2023, 14:00 bis 16:00 Uhr

zum Thema „Chatkontrolle“

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Vorbemerkung

Die Bekämpfung des sexuellen Kindesmissbrauchs ist eine überragend wichtige gesellschaftliche Aufgabe, die es mit allen zur Verfügung stehenden geeigneten und angemessenen Mitteln zu erfüllen gilt. Die sogenannte Chatkontrolle schießt aber deutlich über das Ziel dieser Aufgabe hinaus. Sie bietet kaum einen größeren Schutz für Kinder, sondern wäre stattdessen Europas und Deutschlands Einstieg in eine unverhältnismäßige anlasslose und flächendeckende Überwachung der privaten Kommunikation.

Als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit ist mir der Schutz der Bürgerinnen und Bürger vor ungerechtfertigten und unverhältnismäßigen Eingriffen insbesondere in das Recht auf informationelle Selbstbestimmung, das Fernmeldegeheimnis und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme äußerst wichtig. Der Verordnungsentwurf führt meines Erachtens zu nicht zu rechtfertigenden Eingriffen in die in der EU-Grundrechte-Charta und dem Grundgesetz verbrieften Grundrechte.

Als besonders gravierend ist hervorzuheben, dass der Entwurf im Ergebnis das Ende der vertraulichen Kommunikation festschreibt, sei es durch Aufbrechen der Ende-zu-Ende-Verschlüsselung oder durch das sogenannte Client-Side-Scanning.

Der Verordnungsentwurf sieht verpflichtende Alterskontrollen durch App- und Software-Stores und teilweise sogar den über heutige Regelungen weit hinausgehenden Ausschluss bestimmter Altersgruppen von Software-Anwendungen vor. Dies führt im Ergebnis zu einer faktischen Beschränkung der Kommunikation und gefährdet die wichtige Möglichkeit, das Internet anonym oder pseudonym nutzen zu können. Ein Aufheben der Anonymität hätte in vielen Ländern insbesondere für Oppositionelle oder Whistleblower schwerwiegende Folgen, innerhalb und außerhalb der Europäischen Union.

Die Technologien, die zum Auffinden des CSA-Materials eingesetzt werden sollen, weisen zum Teil noch Fehlerquoten von bis zu 12 % auf.[1] Alleine für Deutschland betrachtet hätte bei einem Dienst wie beispielsweise WhatsApp mit insgesamt circa 65 Millionen deutschen Nutzenden bis zu 7,8 Millionen zu Unrecht der Verbreitung von CSA/Material verdächtigte bzw. beschuldigte Personen zur Folge.[2] Kriminelle dagegen können die Maßnahmen leicht umgehen und bleiben unerkannt.

[1] Commission Staff Working Document, Impact Assessment Report vom 11. Mai 2022, SWD(2022) 209 final, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52022SC0209&qid=1652763997858.
[2] Siehe Bundesnetzagentur, Nutzung von Online-Kommunikationsdiensten in Deutschland – Ergebnisse der Verbraucherbefragung 2021, abrufbar unter https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2022/20220127_Onlinekommunikation.html.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Zur Bekämpfung des sexuellen Kindesmissbrauchs sollten effektive und zielgerichtete Maßnahmen umgesetzt werden. Eine anlasslose und unverhältnismäßige Massenüberwachung gehört nicht dazu. So etwas kennen wir ansonsten nur aus autoritären Staaten. Einmal eingeführt, droht auch in Europa eine Ausweitung der überwachten Inhalte. Das zeigen die Erfahrungen der Einführung anderer Überwachungsmaßnahmen. Ich setze mich daher eindringlich dafür ein, dass die Chatkontrolle in dieser Form nicht verabschiedet wird.

Im Folgenden beantworte ich gerne den Fragenkatalog aus datenschutzrechtlicher Sicht.

Fragenkatalog

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 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (VO-E) hat tiefgreifende Implikationen für das Datenschutzniveau in der EU und insbesondere für den Schutz der Vertraulichkeit der Kommunikation und den Schutz der Privatsphäre in der Kommunikation.

   Der Verordnungsentwurf ist meines Erachtens weder mit dem Recht auf Achtung des Privatlebens nach Artikel 7 noch mit dem Recht auf Schutz personenbezogener Daten nach Artikel 8 der EU-Grundrechte-Charta (GRCh) vereinbar. Soweit man ihn an grundgesetzlichen Regelungen zu messen hätte, wäre der Entwurf weder mit dem Fernmeldegeheimnis nach Artikel 10 Grundgesetz (GG), noch dem Recht auf informationelle Selbstbestimmung vereinbar, welches sich aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz herleitet.

   Vorweg möchte ich auf den weiten Anwendungsbereich des Verordnungsentwurfs hinweisen, da er – wie unter Frage 2 weiter ausgeführt wird – im Ergebnis fast die gesamte Online-Kommunikation betrifft und es sich per definitionem schon nicht um gezielte Maßnahmen handelt. Erschwerend kommt hinzu, dass im Vergleich zur (unzulässigen) Vorratsdatenspeicherung nicht nur Verkehrsdaten – also Angaben darüber, wer mit wem wann kommuniziert hat – erfasst sind, sondern darüber hinaus auch und gerade die Inhalte der privaten Kommunikation selbst.

   Im Folgenden möchte ich einige datenschutz(grund)rechtlich wichtige Implikationen durch die im Verordnungsentwurf vorgesehenen Maßnahmen beleuchten:

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

1.1. Pflicht zur Risikobewertung

Artikel 3 bis 6 VO-E verpflichten Diensteanbieter zur Durchführung einer Bewertung des Risikos, dass ihre Dienste für die Verbreitung von Material über sexuellen Kindesmissbrauch (CSA-Material) oder für die Kontaktanbahnung (Grooming) missbraucht werden könnten. Darauf aufbauend sollen Diensteanbieter verpflichtet werden, hinreichende Maßnahmen zur Minderung des festgestellten Risikos zu treffen.

Als eine Maßnahme einer Risikominimierung dürften Diensteanbieter für Nutzende verpflichtende Altersverifizierungen einführen, die eine anonyme oder pseudonyme Nutzung des Internets gefährden. Im Einzelnen dazu und hinsichtlich der weiteren Implikationen möchte ich auf meine Ausführungen zu Frage 7 verweisen.

Meines Erachtens mangelt es dem Entwurf an Normenklarheit und Bestimmtheit sowohl für Diensteanbieter als auch Nutzende, welche Parameter dieser Risikobewertung zugrunde gelegt und in welchem Maße diese gewichtet werden.

1.2. Erlass von Aufdeckungsanordnungen und Aufdeckungspflichten

Der Verordnungsentwurf sieht in Artikel 7 VO-E die Möglichkeit vor, dass nationale Gerichte oder unabhängige Verwaltungsbehörden zeitlich befristete Anordnungen zum Aufdecken von bereits bekannten sowie neuen Missbrauchsdarstellungen und „Grooming“ gegenüber bestimmten Diensten erlassen können. Dies geschieht auf Antrag nationaler Koordinierungsbehörden, die seitens der Mitgliedstaaten zu benennen sind.

Dienste, die eine solche Anordnung erhalten haben, sind nach Artikel 10 VO-E verpflichtet, Technologien zum Auffinden von CSA-Material einzusetzen. Diese Technologien sollen wirksam CSA-Material erkennen, nur zur Aufdeckung unbedingt erforderliche Informationen extrahieren, dem neuesten Stand der Technik entsprechen und hinreichend zuverlässig sein. Die genauen Indikatoren solcher Technologien soll ein noch einzurichtendes EU-Zentrum bereitstellen.

Meines Erachtens begegnet der Aspekt der Aufdeckungsanordnungen erheblichen grundrechtlichen Bedenken, da er eine Einsichtnahme der Diensteanbieter in private Kommunikations- und Informationsinhalte erfordert. Als Folge einer Aufdeckungsanordnung dürften zunächst sämtliche Inhalte aller Nutzenden eines Dienstes einer Prüfung unterzogen und gegebenenfalls verschlüsselte Kommunikation aufgebrochen werden.

Im Folgenden möchte ich gerne in gebotener Kürze darstellen, wieso das in dem Verordnungsentwurf vorgesehene Scannen auf eine Aufdeckungsanordnung hin meines Erachtens nicht mit dem Recht auf Achtung des Privatlebens nach Artikel 7 GRCh vereinbar ist.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Rechtsgrundlage des Verordnungsentwurfs ist Artikel 114 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV), wonach Festlegungen von Maßnahmen vorgesehen sind, die das Funktionieren des Binnenmarktes sicherstellen sollen. Ziel des Entwurfs ist neben der Sicherstellung des Binnenmarktes die Bekämpfung von Kindesmissbrauch im Internet.

Natürlich bestehen an der Legitimität des verfolgten Ziels, Kindesmissbrauch im Internet zu bekämpfen, keinerlei Zweifel. Jedoch bin ich davon überzeugt, dass das im Verordnungsentwurf vorgesehene Mittel des Scannens auf eine Aufdeckungsanordnung hin nicht geeignet ist, dieses Ziel zu erreichen.

Denn Täterinnen und Täter dürften die vorgesehene Maßnahme ohne überbordende Hürden technisch umgehen können, indem sie etwa nicht die Inhalte selbst, sondern Links zu in Clouds gespeicherten, verschlüsselten Dateien teilen, zu denen allein sie die Schlüssel haben und auf die sie dann z.B. über das Darknet zugreifen. Diese Vorgehensweise ist bereits bekannt und wird angewandt. Eine weitere Umgehungsmöglichkeit könnte in der technischen Manipulation des illegalen Materials derart bestehen, dass es von den automatisierten Systemen nicht mehr als solches erkannt wird. Auch das Client-Side-Scanning kann etwa durch die Verwendung manipulierter oder selbst entwickelter Software umgangen werden.

Darüber hinaus habe ich Zweifel, dass in Anbetracht der zu erwartenden schier endlosen Masse an (auch falschen positiven) Erkennungen und potentiellen Meldungen Strafverfolgungsbehörden in der Praxis nicht in der Lage sein werden, die gesammelten Daten überhaupt ressourcenmäßig in einem hinreichenden Maße weiterverwenden zu können, auch nach einer Filterung durch das EU-Zentrum.

Erhebliche Zweifel habe ich auch an der rechtlichen Erforderlichkeit der im Verordnungsentwurf vorgesehenen Maßnahmen der Kontrolle, insbesondere hinsichtlich der damit verbundenen Aufhebung der Vertraulichkeit der Kommunikation. Erforderlich ist ein Mittel, wenn es keine milderen, aber gleich geeignete Mittel gibt.

Die Maßnahmen werden wohl zwangsläufig auch Nutzende treffen, die in keinerlei Verbindung zu illegalen Handlungen stehen. Der Vorschlag droht die Ende-zu-Ende-Verschlüsselung zu durchbrechen, indem Inhalte privater Kommunikation derjenigen Dienste flächendeckend gescannt werden sollen, die von der zuständigen Behörde eine sogenannte Aufdeckungsanordnung erhalten haben. Hiervon sind keine Ausnahmen vorgesehen, auch nicht für Berufsgeheimnistragende wie Ärzteinnen und Ärzte, Psychologinnen und Psychologen, Anwältinnen und Anwälte oder staatlich anerkannte Jugend- und Sozialarbeiterinnen und -berater.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Mildere, gleich geeignete Mittel müssen auch jenseits vermeintlich einfacher technischer Lösungen (wie der in dem Verordnungsentwurf vorgesehenen Aufdeckungssoftware) gesucht werden. Dazu zählt in erster Linie eine Stärkung der Strafverfolgungsbehörden. Das bestehende Verfolgungsdefizit resultiert meines Erachtens im Wesentlichen nicht daraus, dass Strafverfolgungsbehörden zu wenig Kenntnisse über die Inhalte der Online-Kommunikation haben, sondern an strukturell unzureichender personeller und technischer Ausstattung der Strafverfolgung. Ein Mehr an Daten ist nicht erforderlich, um Kindesmissbrauch im Internet effektiv zu bekämpfen, geeigneter erscheint eine Stärkung der Maßnahmen und Strukturen, die schon heute zu beeindruckenden Erfolgen gegen die Täter und ihre Netzwerke führen. Nicht ohne Grund hat sich die Bundesregierung im Koalitionsvertrag der Forderung verpflichtet, dass die Ende-zu-Ende-Verschlüsselung nicht durchbrochen werden darf.[3] Die Verarbeitung von Daten nicht Betroffener als quasi Kollateralschaden in dem Umfang wie er von dem Verordnungsentwurf vorgesehen ist, kann in keiner Form erforderlich sein.

Jedenfalls aber stehen die Eingriffe in die Grundrechte meines Erachtens außer Verhältnis zum Beitrag zum verfolgten Ziel und sind damit nicht angemessen. Das Durchbrechen der Ende-zu-Ende-Verschlüsselung und die Kontrolle über potentiell jegliche Online-Kommunikation der EU-Bürgerinnen und -Bürger greifen in das in Artikel 7 GRCh garantierte Recht auf Achtung des Privatlebens ein. Sie greifen potentiell tief in die Intimsphäre der Betroffenen ein.

Dies gilt insbesondere vor dem Hintergrund, dass durch Aufdeckungsanordnungen, neben der Kontrolle etwa von Textnachrichten, Bildern, Videos und Dateien, auch Sprachnachrichten abgehört werden. In der deutschen Gesetzgebung wird die besondere Schutzwürdigkeit des gesprochenen Wortes durch die Vorschrift des § 201 Strafgesetzbuch (StGB) verdeutlicht, der die Verletzung der Vertraulichkeit des Wortes gesondert unter Strafe stellt. Dies unterstreicht auch der Strafrahmen der Vorschrift, der mit einer möglichen Freiheitsstrafte von bis zu drei Jahren höher liegt als der Strafrahmen für die Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen gemäß § 201a StGB (Freiheitsstrafe bis zu zwei Jahre) und für die Verletzung des Briefgeheimnisses gemäß § 202 Absatz 1 StGB (Freiheitsstrafe bis zu einem Jahr).

Meinem Kenntnisstand nach sind insbesondere die Verfahren zum Aufdecken unbekannten Materials weiterhin äußerst fehleranfällig und führen dazu, dass auch legale und alltägliche Kommunikationsinhalte Treffer auslösen können. Mir sind keine

[3] Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP), abrufbar unter: https://www.bundesregierung.de/resource/blob/974430/1990812/1f422c60505b6a88f8f3b3b5b8720bd4/2021-12-10-koav2021-data.pdf.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

hinreichend zuverlässigen Technologien bekannt, die derzeit dazu in der Lage wären, zuverlässig unbekannte illegale von legalen Inhalten zu unterscheiden.

Darüber hinaus liegt durch die geplanten Maßnahmen ein erheblicher Eingriff in das Grundrecht auf Schutz personenbezogener Daten im Sinne des Artikel 8 GRCh und – wenn man die Maßnahmen am Grundgesetz messen müsste - das Recht auf informationelle Selbstbestimmung nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG vor.

Für den Einzelnen ist nicht transparent, ob, wie und wann seine Kommunikation Gegenstand einer „Durchleuchtung“ auf Grundlage des Verordnungsentwurfs war. Meines Erachtens stellt dies einen Verstoß gegen den Transparenzgrundsatz nach Artikel 5 Absatz 1 Buchstabe a Datenschutz-Grundverordnung (DSGVO) dar, der Geltung beansprucht, weil die Regelungen der DSGVO vom Verordnungsentwurf unberührt bleiben Eine unbefangene, auf Vertraulichkeit setzende Kommunikation wird damit unmöglich. Es besteht die Gefahr, dass Nutzende von Messengerdiensten, sozialen Netzwerken oder anderen Diensten wie Clouds damit zum gläsernen Objekt werden.

Die undifferenzierte Suche nach CSA-Material und mit ihr einhergehende Datenverarbeitungen widersprechen damit auch dem Grundsatz der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c DSGVO.

Eine Rechtfertigung dieser schwerwiegenden Eingriffe erscheint mir aufgrund der deutlichen Unverhältnismäßigkeit im Ergebnis ausgeschlossen. Eine anlasslose Massenüberwachung ist auch nach der Rechtsprechung des Europäischen Gerichtshofes nicht mit der GRCh vereinbar.[4]

1.3. Meldepflichten, Entfernungsanordnungen und Sperranordnungen

Die Artikel 12 bis 18 VO-E verpflichten Diensteanbieter, erkanntes CSA-Material dem neu einzurichtenden EU-Zentrum zu melden. Entfernungsanordnungen oder Sperranordnungen dürfen meines Erachtens nicht allein von den seitens der Mitgliedstaaten einzurichtenden Koordinierungsbehörden erlassen werden könnten, sondern von Gerichten oder unabhängigen Verwaltungsbehörden. Diese Hürde wurde im aktuellen Kompromissvorschlag der schwedischen Ratspräsidentschaft gestrichen. Eine unabhängige Kontrolle entfällt damit. Durch die geplanten Eingriffe dürften regelmäßig vollendete Tatsachen geschaffen werden. Ein nachträglicher richterlicher Rechtsschutz könnte zu spät kommen und somit würde die Rechtsweggarantie leerlaufen.

[4] Siehe etwa EuGH, Urteil vom 27. Oktober 2022, Rs. C-793/19 und C-794/19 sowie EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

1.4. Fehlende datenschutzrechtliche Aufsicht

Datenschutzaufsichtsbehörden sollen sich vor dem Einsatz der jeweiligen Technologien gemäß Artikel 7 Absatz 3 VO-E nur mit unverbindlichen Stellungnahmen beteiligen können. Eine darüber hinausgehende Möglichkeit die Wahrung der Rechte der Bürgerinnen und Bürger zu gewährleisten, wie beispielsweise durch ein Veto-Recht der Datenschutzaufsichtsbehörden gegen bestimmte Technologien oder deren Einsatzszenarien, ist gerade nicht vorgesehen. Sobald eine Technologie einmal eingesetzt wird, ist eine weitere Beteiligung ebenfalls nicht mehr vorgesehen. Diese eingeschränkte Rolle der Datenschutzbehörden halte ich bei derart schwerwiegenden, drohenden Grundrechtseingriffen für absolut unzureichend.

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?*

Auf Basis von Artikel 7 VO-E dürften uneingeschränkt alle Dienste und Geräte auf denen digitale Kommunikation stattfindet oder stattfinden könnte, von den Regelungen des Verordnungsentwurfes umfasst sein. Dabei ist nach Artikel 7 Absatz 4 VO-E irrelevant, ob die Dienste tatsächlich verwendet werden um Missbrauchsmaterial auszutauschen oder ob dort Grooming stattfindet. Vielmehr genügt ein „erhebliches Risiko“, dass diese hierfür verwendet werden könnten. Damit sind etwa Hostingdienste, Stores für Softwareanwendungen oder Internetzugangsdienste vom Anwendungsbereich erfasst. Aus datenschutzrechtlicher Sicht ist besonders eklatant, dass auch persönliche Cloudspeicher vom Anwendungsbereich erfasst sind, die etwa als Backup der eigenen Fotos auf den Mobiltelefonen dienen und gerade nicht geteilt werden.

Im Ergebnis besteht eine immens weite Betroffenheit von Diensten, die zu einem Scannen der privaten Kommunikation verpflichtet werden können und eine Tragweite, die nahezu jegliche Kommunikation aller EU-Bürgerinnen und Bürger erfassen würde.

Ebenso sehe ich es als höchst problematisch an, dass in Bezug auf bestimmte Dienste jegliche private Kommunikation ausgelesen werden soll und keinerlei Ausnahmen vorgesehen sind. So erfolgt zum Beispiel keine Privilegierung der Kommunikation von Berufsgeheimnisträgern wie beispielsweise Ärztinnen und Ärzte, Psychologinnen und Psychologen oder Rechtsanwältinnen und Rechtsanwälte, die einer beruflichen Schweigepflicht unterliegen und insoweit eine Offenbarung gegenüber Dritten im deutschen Recht gemäß § 203 StGB strafbewehrt ist. Die Strafvorschrift des § 203

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Absatz 1 StGB sieht einen Strafrahmen von bis zu einem Jahr Freiheitsstrafe für das unbefugte Offenbaren von Informationen durch Berufsgeheimnisträger vor und unterstreicht damit die besondere Schutzwürdigkeit dieser Kommunikation. Auch die derzeit in Entwicklung stehende geschützten Kommunikationswege im Medizinwesen würden vermutlich diesen Überwachungsvorschriften unterliegen, so dass wesentliche Zusagen zur Vertraulichkeit nicht mehr zu halten wären.

Eine höhere Eingriffsintensität liegt auch bei dem Scannen der Kommunikation zum Zwecke der Aufdeckung der Kontaktaufnahme von Erwachsenen zu Kindern (Grooming) vor. Denn ein Scannen soll nicht nur in Bezug auf (un)bekanntes CSA-Material erfolgen, sondern es soll jegliche textliche Kommunikation ohne weitere Unterscheidungsmöglichkeit nach ihrem Inhalt ausgewertet werden. Damit dürften auch ganz alltägliche Gespräche Beteiligter jedes Alters und jeder Alterskonstellation gescannt werden.

Auch wenn die Begründung des Verordnungsentwurfs anführt, dass es sich bei einer Aufdeckungsanordnung um eine gezielte Maßnahme gegen einen konkreten Diensteanbieter handele, erfolgt in Bezug auf den jeweiligen Dienst jedoch stets ein flächendeckendes Scannen sämtlicher öffentlicher und privater Kommunikation aller Nutzenden, so dass für den jeweiligen Dienst keinesfalls von einer gezielten Maßnahme im Einzelfall gesprochen werden kann. Bei einem Dienst wie WhatsApp könnte hierbei beispielsweise sämtliche private Kommunikation aller circa 67 Millionen Nutzenden in Deutschland[5] beziehungsweise in dreistelliger Millionenhöhe von Nutzenden innerhalb der Europäischen Union ausgelesen werden.

Es ist zu erwarten, dass als Folge der permanenten und ubiquitären Überwachung auch legal Nutzende einem Hemmnis in ihrer Kommunikationsfreiheit unterliegen und insoweit das Nutzungsverhalten durch eine Art Selbstzensur beeinträchtigt wird, weil man selbst bei legalem und legitimen Verhalten wesentlich leichter als bisher in Gefahr gerät, verdächtigt und Ziel von Ermittlungsmaßnahmen zu werden.

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?*

Hierzu nehme ich Bezug auf die Ausführungen zu Frage 1 und hinsichtlich der verpflichtenden Alterskontrollen auf die Ausführungen zu Frage 7. Im Ergebnis halte ich

[5] Siehe Bundesnetzagentur, Nutzung von Online-Kommunikationsdiensten in Deutschland – Ergebnisse der Verbraucherbefragung 2021, abrufbar unter https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2022/20220127_Onlinekommunikation.html.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

eine vollständige Überarbeitung des Entwurfes für zwingend erforderlich. Insbesondere dürfen keine Mittel vorgesehen werden, die zu einem tatsächlichen Aufbrechen der Ende-zu-Ende-Verschlüsselung oder dessen Schutzwirkung (wie etwa beim Einsatz von Client-Side-Scanning) führen.

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 Fehlerquote im Hinblick auf den Anteil zu Unrecht Verdächtigter („false positives“) der Technologien zum Aufspüren von Grooming beträgt laut Folgenabschätzung der EU-Kommission circa 10% beziehungsweise bei aktuell eingesetzten Techniken sogar 12%.[6]

Das bedeutet konkret, dass beispielsweise für einen großen Messengerdienst, bei welchem monatlich 100.000 Verdachtsfälle von Grooming an das EU-Zentrum gemeldet werden könnten, circa 10.000 bis 12.000 Nutzende zu Unrecht des Groomings verdächtigt würden, obwohl es sich um zulässige, private Unterhaltungen gehandelt hat. Erst durch eine menschliche Sichtung der Verdachtsfälle und Prüfung der vollständigen Kommunikationsinhalte bei dem EU-Zentrum könnte die Fehlerhaftigkeit dieser 10.000 bis 12.000 Fälle dann herausgefunden werden. Diese – vor allem in absoluten Zahlen – hohe Quote an zu Unrecht Verdächtigten ist vor dem Hintergrund der Erforderlichkeit (siehe hierzu auch die Ausführung zu Frage 1) und des Grundsatzes der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c DSGVO sowie vor dem Hintergrund der unionsgrundrechtlich garantierten Unschuldsvermutung nicht hinnehmbar. Deshalb und gerade aufgrund der Tatsache, dass das Scannen der privaten Kommunikation nicht zielgerichtet ist, schließe ich mich der Forderung von Europäischen Datenschutzausschuss (EDSA/EDPB) und dem Europäischen Datenschutzbeauftragten (EDPS) an, dass der Einsatz von Technologien, die ein Aufspüren von Grooming ermöglichen sollen, wieder vollständig aus dem Verordnungsentwurf zu streichen.[7]

Technologien, die eingesetzt werden sollen um unbekanntes CSA-Material aufzufinden, weisen laut Folgenabschätzung der EU-Kommission zwar „nur“ eine Fehlerquote

[6] Commission Staff Working Document, Impact Assessment Report vom 11. Mai 2022, SWD(2022) 209 final, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52022SC0209&qid=1652763997858.
[7] EDPB-EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse vom 28. Juli 2022, Randnummer 76, abrufbar unter: https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

von 0,1% auf. Hinsichtlich dieser Aussage ist jedoch schon fraglich, auf welchen Metriken und Grundlagen sie beruht, insbesondere wie ein Fehler definiert wird. Selbst unter Zugrundelegung dieser behaupteten Fehlerquote, kann es im Ergebnis – vor allem bei großen Dienstanbietern – trotzdem noch zu erheblichen hohen absoluten Zahlen zu Unrecht verdächtigter Personen kommen. Auch diese Technologie sehe ich deshalb äußerst kritisch.

Aufgrund von unüberwindbaren, praktischen Limitierungen bei der automatischen Erkennung muss das Risiko einer falschen Verdächtigung schlicht als gegeben angenommen werden. Selbst bei einer in der Praxis völlig unrealistischen Spezifizität von über 99,9%, bei dem 99,9% aller unbedenklichen Inhalte korrekt als harmlos klassifiziert werden (richtig-negativ), würden 0,1% aller unbedenklichen Inhalte fälschlicherweise als problematisch, sprich als CSA-Material, klassifiziert werden. Sie wären somit falsch-positiv.

In absoluten Zahlen würde somit eine von 1000 harmlosen Inhalten fälschlicherweise als verdächtig klassifiziert werden. Berücksichtigt man nun, dass laut einer Erhebung des Statistischen Bundesamtes 88% aller 16 – 74 jährigen Deutschen Messenger verwenden,[8] führt dies zu immens hohen täglichen Fallzahlen zu Unrecht verdächtigter Personen.

Die entsprechenden Falschmeldungen und „false positives“ sowie die Durchleuchtung der persönlichen Kommunikation werden auch dazu führen, dass Nutzende die jeweiligen Dienste aus Angst vor durchgehender Überwachung nur noch eingeschränkt oder überhaupt nicht mehr nutzen (sog. „chilling effects“). Außerdem werden Nutzende durch die geplanten Maßnahmen das Vertrauen in die Integrität der betroffenen IT-Systeme verlieren.

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?*

   Mir sind keine Technologien bekannt, die verlässlich zwischen unbedenklicher, sexuell oder romantisch aufgeladener, Kommunikation und Grooming unterscheiden können.

[8] Siehe Bundesnetzagentur, Nutzung von Online-Kommunikationsdiensten in Deutschland – Ergebnisse der Verbraucherbefragung 2021, abrufbar unter https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2022/20220127_Onlinekommunikation.html.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

In Anbetracht der Komplexität sind diese auch weder kurz- noch mittelfristig zu erwarten.

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

Meinem Erkenntnistand nach gibt es keine alternativen technischen Ansätze zu den konkret im Verordnungsentwurf vorgesehenen Maßnahmen, ohne dass die Kommunikationsinhalte tatsächlich analysiert werden müssten und damit die Vertraulichkeit der Kommunikation nicht gewährleistet wäre.

Statt eines flächendeckenden Auslesens jeglicher öffentlicher und privaten Kommunikation sollte der Schwerpunkt der Maßnahmen zur wirksamen Bekämpfung vielmehr im Ausbau der Ressourcen für Strafverfolgungsbehörden sowie in der Prävention des sexuellen Kindesmissbrauchs liegen – auch außerhalb der Online-Welt. Die Prävention hat die EU-Kommission im Übrigen auch selbst zu ihrer Priorität zur Bekämpfung des sexuellen Kindesmissbrauchs erklärt.

Daneben könnten weitere Maßnahmen getroffen werden, wie etwa, dass Diensteanbieter verpflichtet werden, niedrigschwellige Meldewege für betroffene Personen einzurichten, die an Strafverfolgungsbehörden oder andere staatliche Beratungsstellten angebunden sind. In diesem Zusammenhang könnten Login-Fallen der gezielten Ermittlung und Aufklärung durch Strafverfolgungsbehörden Vorschub leisten. In diesem Verfahren könnten Diensteanbieter verpflichtet werden, nach einer Meldung und bei Feststellung eines Anfangsverdachts sowie mit richterlicher Anordnung beim nächsten Login des Verdächtigen die IP-Adresse an die Strafverfolgungsbehörden zu übermitteln.

Ergänzend zu sogenannten Login-Fallen, könnte das sogenannte "Quick Freeze"-Verfahren eine verhältnismäßige und effektive Möglichkeit darstellen, Strafverfolgungsbehörden bei der Identifizierung von Verdächtigen zu unterstützen. Hierbei werden Telekommunikationsdienste per Anordnung verpflichtet, bestimmte Verkehrsdaten nicht zu löschen und innerhalb einer angemessenen Frist bei richterlicher Anordnung aufgrund hinreichender Nachweise diese an die Strafverfolgungsbehörde zu übermitteln.

Um einmal zielgenau gesicherte Daten dann effizient für die Strafverfolgung zu erschließen, könnten die im Verordnungsentwurf benannten Technologien auf diesem Datenbestand genutzt werden, um die Ermittlerinnen und Ermittler zu unterstützen.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

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?*

   Alle Diensteanbieter müssen bei der Risikobewertung (siehe hierzu die Ausführungen in Frage 1) nach Artikel 3 Absatz 2 Buchstabe b VO-E unter anderem berücksichtigen, ob sie Funktionen vorhalten, die eine Altersüberprüfung ermöglichen. Für interpersonelle Kommunikationsdienste wie Videokonferenz- oder Messengerdienste ist eine Altersverifikation nach Artikel 4 Absatz 3 VO-E verpflichtend, wenn sie ein Risiko ermittelt haben, dass ihre Dienste für den Zweck der Kontaktaufnahme zu Kindern genutzt werden. Stores müssen das Alter ihrer Nutzerinnen und Nutzer verifizieren, um zu verhindern, dass minderjährige Nutzer Zugang zu Software-Anwendungen erhalten, bei denen die Stores ein solches erhebliches Risiko festgestellt haben, Artikel 6 Absatz 1 Buchstabe c VO.

   Abgesehen von offiziellen Ausweisdokumenten, wie dem deutschen elektronischen Personalausweis[9] sind mir keine Technologien bekannt, die eine zuverlässige, anonyme Altersverifikation ermöglichen. Es gibt derzeit jedoch keine europaweite technische Lösung mit der das Alter von Nutzerinnen und Nutzern in einem Online-Kontext mit Sicherheit festgestellt werden kann, ohne sich auf eine offizielle digitale Identität zu stützen. Eine digitale Identität ist aber nicht für alle EU-Bürgerinnen und EU-Bürger verfügbar.[10]

   Es ist ungewiss, ob insbesondere global agierende Diensteanbieter die Funktionen des deutschen elektronischen Personalausweises nutzen würden oder nicht auf alternative Technologien zurückgreifen, wie etwa KI-gestützte Alterskontrolle auf Basis von Gesichtserkennung oder von Verhaltensanalysen. Ferner könnten sie etwa mit externen Vertrauensstellen zusammenarbeiten.

   Diese Lösungen unterschreiten meinem Kenntnisstand nach regelmäßig das notwenige Niveau an Zuverlässigkeit. Dies birgt etwa die Gefahr, dass etwa besonders jung aussende, aber eigentliche berechtigte Nutzerinnen und Nutzer ausgeschlossen werden.[11]

---

[9] BSI, Technische Richtlinie TR-03127 - eID-Dokumente basierend auf Extended Access Control, Version 1.40 vom 6. Oktober 2021, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03127/BSI-TR-03127_1-40.pdf.

[10] EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse vom 28. Juli 2022, Randnummer 92, abrufbar unter: https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf.

[11] a.a.O.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Darüber hinaus haben solche Lösungen einen erheblichen Eingriff in die Datenschutzrechte zur Folge, da sie regelmäßig zusätzliche, häufig auch sensible personenbezogene Daten etwa zur Profilbildung benötigen. Die Erhebung und Erfassung solcher Daten ermöglicht wiederum eine Identifikation, welche die Anonymität der eingesetzten Lösung gefährdet.

Der Einsatz vertrauenswürdiger Drittanbieter birgt die Gefahr, dass diese Dritte verschiedene Aufrufe miteinander verknüpfen und eine Identifizierung der Nutzerinnen und Nutzer durchführen.

Führt die verpflichtende Alterskontrolle zu einer Nutzeridentifikation, kann die Aufhebung der Anonymität in bestimmten Ländern insbesondere für Oppositionelle oder Whistleblower gefährliche, im schlimmsten Fall sogar lebensbedrohliche Konsequenzen zur Folge haben.

Ferner kann der weite Anwendungsbereich des VO-E auf nahezu alle Online-Dienste und Stores für Software-Anwendungen zu einer Überidentifikation führen, da nicht klar umrissen ist, in welchen Fällen welche Dienste eine Altersverifikation vornehmen müssen.

Die EU-Kommission führt selbst an, dass das Ziel des Verordnungsentwurfs in der Stärkung der digitalen Erfahrungen von Kindern und in der Stärkung ihrer digitalen Kompetenz liegt. Wenn bestimmte Applikationen jedoch gesperrt würden, würde eine solche Blockierung dem Gedanken der Stärkung der digitalen Kompetenz von Kindern zuwiderlaufen. Vielmehr sollten Kinder entsprechend für die Gefahren sensibilisiert werden, die von bestimmten Applikationen ausgehen können – jedoch nicht von vorneherein gänzlich von deren Nutzung ausgeschlossen werden. Ansonsten würde diese Maßnahme faktisch zu einer Zensur von Teilen des Netzes führen.

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?*

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Europäische Gesetzgebungen betreffen eine Vielzahl von Ländern und europäische Bürgerinnen und Bürger und spielen sowohl aus politischer, als auch wirtschaftlicher Sicht im internationalen Vergleich durchaus eine beachtenswerte Rolle. Allein aus diesem Grund wird der Vorschlag der Kommission entsprechende Strahlwirkung auf andere Länder und Staaten im europäischen Ausland entfalten.

Selbst wenn dies nicht der Fall wäre, würde es sich für die Anbieter betreffender Dienstleister aus kommerzieller Sicht nicht lohnen, für die EU eine notwendige Sonderentwicklung neben dem eigentlichen Hauptprodukt zu entwickeln, sodass eine globale Implementierung der geforderten Schnittstellen, Anbindungen und Technologien in das jeweilige Hauptprodukt zu erwarten ist.

Sobald die Technologien und Schnittstellen einmal implementiert sind, steht der illegitimen Verwendung dieser durch autoritäre Staaten oder böswilligen Akteuren im Grunde nichts mehr entgegen. Erregt es heute noch Aufsehen mit folgenden Protesten, wenn westliche Anbieter in autoritären Staaten Überwachungsmaßnahmen in ihren Diensten vorsehen, wären diese in Zukunft „surveillance ready".

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?*

   Ich empfinde es als wichtig, das Framing von Privatsphäre versus Kinderschutz gerade nicht zu bedienen. Alle Maßnahmen zur Strafverfolgung müssen verhältnismäßig sein und mit Blick auf Eingriffe in andere Grundrechte den Anforderungen der Verhältnismäßigkeit genügen. Hinsichtlich dieser Abwägung im Falle des Verordnungsentwurfs möchte ich auf meine Ausführungen zu Frage 1 verweisen.

   Ergänzend zu den bereits angeführten Folgen für die Rechte und Freiheiten Betroffener, möchte ich anmerken, dass Kinder und Jugendliche besonders schutzbedürftig sind, so dass der Grundrechteingriff ihnen gegenüber besonders schwerwiegend ist. Auch droht durch die unausweichlichen falsch-positiver Meldungen in Verbindung mit etwaigen strafrechtlichen Ermittlungen bei zum Beispiel einvernehmlichem Sexting unter Jugendlichen unnötiger Kontakt mit Strafermittlungsbehörden, welche für diese Jugendlichen durchaus prägenden Charakter haben könnte.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Darüber hinaus erwarte ich, dass sich auch bei Kindern und Jugendlichen eine Abschreckungswirkung auf die Ausübung der freien Willensäußerung, der sogenannte „Chilling Efffect“ einstellen wird, dies untergräbt das Fundament einer freien Gesellschaft.

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?*

    Hierzu nehme ich Bezug auf die Ausführungen zu Frage 6.

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?*

    Meines Erachtens ist der Geltungsbereich des Verordnungsentwurfs überschießend. Hierzu nehme ich Bezug auf meine Ausführungen zu Frage 2.

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?*

    Hierzu nehme ich Bezug auf die Ausführungen zu Frage 6.

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?*

    Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

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?*

    Hierzu nehme ich Bezug auf die Ausführungen zu Frage 6.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

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?*

    Um die Verpflichtung zur Sperrung einzelner URLs durch die Internetzugangsanbieter nach Artikel 16 VO-E erfüllen zu können, müssten diese detaillierte Informationen über das Surfverhalten und der aufgerufenen Webseiten der Nutzenden erfassen, welches deutlich über die bloße Kenntnis der aufgerufenen Domain hinausgeht.

    Durch den zunehmenden Einsatz von Transportverschlüsselung hat der Internetzugangsanbieter auch keine Möglichkeit ohne Weiteres an die benötigten Informationen zu gelangen und müsste dazu übergehen, https-Verbindungen zum Beispiel mittels Deep Packet Inspection aufzubrechen oder die gesamte Domain zu sperren.

    Das Aufbrechen von https-Verbindungen stellt sich ähnlich problematisch dar wie das Durchbrechen der Ende-zu-Ende-Verschlüsselung. Ich habe erhebliche datenschutzrechtliche Bedenken hinsichtlich des Schutzes der Vertraulichkeit der Kommunikation und des Schutzes der Privatsphäre in der Kommunikation.

    Ferner ist eine Sperrung von Webseiten der Rechtsprechung des Europäischen Gerichtshofes nach nur auf eine richterliche Anordnung hin zulässig, wobei das Gericht bei seiner Entscheidung einen angemessenen Ausgleich der betroffenen Interessen herstellen muss.[12] Die Sperrung ganzer Domains führt regelmäßig zu überschießenden Sperrungen (sogenanntes Overblocking) und kann meines Erachtens den Anforderungen des europäischen Gerichtshofes an die Zielgerichtetheit von Netzsperren daher nicht genügen.

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?*

[12] EuGH, Urteil vom 27. März 2014, Rs. C-314/12.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

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?*

    Hierzu nehme ich Bezug auf die Ausführungen zu Frage 1 und Frage 15.

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?*

    Ich habe keine Erkenntnis über das methodische Vorgehen des EU-Zentrums.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de