Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Bern, 07.08.2024

Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern

Bericht des Eidgenössischen Justiz- und Polizeidepartements (EJPD) zum Verordnungsvorschlag der EU-Kommission vom 11. Mai 2022

Zusammenfassung

Der Bundesrat hat den vorliegenden Bericht in seiner Stellungnahme vom 23. November 2022 zur Motion 22.4113 (Bellaiche; Chat-Kontrolle. Schutz vor anlassloser dauernder Massenüberwachung) in Aussicht gestellt. Die Motion erfolgte im Zusammenhang mit dem Vorschlag der EU-Kommission für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (englisch «child sexual abuse»; nachfolgend **CSA-Verordnungsvorschlag** oder **CSA-VO-V**). Im Bericht wird zunächst auf einzelne Pflichten und Bestimmungen des CSA-Verordnungsvorschlags eingegangen. Zu diesen Pflichten gehören etwa die der Aufdeckung (Art. 7 ff. CSA-VO-V), Entfernung (Art. 14 f. CSA-VO-V) und Sperrung (Art. 16 ff. CSA-VO-V) von bekanntem und neuem kinderpornografischem Material sowie der Kontaktaufnahme zu Kindern (Grooming). Der Bericht behandelt darauf die Frage, was für Handlungsbedarf im Online-Kindes- und Jugendschutz besteht und zeigt schliesslich auf, welche Massnahmen der Bund bereits ergriffen hat, welche Massnahmen geplant sind und welche rechtlichen Auswirkungen der CSA-VO-V auf die Schweiz haben könnte.

Der Bericht stützt sich auf den **Vorschlag der EU-Kommission vom 11. Mai 2022**. Es ist noch offen, ob und wie der CSA-Verordnungsvorschlag verabschiedet werden wird. Einer der umstrittenen Punkte ist die sogenannte **Aufdeckungsanordnung («Chatkontrolle»)**, mit der die Anbieterinnen von Diensten der Informationsgesellschaft verpflichtet werden sollen, Überwachungsmassnahmen durchzuführen, um sexuellen Kindesmissbrauch im Internet aufzudecken (Art. 7 Abs. 1 und Art. 10 CSA-VO-V). Darüber hinaus wird in der EU auch beraten, ob eine Aufdeckung auch Ende-zu-Ende-Verschlüsselungen betreffen kann oder nicht.

Der **Schutz von Kindern und Jugendlichen vor Cybermobbing und sexuellem Missbrauch** im Internet war schon verschiedentlich Gegenstand von parlamentarischen Vorstössen und von Berichten des Bundesrates. Er ist bereits mit verschiedenen gesetzlichen Regelungen gestärkt worden, wie beispielsweise mit der 2021 in Kraft getretenen Teilrevision des Fernmeldegesetzes. Auf der operativen Ebene engagiert sich u.a. fedpol für den Bund in internationalen Organisationen und Plattformen wie NEDIK und dem Cyberboard.

Der CSA-Verordnungsvorschlag stellt **keine Weiterentwicklung des Schengen-Besitzstands** dar. Dennoch kann nicht ausgeschlossen werden, dass Personen mit Sitz oder Wohnsitz in der Schweiz von den vorgeschlagenen Regelungen und damit auch von den Aufdeckungsanordnungen betroffen wären. Dies könnte etwa der Fall sein, wenn sie Dienste von Anbieterinnen in EU-Staaten oder von Anbieterinnen ausserhalb der EU, die ihre Tätigkeit aber auf den EU-Raum ausrichten, nutzen.

Solche Aufdeckungsanordnungen könnten in einem **Konflikt zum Territorialitätsprinzip** stehen. Ausdruck dieses Prinzips ist das in Artikel 271 des Strafgesetzbuches verankerte Verbot, ohne Bewilligung für einen fremden Staat Handlungen vorzunehmen, die einer Behörde oder einem Beamten zukommen. Solche staatlichen Handlungen sind im Einzelfall auf dem Wege der Rechtshilfe zu beantragen oder generell-abstrakt in einem Staatsvertrag (wie z.B. der Budapest-Konvention) vorzusehen.

Im Bereich der Amts- und Rechtshilfe lässt sich eine Tendenz zum Abbau von souveränitätsrechtlichen Hindernissen feststellen. Diese Tendenz dürfte insbesondere auch im Bereich e-Evidence und anderer Kooperationsformen in Strafsachen zunehmen, und sie könnte auch durch den CSA-Verordnungsvorschlag verstärkt werden.

Inhaltsübersicht

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BA	Bundesanwaltschaft
BAKOM	Bundesamt für Kommunikation
BBl	Bundesblatt
BJ	Bundesamt für Justiz
BR	Bundesrat
BSK	Basler Kommentar
Bst.	Buchstabe
BSV	Bundesamt für Sozialversicherungen
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 18. März 2016, SR 780.1
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft (BV) vom 18. April 1999, SR 101
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse material
CSA-VO-V	Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (im Englischen: Child Sexual Abuse [CSA]; CSA-Verordnungsvorschlag[1]
DSA	Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), L 277/1
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020, SR 235.1
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), L 119/1
E.	Erwägung

[1] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, Vorschlag des Europäischen Parlamentes und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vom 11. Mai 2022.

EDI	Eidgenössisches Departement des Innern
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950, SR 0.101
EU	Europäische Union
FDA	Anbieterinnen und Anbieter von Fernmeldediensten
FDV	Verordnung über Fernmeldedienste vom 9. März 2007, SR 784.101.1
fedpol	Bundespolizei
FMG	Fernmeldegesetz (FMG) vom 30. April 1997, SR 784.10
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, IRSG) vom 20. März 1981, SR 351.1
JSFVG	Bundesgesetz über den Jugendschutz in den Bereichen Film und Videospiele (JSFVG) vom 30. September 2022 (BBl 2022 2406; noch nicht in Kraft)
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KKPKS	Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz
m.V.a.	mit Verweisen auf
N/NR	Nationalrat
NCMEC	National Center for Missing and Exploited Children
NCSC	Nationales Zentrum für Cybersicherheit
NEDIK	Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung
OFK	Orell Füssli Kommentar
RK-N	Kommission für Rechtsfragen des Nationalrates
RK-S	Kommission für Rechtsfragen des Ständerates
RVOV	Regierungs- und Verwaltungsorganisationsverordnung (RVOV) vom 25. November 1998, SR 172.010.1
Rz.	Randziffer
SKP	Schweizerische Kriminalprävention
SR	Systematische Rechtssammlung des Bundes
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0
StPO	Schweizerische Strafprozessordnung (Strafprozessordnung, StPO) vom 5. Oktober 2007, SR 312.0
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
ZPO	Schweizerische Zivilprozessordnung (Zivilprozessordnung, ZPO) vom 19. Dezember 2008, SR 272

I. Übersicht

A. Ausgangslage

Am 11. Mai 2022 hat die EU-Kommission den Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (englisch «child sexual abuse») vorgelegt (nachfolgend **CSA-Verordnungsvorschlag**; **CSA-VO-V**)[2]. Als Reaktion darauf haben die damalige Vorsteherin des EJPD und die deutschsprachigen Justizministerinnen und -minister Deutschlands, Österreichs, Luxemburgs und des Fürstentums Liechtenstein am 8. Mai 2023 ein gemeinsames Schreiben an die EU-Justizministerinnen und -minister gerichtet, in dem betont wird, dass die Grundrechte gewahrt werden müssen.

In der Schweiz gab der CSA-Verordnungsvorschlag im Jahr 2022 im Nationalrat Anlass zu einer Interpellation[3] und einer Motion[4]. Mit der Motion 22.4113 soll der Bundesrat beauftragt werden, das von Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) und Artikel 13 der Bundesverfassung (BV) garantierte Recht auf Schutz der Privatsphäre durchzusetzen und die Einwohnerinnen und Einwohner der Schweiz vor der im CSA-Verordnungsvorschlag vorgesehenen Chatkontrolle zu schützen. Der Bundesrat hat in seiner Stellungnahme vom 23. November 2022 festgehalten, dass sich die Auswirkungen des CSA-Verordnungsvorschlags auf die Schweiz zum jetzigen Zeitpunkt noch nicht abschliessend beurteilen lassen; um den Handlungsbedarf frühzeitig zu erkennen, hat er die vorliegende **Analyse zum Handlungsbedarf beim Kindes- und Jugendschutz im Internet** sowie zu den **Auswirkungen des CSA-Verordnungsvorschlags** angekündigt.

Am 27. April 2023 hat die RK-N den EDÖB zum CSA-Verordnungsvorschlag angehört. Im Anschluss daran hielt die RK-N fest, dass sie ein besonderes Augenmerk darauf richten werde, wie sich die Kontrolle von Chatnachrichten in der Europäischen Union (EU) entwickelt und was für Folgen dies für die Schweizer Bevölkerung haben könnte.[5] Der Nationalrat hat die Motion 22.4113 am 25. September 2023 deutlich angenommen (144 Stimmen dafür, 24 dagegen, 21 Enthaltungen). Die vorberatende Kommission des Ständerats (RK-S) hat das Geschäft am 18. März 2024 behandelt und mit neun zu einer Stimme beschlossen, es im Hinblick auf den vom Bundesrat angekündigten Bericht zu sistieren.

B. Inhalt des Berichts

Der vorliegende Bericht geht zunächst auf den **Inhalt** des CSA-Verordnungsvorschlags ein und erläutert im Anschluss **den aktuellen Stand und die Entwicklungen in der EU**. Dabei liegt ein besonderes Augenmerk auf der «Chatkontrolle» (Aufdeckungsanordnungen). Ferner behandelt dieser Bericht, wie in der bundesrätlichen Stellungnahme vom 23. November 2022 in Aussicht gestellt, die Frage **des materiellen Handlungsbedarfs im Online-Kindes- und Jugendschutz** und zeigt auf, welche Massnahmen bereits ergriffen wurden oder vorgesehen sind.

Ausserdem setzt sich der vorliegende Bericht mit den möglichen **rechtlichen Auswirkungen**

---

[2] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, Vorschlag des Europäischen Parlamentes und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vom 11. Mai 2022.

[3] Interpellation 22.3404 Judith Bellaiche vom 9. Mai 2022, Chat-Kontrolle.

[4] Motion 22.4113 Judith Bellaiche vom 29. September 2022, Chat-Kontrolle. Schutz vor anlassloser dauernder Massenüberwachung.

[5] Schriftliche Stellungnahme des EDÖB vom 4. April 2023. Siehe auch die Medienmitteilung «Für einen Straftatbestand Stalking» vom 28. April 2023.

des CSA-Verordnungsvorschlags für die Schweiz auseinander. Dabei steht die Frage im Vordergrund, inwiefern in der Schweiz ansässige Anbieter von Diensten der Informationsgesellschaft – d.h. Hostingdienste, interpersonelle Kommunikationsdienste, Stores für Softwareanwendungen und Internetzugangsdienste (Art. 2 Bst. f CSA-VO-V) – sowie die breite Bevölkerung von den geplanten Regelungen betroffen wären. Der Bericht stützt sich dabei auf den Vorschlag ab, welcher am 11. Mai 2022 von der EU-Kommission vorgelegt wurde. Zwischenzeitlich wurden am CSA-VO-V verschiedene Änderungen vorgeschlagen, doch fanden diese bisher keine Mehrheit.

II. Der CSA-Verordnungsvorschlag

A. Allgemeine Pflichten

Der CSA-Verordnungsvorschlag will den sexuellen Missbrauch von Kindern im Internet bekämpfen (Art. 1 Abs. 1 CSA-VO-V). La proposition de règlement distingue entre les services d'hébergement (art. 2 let. a CSA-VO-V), les services de communications interpersonnelles (art. 2 let. b CSA-VO-V), les boutiques d'applications logicielles (art. 2 let. d CSA-VO-V) et les services d'accès à l'internet (art. 2 let. e CSA-VO-V). Pour désigner ces quatre services, le règlement utilise le terme générique de «services de la société de l'information pertinents» (art. 2 let. f CSA-VO-V).

La proposition de règlement cherche à lutter contre trois types d'abus :

- La **diffusion de matériel connu** relatif à des abus sexuels sur enfants (art. 2 let. m CSA-VO-V): La pédopornographie ou les spectacles pédopornographiques qui ont déjà été détectés et identifiés comme tels.
- la **diffusion de matériel nouveau** relatif à des abus sexuels sur enfants (art. 2 let. n CSA-VO-V): Le matériel constituant potentiellement de la pédopornographie ou un spectacle pédopornographique.
- les **sollicitations d'enfants** (art. 2 let. o CSA-VO-V): La sollicitation d'enfants à des fins sexuelles (pédopiégeage ou plus communément appelée **«grooming»**)

Den Anbietern der Dienste der Informationsgesellschaft werden Pflichten bezüglich der **Aufdeckung** (Art. 7 ff. CSA-VO-V; sog. «Chatkontrolle» siehe auch unten II.B), **Entfernung** (Art. 14 f. CSA-VO-V) und **Sperrung** (Art. 16 ff. CSA-VO-V) von bekanntem und neuem kinderpornografischen-Material sowie der Kontaktaufnahme zu Kindern (sog. Grooming) und **Meldepflichten** (Art. 12 f. CSA-VO-V) auferlegt.[6]

Der CSA-Verordnungsvorschlag enthält **weitere Pflichten**, wie z.B.:

- die Pflicht für die Anbieter von Hostingdiensten und von interpersonellen Kommunikationsdiensten, das **Risiko zu bewerten**, inwieweit ihre Dienste für die Verbreitung von Material über sexuellen Kindesmissbrauch oder für *Grooming*[7] missbraucht werden könnten (Art. 3 CSA-VO-V);
- die Pflicht für die Anbieter von Hostingdiensten und von interpersonellen Kommunikationsdiensten, das identifizierte **Risiko zu mindern** (Art. 4 CSA-VO-V); die Risikoberichte der Anbieter müssen der zuständigen Koordinierungsbehörde übermittelt werden (Art. 5

[6] Begründung des CSA-Verordnungsvorschlags, S. 19; EDÖB, schriftliche Stellungnahme des EDÖB vom 4. April 2023; Presseartikel vom 26. Oktober 2022, «Was das neue EU-Recht gegen sexuellen Kindesmissbrauch im Internet bringt».

[7] Unter Grooming wird die gezielte Kontaktaufnahme Erwachsener mit minderjährigen Personen in der Absicht, sie sexuell zu missbrauchen, verstanden.

CSA-VO-V); und

- die Pflicht für die App-Store-Anbieter, sicherzustellen, dass Kinder **keine Apps herunterladen können**, bei denen sie ein erhebliches Risiko festgestellt haben, dass diese für die Kontaktaufnahme mit Kindern genutzt werden könnten (Art. 6 Abs. 1 Bst. b CSA-VO-V).

Diese Pflichten gelten unabhängig vom Niederlassungsort für alle Anbieter, die ihre Dienste in der EU anbieten (Art. 1 Abs. 2 CSA-VO-V; vgl. dazu auch hinten, IV.B).

Auf Anordnung der zuständigen Justizbehörde oder einer unabhängigen Verwaltungsbehörde muss der Anbieter von Hostingdiensten konkrete Inhalte, die nach sorgfältiger Prüfung der zuständigen Behörde als Darstellungen sexuellen Kindesmissbrauchs eingestuft wurden, auf seinem Dienst entfernen oder den Zugang dazu in allen Mitgliedstaaten sperren (Art. 14 f. CSA-VO-V). Ausserdem hat der Anbieter von Internetzugangsdiensten angemessene Massnahmen zu ergreifen, um den Zugang zu URL-Adressen mit bestimmtem Material über sexuellen Kindesmissbrauch, die sich an der Quelle nicht angemessen entfernen lassen, zu sperren (Art. 16 u. 17 CSA-VO-V).

Der CSA-VO-V sieht die Errichtung eines **EU-Zentrums für die Verhütung und Bekämpfung von sexuellem Kindsmissbrauch** vor (Art. 40 Abs. 1 CSA-VO-V). Die Anbieter von Hostingdiensten und interpersonellen Kommunikationsdiensten, die auf andere Weise als durch eine Entfernungsanordnung Hinweise auf einen potenziellen Kindsmissbrauch im Internet in ihrem Dienst erhalten, haben dies dem EU-Zentrum unverzüglich mitzuteilen (Art. 12 f. CSA-VO-V).

Das EU-Zentrum für die Verhütung und Bekämpfung von sexuellem Kindsmissbrauch nimmt bei der Umsetzung der vorgesehenen Regelungen eine zentrale Rolle ein. Les multiples compétences du centre de l'UE sont listées aux art. 43 ss de la proposition de règlement. En plus de faciliter la mise en œuvre de la proposition de règlement (art. 43 et 48 s. CSA-VO-V), le centre de l'UE crée et assure le bon fonctionnement de différentes bases de données prévues par la proposition de règlement (art. 44 ss CSA-VO-V). Il met également à disposition les technologies que les fournisseurs de services peuvent utiliser gratuitement pour se conformer aux injonctions de détection (art. 50 CSA-VO-V). En plus de collaborer avec les autorités de coordination désignées par chaque Etat membre (art. 21 par. 2 CSA-VO-V), la proposition de règlement prévoit une collaboration avec Europol (art. 53 CSA-VO-V) et avec d'autres organisations partenaires (art. 54 CSA-VO-V).

Die EU-Mitgliedstaaten sind verpflichtet, eine **nationale Koordinierungsbehörde** für Fragen des sexuellen Missbrauchs von Kindern zu benennen (Art. 25 ff. CSA-VO-V), die für die innerstaatliche Anwendung und Durchsetzung der vorgeschlagenen CSA-Verordnung zuständig ist.[8]

B. Die Aufdeckungsanordnung («Chatkontrolle») im Besonderen

Der wohl umstrittenste Punkt des CSA-Verordnungsvorschlags ist die sogenannte Chatkontrolle, die Aufdeckungsanordnung. Die Aufdeckungsanordnung verpflichtet den Anbieter der Dienste der Informationsgesellschaft zu Überwachungsmassnahmen durch die Installation und den Betrieb von Technologien (Art. 7 Abs. 1 und Art. 10 CSA-VO-V). Ce faisant, il peut – mais ne doit pas nécessairement – utiliser les technologies mises à disposition par le centre de l'UE. Les technologies utilisées doivent néanmoins répondre aux critères fixés par la proposition de règlement (art. 10 par. 2 CSA-VO-V).

Eine willkürliche, kontinuierliche, anlasslose und zeitlich unbeschränkte Überwachung der

[8] Analysedokument «Die Schweiz und die Digitalstrategie der Europäischen Union» des UVEK, EDA, EFD, WBF, EDI und EJPD vom 15. März 2023, Massnahme 6, S. 21 f.

Kommunikation ist nicht Ziel der Aufdeckungsanordnungen.[9] Der Erlass einer Aufdeckungsanordnung soll gemäss Art. 7 Abs. 4-7 CSA-VO-V vielmehr nur zulässig sein, wenn Beweise vorliegen für ein erhebliches Risiko, dass der Dienst zum Zwecke des sexuellen Kindesmissbrauchs im Internet genutzt wird und wenn die Gründe für den Erlass einer Aufdeckungsanordnung schwerer wiegen als die negativen Folgen für die Rechte und berechtigten Interessen aller betroffenen Parteien, insbesondere was die notwendige Herstellung eines angemessenen Gleichgewichts zwischen den Grundrechten dieser Parteien betrifft.

Sind diese Voraussetzungen nach Einschätzung der zuständigen nationalen Koordinierungsbehörde am Niederlassungsort des Dienstes erfüllt, führt sie die notwendigen Untersuchungen und Bewertungen durch (Art. 7 Abs. 2 CSA-VO-V). Sie gibt dem betroffenen Anbieter und dem EU-Zentrum für die Verhütung und Bekämpfung sexuellen Kindesmissbrauchs die Möglichkeit zur Stellungnahme. Darauf kann die nationale Koordinierungsbehörde bei der zuständigen Justiz- oder Verwaltungsbehörde des EU-Mitgliedstaats, in dem der Dienst seine Niederlassung hat, den Erlass einer **Aufdeckungsanordnung** beantragen (Art. 7 Abs. 1 CSA-VO-V), worüber diese sodann nach Konsultation der nationalen Koordinierungsbehörde entscheidet (Art. 7 Abs. 1 und Art. 8 CSA-VO-V).

Die Aufdeckungsanordnung beinhaltet Informationen zur Vollstreckung der Anordnung, den Namen des Dienstleistungserbringers, die konkrete Dienstleistung, für die die Anordnung ausgesprochen wird und die Dauer der Überwachung (Art. 8 CSA-VO-V). Diese ist bei Darstellungen sexuellen Kindesmissbrauchs auf 24 Monate und bei der Kontaktaufnahme zu Kindern (sog. Grooming) auf 12 Monate beschränkt (Art. 7 Abs. 9 CSA-VO-V). Anhang I enthält ein Muster für eine Aufdeckungsanordnung.

Die durch eine Aufdeckungsanordnung verpflichteten Anbieter und die betroffenen Nutzerinnen und Nutzer können diese vor Gericht anfechten (Art. 9 Abs. 1 CSA-VO-V).[10]

C. Aktueller Stand und Entwicklungen in der EU

Aktuell wird der CSA-VO-V im Rat der EU und parallel dazu im Parlament der EU behandelt. Besonders die Aufdeckungsanordnung und auch die Ende-zu-Ende-Verschlüsselung der CSA-VO-V[11] haben dabei Anlass zu Diskussionen und Differenzen geführt, die nach wie vor bestehen.

Am 10. Oktober 2023 hat die damalige spanische Ratspräsidentschaft einen Kompromissvorschlag hinsichtlich der Aufdeckungsanordnung eingebracht: Zunächst sollten nur Aufdeckungsanordnungen für bekanntes kinderpornografisches Material in der CSA-VO-V umgesetzt werden. Weil Aufdeckungsanordnungen für noch unbekanntes kinderpornografisches Material und Grooming besonders umstritten sind, sollten diese Punkte zu einem späteren Zeitpunkt, nach dem Inkrafttreten des CSA-VO-V, diskutiert werden. Die deutsche Delegation

---

9 Stellungnahme des Bundesrates vom 23. November 2022 zur Motion 22.4113 Judith Bellaiche vom 29. September 2022, «Chat-Kontrolle. Schutz vor anlassloser dauernder Massenüberwachung». Der Bundesrat hat darin Folgendes festgehalten: «Eine kontinuierliche, anlasslose staatliche Überwachung digitaler Kommunikation ist im Vorschlag der EU-Kommission nicht vorgesehen.» Im Dokument «Die Schweiz und die Digitalstrategie der Europäischen Union», Massnahme 6, S. 21 f. wird diese Meinung ebenfalls vertreten: «Eine kontinuierliche, anlasslose staatliche Überwachung jeglicher interpersonellen digitalen Kommunikation ist im aktuellen Vorschlag der KOM nicht vorgesehen.» (zuletzt abgerufen am 3. Mai 2024); kritischer äussert sich der EDÖB in seiner schriftliche Stellungnahme vom 4. April 2023: «Mittels Aufdeckungsanordnung verpflichten die Koordinierungsbehörde private Anbieter, die Schrift-, Sprach- und Bildkommunikation ihrer Kundinnen und Kunden während einer Phase von mehreren Monaten flächendeckend zu überwachen. Die Massnahmen gelten als automatisiert, da sie durch den Einsatz von Überwachungssoftware erfolgen, die das EU-Zentrum den unterstellten Anbietern zur Verfügung stellt. Ein Anfangsverdacht gegen einzelne Nutzer wird weder für den Erlass einer Aufdeckungsanordnung noch für die Durchführung der Überwachungsmassnahmen vorausgesetzt.».

10 Schriftliche Stellungnahme des EDÖB vom 4. April 2023.

11 Die Ende-zu-Ende-Verschlüsselung verhindert, dass übermittelte Daten von Dritten gelesen oder geändert werden können. Die Nachrichten werden vom Absender verschlüsselt, der Empfänger ruft die verschlüsselten Daten ab und entschlüsselt sie selbst.

unterbreitete darauf einen Gegenvorschlag. Nach diesem sollte der CSA-VO-V in zwei Teile aufgeteilt werden: Die unbestrittenen Elemente des CSA-VO-V sollten in Kraft treten, während über die umstrittene Aufdeckungsanordnung in einem zweiten Schritt entschieden werden solle. Dieser Vorschlag fand keine Unterstützung. Der Rat der EU hat, anders als es die spanische Ratspräsidentschaft geplant hatte, keine allgemeine Ausrichtung verabschiedet.

Anfangs Februar 2024 hat die Kommission zusätzlich zum CSA-VO-V einen Vorschlag zur Aktualisierung der strafrechtlichen Vorschriften über sexuellen Missbrauch und sexuelle Ausbeutung von Kindern vorgelegt. Dazu sollen die Definitionen von einschlägigen Straftaten erweitert werden, um z.B. das Livestreaming von Kindsmissbrauch oder den Besitz und Austausch von Anleitungen für Pädophilie zu regeln.[12]

Mit Stellungnahme vom 13. Februar 2024 hat der europäische Datenschutzausschuss (EDSA)[13] gefordert, dass das Grundrecht auf Privatsphäre uneingeschränkt zu gewährleisten sei.[14] Insbesondere sei es problematisch, dass die Verwendung von Technologien zur Erkennung neuer Missbrauchsmaterialien trotz hoher Fehlerquoten erlaubt blieben. Weiter wird kritisiert, dass der Vorschlag in seiner derzeitigen Form in der Praxis anlasslose Überwachungen zulassen könnte, denn obwohl er eine Aufdeckungsanordnung nur gezielt und bei hinreichenden Verdachtsmomenten gewähre, sei er diesbezüglich zu offen formuliert, so dass auch völlig unbeteiligte Personen betroffen sein könnten.

Am 1. März 2024 wurde der von der derzeitigen belgischen Ratspräsidentschaft vorgelegte neue Kompromissvorschlag erstmals in der «Gruppe Strafverfolgung» (engl. «Law Enforcement Working Party», LEWP) diskutiert. Im Zentrum des Kompromissvorschlags stehen die Risikobewertung sowie der Schutz der Cyber Security und der verschlüsselten Daten. In Bezug auf die Risikobewertung sieht der Vorschlag vor, die Dienstleistungen der Provider in die Risikokategorien «hoch», «mittel», «tief» und «vernachlässigbar» einzuteilen und sodann die der Risikokategorie angemessenen Massnahmen zu ergreifen. Je nach Risiko sollen die Risikobewertungen wiederholt werden. Der Schutz der verschlüsselten Daten soll gemäss dem Kompromissvorschlag sichergestellt werden, indem die Dienstleistungen mit hohem Risiko in den Anwendungsbereich von Standard-Aufdeckungsanordnungen fallen, welche nicht dazu verpflichten, einen Zugang zu verschlüsselten Daten zu schaffen.

Im März und am 9. April 2024 veröffentlichte die belgische Präsidentschaft einen Vorschlag, bei dem die Aufdeckungsanordnung auf diejenigen Fälle beschränkt werden soll, bei denen ein erhebliches und gegenwärtiges oder vorhersehbares Risiko besteht, dass der mit hohem Risiko behaftete Dienst oder Teile oder Komponenten des Dienstes zum Zweck des sexuellen Missbrauchs von Kindern im Internet im Sinne der Absätze 5, 6 bzw. 7 genutzt werden.[15] Aber auch dieser Vorschlag fand keine Mehrheiten. Aktuell bilden Deutschland und Österreich - die sich gegen jegliche Eingriffe in die Ende-zu-Ende-Verschlüsselung stellen - zusammen mit den Niederlanden, Luxemburg und Frankreich wohl die blockierende Minderheit.

Ein weiterer Vorschlag wurde in der LEWP am 8. Mai 2024 behandelt. Demnach sollen bekanntes Child Sexual Abuse Material (CSAM), unbekanntes CSAM und Grooming im Anwendungsbereich der Verordnung verbleiben, aber die Aufdeckungsanordnungen auf visuelle Inhalte beschränkt werden. Am 14. Juni 2024 erfolgte ein Kompromissvorschlag der belgischen Ratspräsidentschaft.[16] Namentlich wurde der Wortlaut zum Schutz der Cybersicherheit und der Verschlüsselung in Artikel 1 Absatz 5 auf Ersuchen der französischen Delegation gestärkt

---

[12] Pressemitteilung der Europäischen Kommission vom 6. Februar 2024, Aktualisierte strafrechtliche Vorschriften bringen Neuerungen im Kampf gegen sexuellen Missbrauch von Kindern.

[13] Der Europäische Datenschutzausschuss ist ein unabhängiges europäisches Gremium. Es ist die Dachorganisation, die die nationalen Datenschutzbehörden der Länder des Europäischen Wirtschaftsraums sowie den Europäischen Datenschutzbeauftragten zusammenbringt.

[14] Stellungnahme des EDSA vom 13. Februar 2024 zum CSA-Verordnungsvorschlag.

[15] Vorschlag der Ratspräsidentschaft vom 9. April 2024 zum CSA-Verordnungsvorschlag.

[16] Vorschlag der Ratspräsidentschaft vom 14. Juni 2024 zum CSA-Verordnungsvorschlag.

sowie auf Ersuchen der tschechischen Delegation eine Definition der «visuellen Inhalte» in Artikel 2 Buchstabe y hinzugefügt. Dem Wunsch nach mehr Klarheit wurde dadurch nachgekommen, indem eine Definition eines Treffers für die Erkennung neuer CSAM in Artikel 2 Buchstabe z aufgenommen wurde. Eine Mehrheit fand der Kompromissvorschlag indes nicht. Am 20. Juni 2024 haben sich die EU-Regierungen nicht wie geplant für die Chatkontrolle ausgesprochen, der belgische Ratsvorsitz nahm das Geschäft kurzfristig von der Tagesordnung. Damit scheiterte das Vorhaben erneut im Rat.[17]

Ob und wann das Europäische Parlament und der Rat die CSA Verordnung (gestützt auf CSA-VO-V) annehmen und ob die Aufdeckungsanordnung darin enthalten sein wird, ist somit zurzeit noch unklar.

Das Europäische Parlament et le Conseil se sont mis d'accord le 15 février 2024 pour prolonger jusqu'au 3 avril 2026 le règlement provisoire relatif une dérogation temporaire à certaines dispositions de la directive "vie privée et communications électroniques" pour la détection volontaire des abus sexuels commis contre des enfants en ligne. Il ne s'agit ainsi pas d'une prolongation de la directive e-Privacy, elle-même, mais du règlement prévoyant une dérogation temporaire à cette directive, à savoir le règlement (EU) 2021/1232 (Verordnung (EU) 2021/1232 des Europäischen Parlaments und des Rates vom 14. Juli 2021 über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG hinsichtlich der Verwendung von Technologien durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet).

L'acte prolongeant jusqu'au 3 avril 2026 le règlement (UE) 2021/1232 est le règlement (UE) 2024/1307 (Verordnung (EU) 2024/1307 des Europäischen Parlaments und des Rates vom 29. April 2024 zur Änderung der Verordnung (EU) 2021/1232 über eine vorübergehende Ausnahme von bestimmten Vorschriften der Richtlinie 2002/58/EG hinsichtlich der Verwendung von Technologien durch Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste zur Verarbeitung personenbezogener und anderer Daten zwecks Bekämpfung des sexuellen Missbrauchs von Kindern im Internet). Dies ermöglicht es den Anbietern sogenannter nummernunabhängiger interpersoneller Kommunikationsdienste (z.B. Nachrichtenübermittlungsdienste), spezielle Technologien für die Verarbeitung personenbezogener und anderer Daten zu nutzen, um sexuellen Kindsmissbrauch in ihren Diensten aufzudecken, zu melden und zu entfernen.[18]

III. Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern in der Schweiz

A. Aktualität und Relevanz des Themas

Der Schutz von Kindern und Jugendlichen im Internet vor sexuellem Missbrauch, Pornografie

[17] Legislative Train Schedule.

[18] Pressemitteilung vom 15. Februar 2024, Sexueller Missbrauch von Kindern: Rat und Europäisches Parlament vereinbaren Verlängerung der Schutzmaßnahme.

und auch Cybermobbing war wiederholt Gegenstand von **parlamentarischen Vorstössen und Initiativen**. Seit 2018 sind folgende zu erwähnen:

- Die parlamentarische Initiative 18.434 Viola Amherd (N; übernommen von Philipp Matthias Bregy) vom 14. Juni 2018: «Cybergrooming mit Minderjährigen endlich unter Strafe stellen» *[N: Fristverlängerung bis zur Wintersession 2025; Zustimmung der RK-S]*;
- Das Postulat 18.3858 Roger Nordmann (N) vom 26.09.2018: «Pornografiekonsum von Kindern und Jugendlichen im Internet einschränken» (vom N abgelehnt).
- Die Interpellation 18.4121 Yvonne Feri (N) vom 29. November 2018: «Immer mehr Kinder werden im Internet von fremden Personen sexuell angemacht. Was unternimmt der Bundesrat?» *(erledigt)*;
- Das Postulat 19.4016 Yvonne Feri (N) vom 12. September 2019): «Sexuelle Gewalt an Kindern im Internet. Was macht das Bundesamt für Polizei?» *(angenommen; Bericht liegt vor; siehe unten **Fehler! Verweisquelle konnte nicht gefunden werden.**);*
- Die Interpellation 19.4054 Rosmarie Quadranti (N; übernommen von Yvonne Feri) vom 18. September 2019: «Bekämpfung von pädosexueller Gewalt im Internet» *(erledigt)*;
- Das Postulat 19.4111 Rosmarie Quadranti (N; übernommen von Heinz Siegenthaler) vom 24. September 2019: «Kinder und Jugendliche vor der Handykamera nicht alleine lassen. Täter stoppen, die Kinder dazu anleiten oder erpressen, sexuelle Handlungen an sich selbst vorzunehmen» *(angenommen; siehe unten **Fehler! Verweisquelle konnte nicht gefunden werden.**)*;
- Das Postulat 19.4105 Fabio Regazzi (N) vom 24. September 2019: «Die Täter vor dem Live-Streaming eines Kindsmissbrauchs stoppen, und der Kinderprostitution im Internet wirksame Grenzen setzen» (*angenommen; siehe unten **Fehler! Verweisquelle konnte nicht gefunden werden.**);*
- Die parlamentarische Initiative 19.486 Fabio Regazzi (N) vom 24. September 2019 «Pädokriminalität im Internet endlich wirksam bekämpfen» *(im N Folge gegeben, keine Zustimmung im S);*
- Die Motion 19.4349 Christine Bulliard-Marbach (N) vom 27. September 2019: «Endlich den Schutz von Kindern vor der rasant ansteigenden pädosexuellen Gewalt im Internet mit einem griffigen nationalen Aktionsplan gewährleisten» *(vom N angenommen, vom S abgelehnt)*
- Die Motion 20.3374 Niklaus-Samuel Gugger (N) vom 6. Mai 2020: «Unter-16-Jährige wirksam vor pornografischen Inhalten auf dem Internet schützen. #banporn4kids#» *[Im N angenommen, im S angenommen mit folgender Änderung: «Der Bundesrat wird beauftragt, der Bundesversammlung die gesetzlichen Anpassungen vorzulegen, dass der Zugang zu legaler Pornographie für Personen unter 16 Jahren erschwert oder verunmöglicht wird. Hierzu sollen die Telekomanbieter verpflichtet werden, die Erziehungsberechtigten auf die technischen Möglichkeiten bei Endgeräten und Angeboten hinzuweisen sowie ihnen Tools und Apps anzubieten, mit denen Jugendliche wirksam vor pornografischen Inhalten geschützt werden können.»]*;
- Die parlamentarische Initiative 20.445 Gabriela Suter (N) vom 11. Juni 2020: «Neuer Straftatbestand Cybermobbing» *[In Kommission des N]*;
- Die Motion 20.3690 Yvonne Feri (N) vom 17. Juni 2020: «Zwingend nötige Anpassung des Straftatbestands der sexuellen Belästigung von Kindern» *(erledigt; vom N angenommen, vom S abgelehnt)*;
- Die Motion 20.4084 Yvonne Feri (N) vom 23. September 2020: «Nationale Strategie zur Bekämpfung der Cyber-Pädokriminalität» *(vom N angenommen, vom S abgelehnt)*;
- Die Interpellation 21.3263 Yvonne Feri (N) vom 18. März 2021 «Anzahl und Relevanz der Meldungen an das Fedpol bei Missbrauchsabbildungen im Internet» *(erledigt)*;

Ausserdem befassen sich zahlreiche Vorstösse **allgemein mit einer zu optimierenden Regulierung im Internet** und/oder **mit der Cyberkriminalitätsbekämpfung** und sind damit auch im Zusammenhang mit der vorgeschlagenen CSA-Verordnung von einer gewissen Relevanz. Zu erwähnen sind folgende Vorstösse und Initiativen:

- Die Interpellation 18.3197 Géraldine Marchard-Balet (N) vom 14. März 2018: «Gesetzliche Vertretung von Dienstleistern in der Schweiz» *(erledigt)*;
- Die Motion 18.3306 Balthasar Glättli (N) vom 15. März 2018: «Rechtsdurchsetzung im Internet stärken durch ein obligatorisches Zustellungsdomizil für grosse kommerzielle Internetplattformen»[19] *(in beiden Räten angenommen; dazu nachfolgend **Fehler! Verweisquelle konnte nicht gefunden werden.**)*;
- Die Motion 18.3379 RK-S (S) vom 23. März 2018: «Zugriff der Strafverfolgungsbehörden auf Daten im Ausland»[20] (*in beiden Räten angenommen)*;
- Die parlamentarische Initiative 19.433 RK-N (N) vom 3. Mai 2019: «StGB-Tatbestände mit Stalking ergänzen» *[Zustimmung RK-S; im Rat noch nicht behandelt]*;
- Die Interpellation 19.4090 Josef Dittli (S) vom 19. September 2019: «Whatsapp und Co. Ein Sicherheitsrisiko für die Schweiz?» *(erledigt)*;
- Die Interpellation 21.3683 Greta Gysin (N) vom 10. Juni 2021: «Prävention gegen Cybergewalt» *(erledigt)*.
- Die Interpellation 21.3684 Greta Gysin (N) vom 10. Juni 2021: «Cybergewalt. Sind die rechtlichen Grundlagen angemessen?» *(erledigt)*;
- Die Interpellation 21.3798 Marco Romano (N) vom 17. Juni 2021: «Bekämpfung der Cyberkriminalität. Läuft beim Bundesamt für Polizei alles rund?» *(erledigt)*;
- Die Interpellation 21.4532 Greta Gysin (N) vom 16. Dezember 2021: «Ein Gesetz zur Regulierung von Kommunikationsplattformen» *(erledigt)*;
- Die parlamentarische Initiative 21.532 Jon Pult (N) vom 16. Dezember 2021: «Illegale Inhalte und Fake News auf Internetplattformen stoppen» *(zurückgezogen)*;
- Das Postulat 22.3145 Andri Silberschmidt (N) vom 16. März 2022: «Wie fit sind die Kantone in der Cyber-Strafverfolgung?» (*angenommen, siehe unten **Fehler! Verweisquelle konnte nicht gefunden werden.**)*;
- Das Postulat 22.3201 Judith Bellaiche (N) vom 17. März 2022: «Digitale Gewalt eindämmen» (*angenommen, siehe unten III.B)*;
- Die Interpellation 22.3156 Greta Gysin (N) vom 16. März 2022: «Verhütung und Bekämpfung von digitaler Gewalt gemäss den Empfehlungen der Expertengruppe Grevio zur Umsetzung der Istanbul-Konvention» *(erledigt)*.
- Die Interpellation 22.4110 Yvonne Feri (N) vom 29.09.2022: «Sexualisierte Gewalt unter Jugendlichen ist erschreckend häufig» (*erledigt*).
- Das Postulat 23.3004 WBK-N vom 20.01.2023: «Schutz vor Zusatzfunktionen in Videospielen» (im N angenommen).
- Die Motion 23.3068 Sozialdemokratische Fraktion (N) vom 8. März 2023: «Digital Services Act für die Schweiz» *[Im N hängig]*.
- Das Postulat 23.4087 Jacqueline de Quattro « Evaluation von Massnahmen gegen Gewalt an Kindern» (zurückgezogen).
- Die Motionen 23.4191 Tamara Funiciello, 23.4192 Lilian Studer, 23.4193 Greta Gysin, 23.4194 Patricia von Falkenstein, 23.4195 Priska Wismer-Felder und 23.4196 Kathrin Bert-

[19] Vgl. auch die Medienmitteilung des Bundesrats vom 5. April 2023 «Grosse Kommunikationsplattformen: Bundesrat strebt Regulierung an».

[20] Vgl. auch die Medienmitteilung des Bundesrats vom 5. April 2023 «Grosse Kommunikationsplattformen: Bundesrat strebt Regulierung an».

schy (N) vom 29.09.2023: «Schutzkonzepte zur Prävention von Missbrauch bei Organisationen, die mit Kindern und Jugendlichen arbeiten» [im N hängig].

- Die Interpellation 23.4502 Katja Christ (N): «Berücksichtigung des Kinder- und Jugendschutzes bei der bevorstehenden Plattformregulierung» (erledigt);

B. Berichte des Bundesrates

In Erfüllung verschiedener parlamentarischer Vorstösse hat der Bundesrat Berichte verfasst oder arbeitet diese aktuell noch aus. Einige Berichte zielen stark auf den Schutz von Kindern und Jugendlichen vor Missbrauch im Internet. Andere behandeln Teilaspekte dieses Themas.

Einen starken Bezug zum Schutz von Kindern und Jugendlichen vor sexuellem Missbrauch im Internet weisen die folgenden Berichte auf:

- Der Bericht des Bundesrates «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmissbrauch via Live-Streaming» vom 8. Dezember 2023 in Erfüllung der Postulate 19.4016 Yvonne Feri vom 14. September 2019 und 19.4105 Fabio Regazzi vom 24. September 2019. Beide Postulate wurden im selben Bericht behandelt.

  Der Bericht gibt einen Überblick über die Verfolgung der Pädokriminalität in der Schweiz: Für die Verfolgung der Pädokriminalität sind die kantonalen Strafverfolgungsbehörden zuständig. Auch bei der Prävention haben die kantonalen Polizeien einen grossen Beitrag zu leisten. Sie haben interkantonale Strukturen zur besseren Koordination der strategischen, operativen und präventiven Tätigkeiten geschaffen. Auf Bundesebene nimmt die Bundespolizei fedpol bei der Cyberkriminalität Zentralstellenaufgaben wahr. Beispielsweise bearbeitet fepdol eingegangene Meldungen des amerikanischen NCMEC und arbeitet in internationalen Arbeitsgruppen zum Thema mit. Im Ergebnis hält der Bericht fest, dass Pädokriminalität ein komplexes Phänomen ist, was die Ermittlung geeigneter Massnahme schwierig gestaltet. Aufgrund der föderalistischen Kompetenzaufteilung kann der Bund nur subsidiär zu den Kantonen tätig werden. Der Bund wird die Präventionsmassnahmen verstärken, wozu er sich bereits in seinem Bericht in Erfüllung des Postulats 19.4111 Rosmarie Quadranti verpflichtete.[21]

- Der Bericht des Bundesrates «Der Schutz von Kindern und Jugendlichen vor Cyber-Sexualdelikten» vom 11. Januar 2023 in der Erfüllung des Postulats 19.4111 Rosmarie Quadranti vom 24. September 2019. Mit dem Postulat wurde der Bundesrat mit der Prüfung der nötigen rechtlichen, technischen und sonstigen Massnahmen beauftragt, damit Kinder und Jugendliche nicht ungehindert zur Herstellung von kinderpornografischem Material erpresst oder angeleitet werden. Der Bundesratsbericht, welcher auf einer in Auftrag gegebenen Studie der Universität Lausanne beruht[22], wurde im Januar 2023 publiziert. Die vier in der Studie behandelten strafbaren Verhaltensweisen sind die Herstellung und Verbreitung von Darstellungen sexueller Handlungen mit Kindern im Internet, Cybergrooming, Sextortion und Live-Streaming von sexuellem Missbrauch an Kindern. All diese Handlungen sind strafrechtlich erfasst. Trotzdem wurden Lücken identifiziert und – gestützt darauf – Handlungsmöglichkeiten aufgezeigt:

  - Neue Forschungen in der Schweiz auf nationaler Ebene könnten die Kenntnisse etwa zu Cyber-Sexualdelikten verbessern und die Erarbeitung der Problematik angemessener, bedürfnis- und entwicklungsorientierter erleichtern;
  - Für den Schutz Minderjähriger vor Cyber-Sexualdelikten sind die Zuständigkeiten und

[21] Bericht des Bundesrates vom 8. Dezember 2023 in Erfüllung der Postulate 19.4016 Feri Yvonne vom 14. September 2019 und 19.4105 Regazzi Fabio vom 24. September 2019, S. 34.

[22] Stefano Caneppele/Christine Burkhardt/ Amandine Da Silva/Lachlan Jaccoud/Fabian Muhly/ Sandra Ribeiro, Mesures de protection des enfants et des jeunes face aux cyber-délits sexuels, Beiträge zur Sozialen Sicherheit. Forschungsbericht Nr.°16/22, Bern 2022.

die Massnahmenumsetzung auf verschiedene Akteure verteilt. Es gilt daher, die Koordination und Zusammenarbeit der Akteure zu fördern, indem die bestehenden Netzwerke wie auch öffentlich-private Partnerschaften gestärkt werden. Vorgeschlagen wird ebenfalls, den Datenaustausch auszubauen.

- Wichtig wäre nach Ansicht der Experten zudem die Abstimmung der getroffenen Massnahmen und das Zusammenwirken der Akteure untereinander um damit Widersprüche in Präventionsprogrammen zu vermeiden. Spannend sei es zudem, künftig innovativere Massnahmen zu entwickeln, welche Unterhaltung und pädagogische Botschaften verbinden.
- Der Fokus sollte auf die Primärprävention gelegt werden, damit auch Eltern, Lehrer und weitere Personen, die mit Kindern und Jugendlichen arbeiten, angesprochen sind und über die nötigen Informationen verfügen, um in Fällen von sexuellen Übergriffen handeln zu können. Dabei dürfen aber die Sekundär- und Tertiärprävention (letztere ist an Straftäterinnen und -täter gerichtet) nicht vergessen gehen.
- Wichtig wäre die Umwandlung polizeilicher und sonstiger Daten in Wissen und Informationen sowie die Evaluation der Wirksamkeit von Präventionsprogrammen.[23]

Der Bundesrat hat sich bereit erklärt, im Rahmen unter Beachtung seiner Zuständigkeiten die Empfehlungen zu den Präventionsmassnahmen umzusetzen. Der Bund wird gezielt Massnahmen als Teil der Aktivitäten der nationalen Plattform «Jugend und Medien» des BSV umsetzen. Gemäss den Empfehlungen soll damit die Koordination zwischen den Akteuren der Medienkompetenzförderung gestärkt, die Entwicklung innovativer Massnahmen unterstützt und ein breiteres Publikum sensibilisiert werden.[24]

Weitere Berichte behandeln Themen mit einem Bezug zum Schutz der Kinder und Jugendlichen vor sexuellen Missbrauch im Internet:

- Der Bericht des Bundesrates «Jugend und Medien» vom 13. Mai 2015 in Erfüllung der Motion 10.3466 Ivo Bischofberger «**Effektivität und Effizienz im Bereich Jugendmedienschutz und Bekämpfung von Internetkriminalität**»: In diesem Bericht nahm der Bundesrat eine Gesamtauslegeordnung zum schweizerischen Kinder- und Jugendmedienschutz (Herausforderungen, Evaluation der bestehenden Massnahmen, künftige regulierende und erzieherische Massnahmen, Nutzungstrends bei den der digitalen Medien und deren Auswirkung auf die ergriffenen Massnahmen, Gefahren online usw.) vor. Mit der Verabschiedung des Berichts beauftragte der Bundesrat das EDI (BSV), die Unterstützung im erzieherischen Kinder- und Jugendmedienschutz weiterzuführen. Im Jahr 2016 wurde die Plattform «Jugend und Medien» zur Förderung von Medienkompetenz gegründet.

- Der Bericht des Bundesrates «Rechtliche Basis für Social Media» in Erfüllung des Postulats 11.3912 Viola Amherd vom 29. September 2011 und der Nachfolgebericht «Rechtliche Basis für Social Media: Erneute Standortbestimmung» zum Postulat 11.3912 Viola Amherd «Rechtliche Basis für Social Media»: In diesem Bericht legte der Bundesrat die Rechtslage in Bezug auf Social Media dar. Im Nachfolgebericht aus dem Jahr 2017 wurde eine erneute Standortbestimmung zu den Rechtsgrundlagen betreffend Social Media vorgelegt.

- Der Bericht des Bundesrates «Die zivilrechtliche Verantwortlichkeit von Providern» vom 11. Dezember 2015: In diesem Bericht wurde geprüft, ob die Zuordnung der Verantwort-

[23] Bericht des Bundesrates vom 11. Januar 2023 in Erfüllung des Postulats 19.4111 Quadranti vom 24. September 2019, Der Schutz von Kindern und Jugendlichen vor Cyber-Sexualdelikten, S. 19.

[24] Bericht des Bundesrates vom 11. Januar 2023 in Erfüllung des Postulats 19.4111 Quadranti vom 24. September 2019, Der Schutz von Kindern und Jugendlichen vor Cyber-Sexualdelikten, S. 21.

lichkeit von Plattformbetreibern und Providern gesetzlich geregelt werden sollte. Der Bundesrat kam zum Schluss, dass eine spezifische, rechtsgebietsübergreifende gesetzliche Regulierung der zivilrechtlichen Verantwortlichkeit von Providern angesichts der bestehenden allgemeinen Rechtsgrundlagen nicht angezeigt ist.[25]

- Der Bericht des Bundesrates «Für ein verhältnismässiges Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs» in Erfüllung des Postulats 19.4031 Albert Vitali vom 16. September 2019: Das Postulat verlangt einen Bericht darüber, wie die rechtlichen Grundlagen so anzupassen sind, dass Überwachungsmassnahmen für Anbieterinnen von Dienstleistungen im Fernmeldebereich verhältnismässig ausfallen, wobei auf die durch die auferlegten Pflichten entstehenden Kosten zu fokussieren ist. Aus Sicht des Bundesrates bedarf es keiner Anpassung auf Gesetzesstufe, da das Bundesgesetz die Interessen der Wirtschaft ausreichend schütze, indem es lediglich den Anbieterinnen von Fernmeldediensten (FDA) umfassende Auskunfts- und Überwachungspflichten auferlegt, aber gleichzeitig auch die Möglichkeit vorsieht, FDA von geringer wirtschaftlicher Bedeutung, worunter insbesondere die KMU fallen, von der Pflicht zur aktiven Überwachungsbereitschaft zu befreien. Anpassungen auf Verordnungsstufe werden vorgeschlagen, jedoch ohne auf die EU-Regelungsabsichten Bezug zu nehmen.

- Nebst dem «Bericht zum US CLOUD Act» vom 17. September 2021 ist auch der «Bericht zur e-Evidence-Vorlage der EU» vom 24. Oktober 2023 des Bundesamts für Justiz zu erwähnen: Das e-Evidence Paket der EU geht zurück auf die Terroranschläge von Brüssel im Jahr 2016, welche die europäischen Justiz- und Innenminister veranlasste, einen besseren Zugang zu elektronischen Beweismitteln zu fordern, was auch vom Rat der EU unterstützt wurde. Das e-Evidence-Paket wurde am 28. Juli 2023 formell verabschiedet. Es schafft einen kohärenten EU-Rahmen für den Umgang mit elektronischen Beweismitteln, deren Erhebung es zudem beschleunigt. So können Strafverfolgungsbehörden der EU-Mitgliedstaaten Beweismittel direkt von digitalen Diensteanbietern in anderen Mitgliedstaaten anfordern (sog. «Herausgabeanordnungen») oder die Aufbewahrung von Daten für einen Zeitraum von bis zu 60 Tagen verlangen, damit relevante Daten nicht zerstört werden oder verloren gehen (sog. «Datenspeicherungsanordnungen»). Es wird dadurch ein zum geltenden Rechtshilfeweg alternativer Mechanismus geschaffen. Diese neuen Regelungen dürften auch grosse Auswirkungen auf die Schweiz haben, da ansässige Diensteanbieter, die ihre Dienste in der EU anbieten, unter bestimmten Voraussetzungen unter die Regelungen fallen werden. Das e-Evidence Paket der EU besteht aus einer Richtlinie, welche die wichtigsten Grundsätze der Vorlage festlegt, und aus einer Verordnung mit detaillierten Bestimmungen.[26]

- Der Bericht des Bundesrates «Ergänzungen betreffend Cybermobbing im Strafgesetzbuch» vom 19. Oktober 2022 in Erfüllung des Postulats 21.3969, Kommission für Rechtsfragen des Nationalrates, vom 25. Juni 2021: Mit dem Postulat wurde der Bundesrat beauftragt, einen Bericht darüber zu erstellen, wie durch entsprechende Ergänzungen des Strafgesetzbuches Cybermobbing und digitale Gewalt bestraft werden können. Der Bundesrat verneint einen Handlungsbedarf in materieller Hinsicht, weil Cybermobbing nach

---

[25] Bericht des Bundesrates «Die zivilrechtliche Verantwortlichkeit von Providern» vom 11. Dezember 2015, S. 4.

[26] Die **Richtlinie** (EU) 2023/1544 verpflichtet digitale Dienstleister, die in der EU bestimmte Dienstleistungen anbieten, dazu, eine Niederlassung in der EU zu etablieren oder einen gesetzlichen Vertreter zu benennen, an den die Behörden der Mitgliedstaaten ihre Herausgabe und Datenspeicherungsanordnungen richten können. Die **Verordnung** (EU) 2023/1543 schafft die Europäische Herausgabeanordnung sowie die Europäische Sicherungsanordnung. Sie regelt damit die Voraussetzungen, unter denen digitale Diensteanbieter in der EU entweder eine Niederlassung haben oder einen gesetzlichen Vertreter ernennen müssen und unter denen die zuständigen (Strafverfolgungs-)Behörden eines EU-Mitgliedstaats im Rahmen eines Strafverfahrens einen solchen service provider direkt zur Herausgabe oder Aufbewahrung von Daten auffordern können. Die Verordnung findet keine Anwendung auf Verfahren, die eröffnet wurden, um einem anderen EU-Mitgliedstaat oder einem Drittstaat (z.B. Schweiz) Rechtshilfe zu gewähren.

dem geltenden Strafrecht aufgrund verschiedener Tatbestände verfolgt und bestraft werden könne.

Bei den anderen Formen «digitaler Gewalt» hat der Bundesrat lediglich strafloses Verhalten ausgemacht, wo weder die Strafnorm der Pornografie (Art. 197 StGB) noch die Ehrverletzungsdelikte (Art. 173 ff. StGB) oder die Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte (Art. 179^{quater} Abs. 3 StGB) anwendbar sind.[27]

Der Bundesrat legt zudem dar, dass die Rechtsdurchsetzung bei über Internet begangenen Straften ein grosses Problem darstelle (Anonymität der Täterschaft, Angewiesenheit auf die im Ausland gespeicherten Daten usw.). Die durch das neue Datenschutzrecht eingeführte Pflicht für die privaten Verantwortlichen, über eine Vertretung in der Schweiz zu verfügen (Art. 14 DSG), wenn gewisse Voraussetzungen erfüllt sind, könnte jedoch die Kontaktaufnahme mit den Anbietern erleichtern. Weitere Arbeiten zur Verbesserung der Rechtsdurchsetzung seien im Gange.[28]

- Der am 20. Juni 2024 publizierte Bericht[29] in Erfüllung der Postulate 22.3145 Andri Silberschmidt (N) vom 16. März 2022: «**Wie fit sind die Kantone in der Cyber-Strafverfolgung**?» und 22.3017 der Sicherheitspolitischen Kommission des Nationalrates **«Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen»** bietet einen Gesamtüberblick über die Bekämpfung der Cyberkriminalität in der Schweiz. Da sich der Bericht hauptsächlich mit den Aktivitäten der Kantone im Bereich der Bekämpfung von Cyberkriminalität befasst, hat fedpol zwei Umfragen durchgeführt, um die relevanten Informationen zu erheben. Zwei grosse Hindernisse stehen einer Verbesserung der Bekämpfung der Cyberkriminalität im Weg: zum einen das Fehlen von gesetzlichen Grundlagen, welche den automatischen Austausch von polizeilichen Informationen zwischen den Kantonen sowie mit dem Bund ermöglichen, und zum anderen das Regime der internationalen Rechtshilfe in Strafsachen.

C. Massnahmen des Bundes

Der Bund ist im Bereich des Kindes- und Jugendschutzes im Internet in verschiedener Hinsicht aktiv. Er hat etwa Revisionen von bestehenden Gesetzen und die Ausarbeitung neuer Erlasse veranlasst, um Kinder und Jugendliche im Internet besser schützen zu können. Er beteiligt sich in internationalen Organisationen zu diesem Thema und hat auch Berichte dazu ausgearbeitet. Die verschiedenen Massnahmen und Aktivitäten des Bundes werden nachfolgend kurz behandelt.

1. Teilrevision des Fernmeldegesetzes

Mit einer **Teilrevision des Fernmeldegesetzes,** die seit dem 1. Januar 2021 in Kraft ist, wurde ein neuer Art. 46*a* FMG zum Kinder- und Jugendschutz eingeführt.[30] Diese neue Bestimmung regelt vier Aspekte:

---

[27] Bericht des Bundesrates «Ergänzungen betreffend Cybermobbing im Strafgesetzbuch» vom 19. Oktober 2022 in Erfüllung des Postulats 21.3969, Kommission für Rechtsfragen des Nationalrats, vom 21. Juni 2021, S. 52. Zudem hat das Parlament Artikel 197*a* nStGB eingeführt, der das unbefugte Weiterleiten von nicht öffentlichen sexuellen Inhalten unter Strafe stellt (AS 2024 27 S. 7). Die neue Strafnorm wird am 01.07.2024 in Kraft treten (AS 2024 27 S. 18).

[28] Bericht des Bundesrates «Ergänzungen betreffend Cybermobbing im Strafgesetzbuch» vom 19. Oktober 2022 in Erfüllung des Postulats 21.3969, Kommission für Rechtsfragen des Nationalrats, vom 21. Juni 2021, S. 52.

[29] Bericht des Bundesrates «Wie fit sind die Kantone in der Cyber-Strafverfolgung?» vom 20. Juni 2024 in Erfüllung der Postulate 22.3145, Andri Silberschmidt, 16. März 2022, und 22.3017, Sicherheitspolitische Kommission des Nationalrates, 15. Februar 2022.

[30] Vgl. Bericht des Bundesrates vom 13. Mai 2015 in Erfüllung der Motion Bischofberger 10.3466 «Effektivität und Effizienz im Bereich Jugendmedienschutz und Bekämpfung von Internetkriminalität», Jugendschutz und Medien

- Der Bundesrat kann Bestimmungen erlassen, um Kinder und Jugendliche vor den Gefahren im Zusammenhang mit Fernmeldediensten zu schützen (Art. 46*a* Abs. 1 FMG).
- Das BAKOM, fedpol und die zuständigen kantonalen Stellen koordinieren geeignete Massnahmen, damit Informationen mit pornografischem Inhalt nach Artikel 197 Absätze 4 und 5 StGB rasch und weltweit gelöscht werden.
- Auf Hinweis von fedpol müssen die Anbieterinnen von Fernmeldediensten Informationen mit pornografischem Inhalt nach Artikel 197 Absätze 4 und 5 unterdrücken (Art. 46*a* Abs. 3 FMG).
- Die Anbieterinnen von Fernmeldediensten müssen Verdachtsfälle über Informationen mit pornografischem Inhalt fedpol melden (Art. 46*a* Abs. 3 FMG).

Umgesetzt wird dies in Art. 89a und Art. 89b FDV.[31]

2. Neues Bundesgesetz über den Jugendschutz in den Bereichen Film und Videospiele

Das **Bundesgesetz über den Jugendschutz in den Bereichen Film und Videospiele**[32] wird am 1. Januar 2025 in Kraft treten. Das Gesetz bezweckt den Schutz der Minderjährigen vor Inhalten in Filmen und Videospielen, die ihre körperliche, geistige, psychische, sittliche oder soziale Entwicklung gefährden können (nArt. 1 JSFVG). Es regelt unter anderem:

- Die Vorgaben für die Alterskennzeichnung, die Inhaltsdeskriptoren und die Alterskontrolle (nArt. 4 Bst. a JSFVG);
- Die Anforderungen an die Jugendschutzregelungen und weitere Massnahmen dazu (nArt. 4 Bst. c JSFVG); und
- Die Massnahmen zur Förderung der Medienkompetenz und zur Prävention (nArt. 4 Bst. e JSFVG).

Das Gesetz sieht eine Koregulierung vor, bei der die Branchen je für die Bereiche Film und Videospiele die konkrete Umsetzung in einer sogenannten Jugendschutzregelung festhalten und dem Bundesrat zur Prüfung und Verbindlicherklärung vorlegen (nArt. 17 JSFVG) können. Der Bundesrat ist gemäss nArt. 19 JSFVG subsidiär dazu befugt, eine Regelung zu schaffen, wenn keine Jugendschutzregelung für verbindlich erklärt wurde, bzw. wenn sie widerrufen oder hinfällig geworden ist. Das Gesetz enthält weitere Vorgaben, etwa um sicherzustellen, dass Minderjährige vor ungeeigneten Inhalten auf Plattformdiensten geschützt werden (nArt. 20 JSFVG). Die Umsetzung des Gesetzes kann mit Testkäufen und Testeintritten überprüft werden (nArt. 21 ff. JSFVG). Einige Umsetzungsfragen hat der Bundesrat in seiner Stellungnahme zur Interpellation Mäder beantwortet.[33]

Im CSA-Verordnungsvorschlag ist folgende Regelung vorgesehen: Die Anbieter von Stores für Software-Anwendungen müssen verschiedene Pflichten erfüllen (Art. 6 CSA-VO-V). Mitunter müssen sie Massnahmen treffen, um den Zugang zu risikoreichen Anwendungen zu verhindern (Art. 6 Abs. 1 Bst. b CSA-VO-V). Weiter müssen sie Massnahmen zur Altersüberprüfung und -beurteilung ergreifen, um minderjährige Nutzerinnen und Nutzer ihrer Dienste zu

– Zukünftige Ausgestaltung des Kinder- und Jugendmedienschutzes der Schweiz, S. 112 ff.

[31] Bericht des Bundesrates vom 13. Mai 2015 in Erfüllung der Motion Bischofberger 10.3466 «Effektivität und Effizienz im Bereich Jugendmedienschutz und Bekämpfung von Internetkriminalität», Jugendschutz und Medien – Zukünftige Ausgestaltung des Kinder- und Jugendmedienschutzes der Schweiz, S. VII, XI, 7, 63 f., 115 f., 125, 137; Erläuternder Bericht vom 26. Oktober 2020 über die Revision der Verordnungen zum FMG, S. 34.

[32] Bundesgesetz vom 30. September 2022 über den Jugendschutz in den Bereichen Film und Videospiele (JSFVG).

[33] Interpellation 23.3077 Jörg Mäder vom 8. März 2023: Erfordert das neue Jugendschutzgesetz eine Ausweispflicht auf Internetplattformen?

identifizieren, damit die vorgenannten Risikominderungsmassnahmen ergriffen werden können (Art. 6 Abs. 1 Bst. c CSA-VO-V).

3. Regelung zu Internetdiensten

Die Kommission für Rechtsfragen des Ständerates (RK-S) hat den Bundesrat mit der Motion 18.3379 «**Zugriff der Strafverfolgungsbehörden auf Daten im Ausland**» vom 23. März 2018 u.a. beauftragt, eine gesetzliche Grundlage zu unterbreiten, welche soziale Netzwerke, die sich mit ihren Dienstleistungen an Schweizer Konsumentinnen und Konsumenten richten, zu einer Vertretung oder einem Zustellungsdomizil in der Schweiz verpflichtet. Die Vertretung oder das Zustellungsdomizil soll dabei als Ansprechpartner der Schweizer Behörden fungieren und es ermöglichen, dass Konsumentinnen und Konsumenten einfacher Beanstandungen einreichen können.

Weiter soll der Bundesrat auf internationaler Ebene aktiv darauf hinwirken, eine Lösung für das Problem der Rechtsdurchsetzung im Internet zu erzielen. Die Schweiz beteiligt sich dafür an den Arbeiten des Europarats für die Weiterentwicklung des Übereinkommens über die Cyberkriminalität.[34] Im Mai 2022 wurde dessen zweites Zusatzprotokoll verabschiedet, wobei die Schweiz nun prüft, ob sie dieses unterzeichnen und ratifizieren wird.

Die Motion 18.3306 Balthasar Glättli («**Rechtsdurchsetzung im Internet stärken durch ein obligatorisches Zustelldomizil für grosse kommerzielle Internetplattformen**») verlangt eine Änderung der Zivilprozessordnung (ZPO) und der Strafprozessordnung (StPO) und will dadurch zu einer effektiveren Rechtsdurchsetzung beitragen. Der Bundesrat hatte bei den Debatten im Parlament darauf hingewiesen, dass der Vorstoss von NR Glättli im breiteren Kontext der vorerwähnten Motion 18.3379 der RK-S zu betrachten ist: Zusammen mit dieser Motion sei nach Lösungen suchen, die umsetzbar und effektiv sind. Eine Änderung von StPO oder ZPO steht dabei nicht im Vordergrund.[35]

Am 1. September 2023 ist das totalrevidierte Datenschutzgesetz (DSG) in Kraft getreten. Art. 14 DSG verpflichtet Personen mit Sitz oder Wohnsitz im Ausland, die alleine oder zusammen mit anderen über den Zweck und die Mittel einer Datenbearbeitung entscheiden, eine Vertretung in der Schweiz zu bezeichnen, wenn sie in der Schweiz Waren oder Dienstleistungen anbieten oder das Verhalten von Personen beobachten und dabei regelmässig umfangreiche Personendaten bearbeiten, sofern diese Bearbeitung ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich bringt. Diese Regelung entspricht den Anliegen der vorgenannten Motionen 18.3306 und 18.3379. Es bleibt zu prüfen, ob ein darüberhinausgehender Handlungsbedarf besteht.

4. Regulierung von grossen Kommunikationsplattformen

Am 5. April 2023 hat der Bundesrat die Öffentlichkeit darüber informiert, die ersten Schritte zur **Regulierung der grossen Kommunikationsplattformen** eingeleitet zu haben. Das UVEK wurde beauftragt, eine Vernehmlassungsvorlage auszuarbeiten. Die Vernehmlassung ist noch nicht eröffnet worden. Soweit sinnvoll sollen die neuen Regeln in Anlehnung an das *Digital Services Act (DSA)*[36] erarbeitet werden.[37]

---

[34] Übereinkommen über die Cyberkriminalität vom 23. November 2001, SR 0.311.43.

[35] Votum von Bundesrätin Simonetta Sommaruga, AB 2018 N 1400.

[36] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), L 277/1.

[37] Medienmitteilung des Bundesrats vom 5. April 2023 «Grosse Kommunikationsplattformen: Bundesrat strebt Regulierung an» (nachfolgend: Medienmitteilung Regulierung von grossen Kommunikationsplattformen); siehe auch Stellungnahme des Bundesrats vom 26. April 2023 zur Interpellation 23.3077 Jörg Mäder vom 8. März 2023: Erfordert das neue Jugendschutzgesetz eine Ausweispflicht auf Internetplattformen?.

Der Bundesrat hat bereits vier Eckpunkte der auszuarbeitenden Vorlage festgelegt:

- Die grossen Plattformen sollen zur Benennung einer Kontaktstelle und eines Rechtsvertreters in der Schweiz verpflichtet werden (vgl. bspw. Art. 24 CSA-VO-V oder Art. 11 und 12 bzw. Art. 13 DSA auf EU-Ebene).
- Hier ist anzumerken, dass diese Pflicht unter Umständen wie erwähnt bereits besteht, wenn Waren oder Dienstleistungen in der Schweiz angeboten werden (s. Art. 14 f. DSG; vgl. Art. 27 DSGVO auf EU-Ebene[38]).
- Nutzende, deren Inhalte gelöscht oder deren Konto gesperrt wurden, sollen bei der Plattform direkt eine Überprüfung der getroffenen Massnahme verlangen können. Zusätzlich sollen die Schweizer Nutzenden das Recht erhalten, an eine unabhängige aussergerichtliche Streitschlichtungsstelle zu gelangen.
- Um Transparenz zu schaffen, sollen die grossen Plattformen Werbung als solche kennzeichnen und bei zielgruppenspezifischer Werbung die wichtigsten Parameter veröffentlichen, nach denen Werbung ausgespielt wird. Damit kann nachvollzogen werden, wer aus welchen Gründen eine bestimmte Werbung erhält.
- Die Nutzenden sollen den Plattformen Aufrufe zu Hass, Gewaltdarstellungen oder Drohungen auf einfache Weise melden können. Die Plattformen müssen die Meldungen prüfen und die Nutzenden über das Ergebnis informieren.

Mindestens zwei dieser vier Eckpunkte, nämlich die **Benennung einer Kontaktstelle und eines Rechtsvertreters** in der Schweiz sowie **die Möglichkeit, Aufrufe zu Hass, Gewaltdarstellungen oder Drohungen einfacher zu melden**, können auch zum Online-Kinder- und Jugendschutz in der Schweiz beitragen.

5. Teilnahme an der WeProtect Global Alliance

Im Jahr 2012 ist die Schweiz der «Weprotect Children Online» beigetreten, welche 2016 mit der «Global Alliance Against Child Sexual Abuse Online» zur «WeProtect Global Alliance» zusammengeschlossen wurde.[39] Die Schweiz wird durch fedpol vertreten.[40]

Die Weprotect Global Alliance bringt die Regierungen, die Privatwirtschaft, die Zivilgesellschaft und die zwischenstaatlichen Organisationen zusammen, um Politiken und Lösungen zum Schutz der Kinder vor der sexuellen Ausbeutung und vor sexuellen Missbräuchen im Internet zu entwickeln. Die übergeordneten Ziele der Allianz sind, Kinder vor diesen Gefahren zu beschützen und das Internet für sie sicher und positiv zu machen.[41]

Mit ihrem Beitritt bekräftigte die Schweiz ihren Willen, die Pädokriminalität im Internet zu bekämpfen und dabei international zu kooperieren.

6. Plattform «Jugend und Medien» des BSV

Seit 2011 laufen die Aktivitäten des Bundes zum Jugendmedienschutz und zur Medienkompetenzförderung mit der nationalen Plattform «Jugend und Medien». Für den Betrieb ist das

---

[38] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), L 119/1.

[39] Stellungnahme des Bundesrats vom 20. November 2019 zum Postulat 19.4105 Fabio Regazzi vom 24. September 2019: «Die Täter vor dem Live-Streaming eines Kindsmissbrauchs stoppen, und der Kinderprostitution im Internet wirksame Grenzen setzen».

[40] Stellungnahme des Bundesrats vom 20. November 2019 zum Postulat 19.4105 Fabio Regazzi vom 24. September 2019: «Die Täter vor dem Live-Streaming eines Kindsmissbrauchs stoppen, und der Kinderprostitution im Internet wirksame Grenzen setzen».

[41] Internetauftritt der WeProtect Global Alliance, Who we are - WeProtect Global Alliance.

BSV verantwortlich. Im Zentrum der Plattform steht eine Webseite mit Informationen und Empfehlungen zur Medienkompetenzförderung. Die Aktivitäten der Plattform richten sich in erster Linie an Eltern sowie Lehr- und Betreuungspersonen, die eine Begleitfunktion im Leben von Kindern und Jugendlichen wahrnehmen. Sie sollen für Chancen und Risiken im Medienalltag sensibilisiert werden, damit sie Kinder und Jugendliche kompetent begleiten und sie dabei unterstützen können, digitale Medien sicher und verantwortungsvoll zu nutzen.[42]

Die **drei Handlungsfelder** der nationalen Plattform sind:

- **Information und Sensibilisierung**: Auf verschiedenen Kanälen werden Informationen über wichtige Themen und Entwicklungen rund um digitale Medien zur Verfügung gestellt.
- **Kompetenz und Wissensaufbau**: Jugend und Medien kann Organisationen und Institutionen, die in der Medienkompetenzförderung aktiv sind, auf unterschiedliche Weise unterstützen. Einerseits ist eine inhaltliche Unterstützung in Form von Beratung oder Wissensaustausch möglich, andererseits unter bestimmten Bedingungen auch punktuelle finanzielle Unterstützung.
- **Netzwerk der Akteure in der Schweiz**: Jugend und Medien engagiert sich für den Austausch und die Zusammenarbeit mit den Akteuren im Bereich Medienkompetenzförderung, um damit die Wissensverbreitung, den Erfahrungsaustausch und die Koordination der bestehenden Aktivitäten zu stärken. Sie arbeitet mit wichtigen Stakeholdern (Bund, zuständige kantonale und lokale Stellen, Wirtschaft, private Organisationen und Hochschulen) zusammen.[43]

Für Zeitspannen von zwei Jahren wird jeweils ein **Schwerpunktthema** gesetzt.

- Für den Zeitraum 2017-2019 behandelte die Plattform «Jugend und Medien» das Schwerpunktthema: **«Extremismus und Radikalisierung»**.[44]

- Das Schwerpunktthema 2018/2019 war **«Sexualität und Internet»**.[45] In einer ersten Phase wurde ein Runder Tisch zur Bedarfserhebung lanciert. Aus diesem ergab sich das Bedürfnis nach einer stärkeren Vernetzung. Daher organisierte das BSV im Anschluss daran einen Think Tank. Dieser erarbeitete ein Haltungspapier «Sexualität und digitale Medien – Kompetenzen fördern, Kinder schützen!»[46]. Aus dem Think Tank ging die bis heute bestehende, vom BSV unabhängige «Nationale Arbeitsgruppe Sexualität und digitale Medien» hervor.[47] Finanziert wurden ausserdem drei Pilotprojekte zur Sensibilisierung von Eltern und Fachpersonen mit Fokus auf besonders vulnerable Zielgruppen.

- Der Schwerpunkt **«Hass im Netz»** (2020/21) thematisierte in erster Linie die Themen Online-Rassismus, Sexismus sowie Queerfeindlichkeit. Ausserdem wurde eine Arbeitsgruppe gegründet, in der sich Bundesstellen austauschen, welche auf unterschiedlichste Weise mit dem Thema «Hass im Netz» konfrontiert sind.[48]

- Lors de la mise en œuvre du point fort **« Protection des données »** en 2020-2021, la plateforme Jeunes et médias a financé des projets qui permettent aux enfants et aux

[42] Internetauftritt der Nationalen Plattform zur Förderung von Medienkompetenz «Jugend und Medien».

[43] Aufzählung der Aktivitäten von «Jugend und Medien».

[44] Schwerpunkte/Extremismus & Radikalisierung von «Jugend und Medien».

[45] Schwerpunktthemen/ Prävention von sexualitätsbezogenen Internetrisiken von «Jugend und Medien».

[46] Haltungspapier «Sexualität und digitale Medien – Kompetenzen fördern, Kinder schützen!» der Nationalen Arbeitsgruppe «Sexualität und digitale Medien».

[47] Internetauftritt der Nationalen Arbeitsgruppe «Sexualität und digitale Medien».

[48] Schwerpunkte/Hass im Netz von «Jugend und Medien».

jeunes de comprendre l'importance du respect de la sphère privée en ligne et ce qu'ils peuvent faire pour protéger aux mieux leurs données.[49] Parallèlement, le projet «Insta4Emma» a voulu sensibiliser les parents et les proches au respect des droits à l'image et de la personnalité des enfants et aux risques d'un partage excessif et peu réfléchi de photos et d'informations concernant les enfants et les jeunes sur les réseaux sociaux de la part des adultes.[50]

- Le point fort sur le **« cyberharcèlement »** (années 2022-2024)[51] a vu la mise en œuvre de la campagne « Not a joke » qui sensibilisé un vaste public, en particulier des enfants et des jeunes, aux conséquences souvent graves du harcèlement en ligne ou *offline*. Cette campagne a permis de répondre à la motion 20.3687 Yvonne Feri.

- Le point fort sur les **« cyber-délits sexuels »** (années 2023-2025) met l'accent sur des mesures de prévention et sensibilisation pour renforcer la protection des enfants et des jeunes en ligne comme annoncé dans le rapport du Conseil fédéral en réponse au postulat 19.4111 Rosmarie Quadranti (v. pages 18 et 19).

7. Révision de la législation en matière de preuves électroniques

Les preuves électroniques amènent de nouvelles problématiques et de nouvelles questions juridiques, notamment dans le domaine de la coopération pénale internationale. Tant sur le plan international que sur le plan national, de nouvelles législations sont adoptées. Un rapport sur le CLOUD Act a été publié par l'Office fédéral de la justice en septembre 2021 et un rapport sur le paquet e-evidence de l'UE a été publié par l'Office fédéral de la justice en octobre 2023. Suivant ces développements internationaux, une réflexion est en cours sur une révision du droit en vigueur en Suisse afin de mieux cibler ce type de preuves notamment en ce qui concerne la coopération pénale internationale.

D. Zusammenarbeit zwischen dem Bund und den Kantonen

In den Bereichen Cyberkriminalität und Kriminalitätsbekämpfung im Internet arbeiten Bund und Kantone im Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK) und der nationalen Plattformen Cyberboard zusammen. Diese Zusammenarbeit ist Teil der Massnahmen zur Verhinderung von sexuellem Kindsmissbrauch im Internet.

1. NEDIK

Das Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK) der Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) ist für die Erkennung und die Verfolgung von Delikten im Internet – insbesondere auch von pädokriminellen Straftaten – von Bedeutung. NEDIK wurde 2018 gegründet. Es besteht aus dem Cybercrime-Kompetenzzentrum des Bundes (bei fedpol angesiedelt) und aus den regionalen Cybercrime-Kompetenzzentren verschiedener Kantonspolizeien.[52] Neben einem strategischen Ausschuss, welcher sich aus Vertreterinnen und Vertretern der Polizeikonkordaten und fedpol zusammensetzt, verfügt NEDIK über einen operativen Ausschuss. Ausschussmitglieder, Vertreter aller Kantonspolizeien und von fedpol, treffen sich zweimal monatlich, um lau-

[49] Schwerpunktthemen/ Datenschutz von «Jugend und Medien».

[50] Sensibilisierungsprojekt Insta4Emma von «Jugend und Medien».

[51] Plattform «Jugend- und Medien», Rubrik «Schwerpunktthemen/ Cybermobbing», abrufbar unter Not a joke – Gib Mobbing keine Chance: Jugend und Medien.

[52] Siehe dazu die Stellungnahme des Bundesrats vom 20. Februar 2019 zur Interpellation 18.4121 Yvonne Feri (N) vom 29. November 2018: «Immer mehr Kinder werden im Internet von fremden Personen sexuell angemacht. Was unternimmt der Bundesrat?».

fende Untersuchungen durch Koordinationsmassnahmen stetig zu verbessern (z.B. die Koordination der Ermittlungen gegen Ransomware-Fälle).

NEDIK stellt den gegenseitigen Wissenstransfer sicher, gibt eine Übersicht über die nationalen Fälle sowie über neue Tendenzen (inkl. Informationen über die *Modi Operandi* und die sofort zu ergreifenden Massnahmen), triagiert interkantonale Fälle und trägt zur Prävention bei. Ausserdem publiziert NEDIK monatliche Bulletins zur Cyberkriminalität in der Schweiz. Bei seinen Tätigkeiten arbeitet NEDIK mit der Schweizerischen Kriminalprävention (SKP) und dem Nationalen Zentrum für Cybersicherheit (NCSC) zusammen.[53]

Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) hat eine Verwaltungsvereinbarung mit der KKPKS gutgeheissen. Dies ist auf den Willen der Kantone zurückzuführen, die Bekämpfung der Internetkriminalität besser zu koordinieren und Ressourcen besser zu bündeln. Die Organisation und die Leistungsfinanzierungen, welche die kantonalen Polizeien bei NEDIK zugunsten der anderen Polizeien erbringen, werden damit geregelt (beispielsweise übernimmt die Kantonspolizei Bern die Führung bei der Bekämpfung der Pädokriminalität und koordiniert die verdeckten verdachtsunabhängigen Fahndungen im digitalen Raum). NEDIK will spezifische Analyseinstrumente einsetzen und eine zentrale Wissensdatenbank betreiben.[54]

Da Kriminalität heute transnational ist, was insbesondere für die digitale Kriminalität und die Pädokriminalität gilt, will NEDIK eine effiziente Kooperation mit dem Ausland sicherstellen.[55] Neben der interkantonalen Koordinationsrolle übernimmt fedpol die internationale Fallkoordination und ist im stetigen Austausch mit ausländischen Partnern wie Europol und Interpol. fedpol ist auch für die Triage ausländischer Verdachtsmeldungen (z.B. die Meldungen des NCMEC) zuständig.[56]

2. Cyberboard

Das Cyberboard ist die nationale Zusammenarbeitsplattform der Strafverfolgungsbehörden (d.h. Polizei und Staatsanwaltschaften) sowie der Präventionsbehörden des Bundes und der Kantone. Mit dem Cyberboard werden eine bessere Zusammenarbeit zwischen diesen Behörden, eine bessere Bündelung ihrer Ressourcen sowie eine effizientere Kriminalprävention zur Verhinderung der Cyberkriminalität angestrebt.[57] Mit dem aus dem Cyberboard entstandenen «Cyber-Case» hat die Schweiz ein Gremium, in dem sowohl kantonale als auch eidgenössische Staatsanwälte unter anderem juristische Fragen klären. Ferner bietet der Cyber-Case Raum, um Wissen und Erfahrungen im Bereich der Strafverfolgung der Cyberkriminalität auszutauschen. Durchgeführt wird der Cyber-Case zwei bis dreimal jährlich unter der Leitung der Bundesanwaltschaft (BA).[58]

---

53 Website der Konferenz der kantonalen Polizeikommandanten zum Thema Kriminalität.

54 Medienmitteilung der KKPJD zum NEDIK.

55 Medienmitteilung der KKPJD zum NEDIK.

56 Bericht des Bundesrates vom 8. Dezember 2023 in Erfüllung der Postulate 19.4016 Feri Yvonne vom 14. September 2019 und 19.4105 Regazzi Fabio vom 24. September 2019, S. 34.

57 Stellungnahme des Bundesrats vom 20. Februar 2019 zur Interpellation 18.4121 Yvonne Feri (N) vom 29. November 2018: «Immer mehr Kinder werden im Internet von fremden Personen sexuell angemacht. Was unternimmt der Bundesrat?».

58 Tätigkeitsbericht der Bundesanwaltschaft 2022, S. 36.

IV. Mögliche rechtliche Auswirkungen des CSA-Verordnungsvorschlags auf die Schweiz

A. Kein Schengen-Besitzstand

Le règlement n'entrerait dans le champ d'application d'aucun accord conclu entre la Suisse et l'UE et ne constituerait notamment pas un développement de l'acquis de Schengen. La proposition de règlement a pour base légale une disposition du TFUE en lien avec le marché intérieur de l'UE, à savoir l'art. 114 qui prévoit la mise en place de mesures destinées à assurer le fonctionnement du marché intérieur.

B. Mögliche rechtliche Auswirkungen des CSA-Verordnungsvorschlags auf die Anbieter, die in der Schweiz ansässig sind

Wenn der CSA-Verordnungsvorschlag in seiner durch die Kommission vorgeschlagenen Version angenommen wird, könnte dies folgende Auswirkungen auf die in der Schweiz ansässigen Anbieter haben:

- Der CSA-Verordnungsvorschlag ist auf die Anbieter einschlägiger Dienste der Informationsgesellschaft (s. Kapitel II.A) anwendbar, die ihre Dienste in der EU anbieten – unabhängig von ihrem Niederlassungsort (Art. 1 Abs. 2 CSA-VO-V). Nach den Erwägungen zum CSA-Verordnungsvorschlag sollen die Vorschriften zur Anwendung kommen, wenn die Anbieter «in der Union Dienstleistungen anbieten, belegt durch eine wesentliche Verbindung zur Union» (Erwägung 6 zum CSA-VO-V). Eine wesentliche Verbindung zur EU soll dann vorliegen, «wenn der einschlägige Dienst der Informationsgesellschaft eine Niederlassung in der Union hat, oder – in Ermangelung einer solchen – anhand der Existenz einer erheblichen Zahl von Nutzern in einem oder mehreren Mitgliedstaaten oder der Ausrichtung von Tätigkeiten auf einen oder mehrere Mitgliedstaaten beurteilt werden» (Erwägung 11 zum CSA-VO-V). Die *Ausrichtung der Tätigkeiten auf einen oder mehrere Mitgliedstaaten* soll anhand aller relevanten Umstände geprüft werden, einschliesslich Faktoren wie:
    - der Verwendung einer in dem betreffenden Mitgliedstaat gebräuchlichen Sprache oder Währung,
    - der Möglichkeit, Produkte oder Dienstleistungen zu bestellen,
    - der Nutzung einer nationalen Domäne oberster Stufe,
    - der Verfügbarkeit einer Software-Anwendung im jeweiligen nationalen App-Store,
    - der Schaltung lokaler Werbung oder von Werbung in der im betreffenden Mitgliedstaat verwendeten Sprache, oder
    - dem Management der Kundenbeziehungen, zum Beispiel durch die Bereitstellung eines Kundendienstes in der im betreffenden Mitgliedstaat gebräuchlichen Sprache.

Das Vorhandensein einer wesentlichen Verbindung sollte auch dann angenommen werden, wenn ein Diensteanbieter seine Tätigkeit nach Artikel 17 Absatz 1 Buchstabe c der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates[59] auf einen oder mehrere Mitgliedstaaten ausrichtet. Die blosse technische Zugänglichkeit einer Website in der EU soll allerdings nicht ausreichen, damit allein aus diesem Grund eine wesentliche Verbindung angenommen wird.

[59] Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (ABl. L 351 vom 20.12.2012, S. 1).

Der Anwendungsbereich wird damit potentiell weit gezogen. Vor diesem Hintergrund ist davon auszugehen, dass **auch Schweizer Dienste**, die in der EU Dienstleistungen anbieten, **unter den Anwendungsbereich der vorgeschlagenen CSA-Verordnung fallen** werden (Art. 1 Abs. 2 CSA-VO-V).[60] Wollen die Anbieter weiterhin in der EU tätig bleiben, müssen sie die CSA-Verordnung einhalten. Schweizer Hostingdienste und Anbieter interpersoneller Kommunikationsdienste können damit mittels Aufdeckungsanordnung zu Installation und Betrieb von Technologien verpflichtet werden, um die Verbreitung von bekannten oder neuen Darstellungen sexuellen Kindesmissbrauchs zu erkennen und zu melden. Auch sind App-Anbieter von dem CSA-Verordnungsvorschlag betroffen: Sie müssen verhindern, dass Minderjährige Apps herunterladen, bei denen die Wahrscheinlichkeit von Grooming hoch ist (Art. 6 Abs. 1 CSA-VO-V). App-Anbieter werden deshalb vor allem dann betroffen sein, wenn auch Kinder und Jugendliche den Dienst in Anspruch nehmen können.[61]

- Die Anbieter einschlägiger Dienste der Informationsgesellschaft, die ihre **Hauptniederlassung nicht in der EU** haben, müssen einen **Rechtsvertreter**in einem der Mitgliedstaaten, in dem der Anbieter seine Dienste anbietet, ansässig oder niedergelassen ist, benennen (Art. 24 Abs. 1 CSA-VO-V). Gemäss Art. 24 Abs. 3 CSA-VO-V ist dieser so zu beauftragen, dass er anstelle des Anbieters von der zuständigen Behörde für die Entgegennahme, Einhaltung und Durchsetzung von Beschlüssen im Zusammenhang mit dem CSA-Verordnungsvorschlag, einschliesslich Aufdeckungsanordnungen, Entfernungsanordnungen und Sperranordnungen, in Anspruch genommen werden kann. Der Rechtsvertreter kann zudem gemäss Art. 24 Abs. 5 CSA-VO-V für Verstösse des Anbieters gegen die Pflichten aus der Verordnung haftbar gemacht werden, wobei dadurch die Haftbarkeit des Anbieters unberührt bleibt. Die Vertreter müssen von den Koordinierungsbehörden, anderen zuständigen Behörden der Mitgliedstaaten und der Kommission für alle Fragen zur Umsetzung des CSA-Verordnungsvorschlags in Anspruch genommen werden können (Art. 24 Abs. 3 CSA-VO). Das gilt auch für die Aufdeckungsanordnungen.[62]
- Der Anbieter ohne Niederlassung in der EU gilt als der rechtlichen Zuständigkeit des Mitgliedstaates unterworfen, in dem sein **Rechtsvertreter ansässig oder niedergelassen** ist (Art. 33 Abs. 2 CSA-VO-V). Benennt ein Anbieter keinen Rechtsvertreter gemäss Art. 24 CSA-VO-V, so liegt die rechtliche Zuständigkeit bei allen Mitgliedstaaten (Art. 33 Abs. 2 CSA-VO-V).[63]

Für die Durchsetzung von Aufdeckungs- und sonstigen Anordnungen gegenüber Anbietern mit Niederlassung in der Schweiz, die in den Anwendungsbereich des CSA-Verordnungsvorschlags fallen, folgt daraus:

- Les fournisseurs suisses de service devraient tout d'abord désigner un représentant légal dans l'UE. Ils devront se conformer aux injonctions de détection, de retrait et de blocage qui leur seront soumises. Ces injonctions pourront être transmises au représentant légal d'un fournisseur suisse de services qui devra les faire exécuter par le fournisseur de services. Ainsi, il devra s'assurer que le fournisseur de services détecte, retire et bloque l'accès à des données sur ordre d'autorités étrangères. Cependant, les injonctions mises en place par le présent règlement concernent la phase d'investigation ou éventuellement celle qui fait suite à une procédure judiciaire pour le retrait, mais non la procédure judiciaire en tant que telle.

---

60 Analysedokument «Die Schweiz und die Digitalstrategie der Europäischen Union» des UVEK, EDA, EFD, WBF, EDI und EJPD vom 15. März 2013.

61 Analysedokument «Die Schweiz und die Digitalstrategie der Europäischen Union» des UVEK, EDA, EFD, WBF, EDI und EJPD vom 15. März 2013, S. 22.

62 Schriftliche Stellungnahme des EDÖB vom 4. April 2023.

63 Analysedokument «Die Schweiz und die Digitalstrategie der Europäischen Union» des UVEK, EDA, EFD, WBF, EDI und EJPD vom 15. März 2013, S. 21 f. (Massnahme 6).

Pour la procédure judiciaire en tant que telle, la proposition de règlement prévoit que les autorités répressives et judiciaires se conforment au droit applicable (art. 22, par. 1, pt. e CSA-VO-V). Ce point est renforcé par le fait que les règlementations en matière de coopération pénale internationale ne sont pas mentionnées à l'art. 1, par. 3 de la proposition de présent règlement. Ni la règlementation sur la décision d'enquête européenne, ni la nouvelle règlementation e-evidence ne sont mentionnées. Ainsi, les procédures pénales seront menées selon le droit interne de chaque État et l'entraide sera demandée et accordée selon les règles en vigueur. L'État qui aura émis l'injonction de détection p.ex. devra ensuite demander l'entraide à la Suisse pour utiliser les données dans une procédure pénale, ou en tout cas devra le faire tant que la nouvelle règlementation e-evidence n'est pas en force.

Les fournisseurs suisses de services devront donc se conformer aux règles mises en place par la proposition de règlement sous revue et adapter leurs procédures afin qu'elles soient compatibles avec ces règles.

- La proposition de règlement ne semble cependant pas prévoir un accès transnational. Ainsi, c'est l'autorité du lieu où est établis le fournisseur suisse de services (ou son représentant légal) qui soumet les injonctions de détection, de blocage et de retrait. Les fournisseurs de services pourraient donc choisir de nommer un représentant légal dans un État de l'UE dont les lois sont proches du système suisse ou dont la langue est la même. Une règle sur les conflits de lois ne semble pas être incluse dans la version actuelle de la proposition de règlement.

C. Mögliche rechtliche Auswirkungen des CSA-Verordnungsvorschlags auf Personen in der Schweiz

Der CSA-Verordnungsvorschlag, und damit auch die hier besonders interessierenden Aufdeckungsanordnungen, könnten auch Personen mit Sitz oder Wohnsitz in der Schweiz betreffen, so dass ihre Kommunikation Gegenstand von Anordnungen würde. Der CSA-Verordnungsvorschlag lässt einige zentrale Fragen unbeantwortet, doch grundsätzlich wäre dies in folgenden drei Konstellationen der Fall:

- Personen in der Schweiz nutzen den **Dienst eines in der EU ansässigen Anbieters**. In dieser Konstellation müssen sie damit rechnen, von Aufdeckungs-, Entfernungs- und Sperranordnungen betroffen zu sein.[64]
- Personen in der Schweiz nutzen den Dienst eines **in der Schweiz ansässigen** Anbieters, der seinen **Dienst (auch) in der EU** anbietet. Dadurch, dass der Anbieter seine Dienstleistung auch in der EU anbietet, ist der CSA-Verordnungsvorschlag auch auf ihn anwendbar (Art. 1 Abs. 2 CSA-VO-V).
- **Personen** in der Schweiz nutzen den Dienst eines **weder in der EU noch in der Schweiz ansässigen Anbieters**, aber dieser Anbieter bietet seine **Dienste auch in der EU an** (womit er unter den CSA-VO-V fällt).

Es kann nicht ausgeschlossen werden, dass in der Praxis eine Aussonderung der Kommunikation zwischen Personen in der Schweiz unterbleibt, denn gemäss den Erwägungsgründen 6 und 11 des CSA-Verordnungsvorschlags soll die Verordnung für alle Anbieter gelten, die innerhalb der EU Dienstleistungen erbringen, unabhängig davon, wo sie niedergelassen sind, sofern eine **wesentliche Verbindung zur EU** besteht. Dies ist nach Erwägungsgrund 11 der Fall, wenn der Anbieter der relevanten Dienste der Informationsgesellschaft über eine Niederlassung in der EU verfügt oder wenn aufgrund einer erheblichen Zahl von Nutzerinnen und

[64] Schriftliche Stellungnahme des EDÖB vom 4. April 2023.

Nutzer in einem oder mehreren EU-Mitgliedsstaaten von einer Ausrichtung der Tätigkeit auf diese anzunehmen ist. Sofern diese Merkmale beim genutzten Dienstleister zutreffen, ist davon auszugehen, dass auch Personen in der Schweiz von dem CSA-Verordnungsvorschlag betroffen sein werden.

D. Erlass und Anfechtung der Aufdeckungsanordnungen

Art. 7 CSA-VO-V legt das Verfahren für den **Erlass** von Aufdeckungsanordnungen fest. Darin involviert sind der betroffene Anbieter von Hostingdiensten bzw. der Anbieter interpersoneller Kommunikationsdienste (Art. 7 Abs. 1, 2 und 3 CSA-VO-V). Die (potentiell) betroffenen Nutzerinnen und Nutzer nehmen an dem der Aufdeckungsanordnung zugrundeliegenden Erlassverfahren nicht teil (vgl. Art. 7 CSA-VO-V).

Die Aufdeckungsanordnung kann sowohl von den betroffenen Diensten als auch von den Nutzern, «die von den zu deren Ausführung ergriffenen Massnahmen betroffen sind», **angefochten** werden (Art. 9 Abs. 1 CSA-VO-V). Die erlassene Aufdeckungsanordnung wird an die Hauptniederlassung des Anbieters oder an seinen benannten Rechtsvertreter gerichtet (Art. 8 Abs. 2 CSA-VO-V). Sie wird nicht direkt an die betroffenen Nutzerinnen und Nutzer übermittelt. Weil diese aber die Aufdeckungsanordnung anfechten dürfen (Art. 9 Abs. 1 CSA-VO-V), setzt die Ausübung ihres Rechts eine **Information über die Existenz der Anordnung** voraus, die dem Anbieter obliegt (Art. 10 Abs. 6). Art. 10 Abs. 6 CSA-VO-V äussert sich zur Information der Nutzerinnen und Nutzer im Zusammenhang mit der Aufdeckungsanordnung. Der Wortlaut dieser Bestimmung wirft die Frage auf, ob bloss allgemein über die Tatsache, dass Technologien zur Ausführung der Aufdeckungsanordnungen eingesetzt werden können, zu informieren ist oder ob es sich um eine Informationspflicht über jede *konkrete Aufdeckungsanordnung* handelt (zum Vergleich: siehe die klaren Formulierungen von Art. 15 Abs. 3 und Art. 18 Abs. 4 CSA-VO-V). Letzteres erscheint mit Blick auf das Recht auf einen wirksamen Rechtsbehelf (Art. 9 Abs. 1 CSA-VO-V), welches nicht illusorisch sein sollte, sachgerechter. Zudem dürfte sich dies auch aus Art. 10 Abs. 5 CSA-VO-V ergeben, indem von «Erkennungsverfügung» und nicht von «*einer* Erkennungsverfügung» die Rede ist sowie der Tatsache, dass diese Klarstellung in Art. 10 CS-V-VO, welche sich an Hosting-Dienstleister und Anbieter von interpersonellen Kommunikationsdiensten richtet, gegen welche eine Aufdeckungsverfügung ergangen ist (s. Art. 1 Abs. 1 CSA-V-VO).

Der Begriff «Nutzer» ist in Artikel 2 Bst. h CSA-VO-V definiert, die Wendung «die von den zu deren Ausführung ergriffenen Massnahmen *betroffen* sind» (Art. 9 Abs. 1 CSA-VO-V) wird hingegen nicht präzisiert. Deshalb ist nicht ganz klar, wem das Recht auf einen wirksamen Rechtsbehelf nach Art. 9 Abs. 1 CSA-VO-V tatsächlich zusteht bzw. ob die «Betroffenheit» allenfalls an einschränkenden Kriterien zu messen ist. Es ist wohl davon auszugehen, dass sämtliche Nutzerinnen und Nutzer eines von einer (Aufdeckungs-)Anordnungen betroffenen Dienstes zur Anfechtung berechtigt sind. Damit ist der Kreis der Anfechtungsberechtigen grundsätzlich gross. Zu beachten ist allerdings, dass (Aufdeckungs-)Anordnungen nur nach einer Abwägung der verschiedenen Interessen erlassen werden sollten und gezielt und präzise sein müssen.[65] Dies könnte u.a. durch eine Beschränkung der (Aufdeckungs-)Anordnungen auf bestimmte Nutzer oder Nutzergruppen erfolgen. Daraus resultierte zumindest mittelbar eine Beschränkung des Kreises der von Aufdeckungsanordnungen betroffenen Personen.

E. Verhältnismässigkeit der Aufdeckungsanordnungen

Ganz grundsätzlich kann fraglich sein, ob die vorgesehene Information über die Existenz einer Aufdeckungsanordnung (s. oben, Kap. IV.D) nicht dazu führt, dass Nutzerinnen und Nutzer mit kriminellen Absichten auf andere, nicht im Anwendungsbereich des CSA-Verordnungsvor-

[65] Vgl. Erwägungsgründe 21 und 22 sowie die Art. 7 und 8 des CSA-Verordnungsvorschlags.

schlags liegende Dienste ausweichen bzw. Anbieter zu nutzen versuchen, die Aufdeckungsanordnungen leerlaufen lassen oder sich der EU-Jurisdiktion zu entziehen versuchen.[66] Damit stellt sich die Frage, ob und inwiefern der Erlass von Aufdeckungsanordnungen tatsächlich geeignetes Mittel ist, sexuellen Missbrauch im Internet zu erkennen und zu verhindern. Eine vollständige Verhinderung bzw. Unterbindung von sexuellem Missbrauch an Kindern im Internet, bzw. eine vollständige Verhinderung der Verbreitung von Darstellungen, welche Kindesmissbrauch zum Gegenstand haben, ist durch die Aufdeckungsanordnungen jedenfalls nicht möglich. Allerdings können diese Anordnungen dazu beitragen, dass die Dienste in geringerem Umfang für die Verbreitung derartiger Inhalte genutzt werden. Ob die Aufdeckungsanordnung zur Verhinderung der Verbreitung von Material über sexuellen Kindesmissbrauch geeignet ist, kann deshalb nicht pauschal verneint werden.[67]

Fraglich ist jedoch, ob sich das Ziel nicht auch mit weniger weitgehenden Mitteln erreichen liesse und ob die Aufdeckungsanordnung insgesamt einer Interessenabwägung, insbesondere mit Blick auf die Privatsphäre und das Recht auf informationelle Selbstbestimmung sowie der Meinungsäusserungsfreiheit der Nutzenden standhalten kann. In der Begründung der Verhältnismässigkeit, die dem CSA-Verordnungsvorschlag vorangeht, nimmt die Kommission auf die im Verordnungsvorschlag vorgesehenen Schutzvorkehrungen Bezug. Mit diesen soll sichergestellt werden, dass die zur Aufdeckung, Meldung und Entfernung eingesetzten Technologien diejenigen Mittel und Techniken sind, welche am wenigsten in die Privatsphäre eingreifen und alle erforderlichen Überprüfungen anonym durchgeführt werden.

Mit Urteil vom 13. Februar 2024 hat der **EGMR im Fall Podchasov vs. Russland**[68] entschieden, dass generelle Speicherung der Internetkommunikation (Inhalt und Kommunikationsranddaten) einen schweren Eingriff in das Recht auf Achtung des Privatlebens (Art. 8 EMRK) darstelle. Für die Rechtmässigkeit des behördlichen Zugriffs auf diese Daten brauche es deshalb verfahrensrechtliche Sicherungen, um Willkür und Missbrauch auszuschliessen und die Verhältnismässigkeit sicherzustellen. Die Verpflichtung, verschlüsselte Daten zu entschlüsseln, sei in jedem Fall unverhältnismässig. Die Verschlüsselung diene dem Schutz des Privatlebens und anderer Freiheitsrechte, wie z.B. der Meinungsäusserungsfreiheit. Zudem schütze sie Unternehmen vor Hacking, Identitäts- und Personendatendiebstahl, Betrug und unerlaubter Offenlegung von vertraulichen Informationen. Eine Entschlüsselung müsste über den Einbau von «Backdoors» erfolgen. Dies würde aber die Verschlüsselung aller Nutzer schwächen. Backdoors ermöglichten eine geheime Überwachung und könnten auch von Kriminellen genutzt werden. Die Verschlüsselung könne zwar ebenfalls zu kriminellen Aktivitäten genutzt werden, doch gebe es geeignetere Mittel als die Entschlüsselung, um diese zu bekämpfen, weshalb sich die Verpflichtung, zu entschlüsseln, als unverhältnismässig erweise. Der EGMR folgt damit der gemeinsamen Stellungnahme 4/2022[69] des Europäischen Datenschutzaustausches und des Europäischen Datenschutzbeauftragten zum CSA-Verordnungsvorschlag.

F. Rechtmässigkeit von Aufdeckungs-, Entfernungs- oder Sperranordnungen

In diesem Abschnitt werden mögliche rechtliche Auswirkungen des CSA-Verordnungsvorschlags thematisiert. Dabei wird auf die Rechtmässigkeit einer Aufdeckungsanordnung gegenüber Schweizer Dienstleistern, auf Probleme im Zusammenhang mit der Erhebung von Einwohnerdaten in der Schweiz und auf die Verwertbarkeit der Daten in einem sich möglicherweise daraus ergebenden Strafverfahren wegen sexuellem Kindsmissbrauch fokussiert.

---

66 Vgl. Stellungnahme der Generalstaatsanwaltschaft Köln, S. 8.

67 Vgl. Stellungnahme der Generalstaatsanwaltschaft Köln, S. 8.

68 Urteil des Europäischen Gerichtshofs für Menschenrechte Podchasov v. Russia vom 13. Februar 2024.

69 Siehe Fussnote 13.

1. Anordnungen gegenüber Diensten in der Schweiz

Fraglich ist, ob und inwiefern sich Aufdeckungs- und andere Anordnungen, welche an in der Schweiz ansässige Anbieter gerichtet sind, mit der **Souveränität der Schweiz** und den Regeln der (internationalen) **Rechts- oder Amtshilfe** vertragen. Hier stellt sich insbesondere die Frage, ob in der Schweiz ansässige Anbieter einer Aufdeckungs-, Entfernungs- oder Sperranordnung **Folge leisten** dürfen oder sie sich gemäss schweizerischem Recht **strafbar** machen:

Gemäss Artikel 271 Ziffer 1 StGB wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe, in schweren Fällen mit Freiheitsstrafe nicht unter einem Jahr bestraft, wer auf schweizerischem Gebiet ohne Bewilligung für einen fremden Staat Handlungen vornimmt, die einer Behörde oder einem Beamten zukommen. Damit sollen die Ausübung fremder Staatsgewalt auf dem Gebiet der Schweiz verhindert sowie das staatliche Machtmonopol und die Souveränität der Schweiz geschützt werden.[70] Die Ausübung fremder Staatsgewalt ist untersagt, wenn die vorzunehmende Handlung von den schweizerischen Behörden nicht bewilligt wurde.[71] Vor diesem Hintergrund ist es keineswegs ausgeschlossen, dass sich der Anbieter einschlägiger Dienste der Informationsgesellschaft, der einer Aufdeckungsanordnung Folge leistet, nach Artikel 271 StGB strafbar machen kann.[72]

Zwischen dem CSA-Verordnungsvorschlag und dem Schweizer Recht besteht damit ein Spannungsverhältnis: Führt ein Anbieter eine Anordnung nicht aus, wird er entsprechend dem Recht des zuständigen EU-Mitgliedstaates bestraft. Führt er die Aufdeckungsanordnung hingegen aus, begeht er unter Umständen eine Straftat nach schweizerischem Recht.

Während ein grundsätzliches Konfliktpotenzial zwischen souveränitätsrechtlich ausgestalteten Konzepten einerseits und extraterritorialen Anordnungsmöglichkeiten andererseits besteht, ist eine punktuelle Aufweichung internationaler Rechtshilfeschranken allerdings nicht ausgeschlossen. Jüngere Entwicklungen im Bereich der Internetkriminalität lassen eine Verlagerung von der klassischen Rechtshilfe hin zu direkteren Strafverfolgungsmechanismen erkennen.

So bezweckt etwa das **Übereinkommen des Europarates über die Cyberkriminalität** (nachfolgend **Budapest-Konvention**)[73] eine schnelle, wirksame und umfassende Zusammenarbeit zwischen den Vertragsstaaten unter anderem im Kampf gegen Kinderpornographie (Art. 9 Budapest-Konvention). Artikel 32 der Budapest-Konvention sieht vor, dass eine Vertragspartei ohne Genehmigung einer anderen Vertragspartei auf gespeicherte Computerdaten[74] zugreifen oder diese empfangen darf, die sich in deren Hoheitsgebiet befinden, wenn sie über die freiwillige Zustimmung der Person verfügt, die befugt ist, die Daten mittels dieses Computersystems[75] an sie weiterzuleiten (was primär nach dem nationalen Recht des Staates zu beurteilen ist, in welchem die betreffende Person handelt). Bei rechtmässiger und freiwilliger Zustimmung

---

70 Urteil des Bundesgerichts 6B_804/2018 vom 4. Dezember 2018, E. 3; OFK StGB-BERNARD A. ISENRING, Art. 271 Rz. 1, in: Andreas Donatsch (Hrsg.), StGB/JStGB Kommentar – Mit weiteren Erlassen und Kommentar zu den Strafbestimmungen des SVG, BetmG, AIG und OBG, 3. Auflage, Zürich 2022.

71 Urteil des Bundesgerichts 6B_804/2018 vom 4. Dezember 2018, E. 3.

72 Ist der Anbieter einschlägiger Dienste der Informationsgesellschaft eine natürliche Person, wird er nach Art. 271 Ziff. 1 StGB mit einer Freiheitstrafe oder mit einer Busse bestraft. Meistens wird es sich aber um eine juristische Person handeln. In einem solchen Fall sieht Art. 102 Abs. 1 StGB vor, dass primär die natürliche Person zu bestrafen ist. Kann diese wegen einer mangelhaften Organisation des Unternehmens nicht identifiziert werden, wird die Straftat dem Unternehmen zugerechnet und dieses kann bei Vorliegen der entsprechenden Sachverhaltsmerkmale mit einer Busse bis zu 5 Millionen Franken bestraft werden (Art. 102 Abs. 1 StGB).

73 Übereinkommen über die Cyberkriminalität vom 23. November 2001, SR 0.311.43.

74 «**Computerdaten**» bedeutet gemäss Konvention jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschliesslich eines Programms, das die Ausführung einer Funktion durch ein Computerprogramm auslösen kann (Art. 1 Bst. b des Übereinkommens über Computerkriminalität des Europarates vom 23.11.2001 (SEV Nr. 185).

75 «Computersystem» bedeutet eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitungen durchführen (Art. 1 Bst. a des Übereinkommens über Computerkriminalität des Europarates vom 23.11.2001 (SEV Nr. 185).

der befugten Person können folglich innerhalb der Budapest-Konventionsvertragsstaaten grenzübergreifend Daten herausgegeben und empfangen werden. Das derzeit zur Unterzeichnung offenstehende (und noch nicht in Kraft getretene) zweite Zusatzprotokoll zur Budapest-Konvention[76] dürfte solche direkten Kooperationsmöglichkeiten weiter verstärken.

Im Bereich der elektronischen Datenerhebung gilt zudem gemäss herrschender Schweizer Rechtsprechung das sogenannte **Zugriffsprinzip**: Wer über einen Internetzugang im Inland einen abgeleiteten Internetdienst benutzt, der von einer ausländischen Firma angeboten wird, handelt nicht «im Ausland». Auch der blosse Umstand, dass die elektronischen Daten des betreffenden abgeleiteten Internetdienstes auf Servern (bzw. Cloud-Speichermedien) im Ausland verwaltet werden, lässt eine von der Schweiz aus erfolgte gesetzeskonforme Online-Recherche aus Sicht Bundesgerichts nicht als unzulässige Untersuchungshandlung auf ausländischem Territorium erscheinen.[77]

Ob die Schweiz nun im Kontext von Aufdeckungs- und anderen Anordnungen, welche aus dem Ausland an in der Schweiz ansässige Anbieter gerichtet sind an der grundsätzlichen Rechtswidrigkeit extraterritorialer Anordnungen festhalten möchte und inwiefern eine punktuelle Aufweichung ihres Souveränitätsverständnisses angezeigt sein könnte, wird im Kontext der internationalen Entwicklungen zu entscheiden sein. Die Schweiz verfolgt daher diese Entwicklungen bei internationalen Organisationen und bei ihren wichtigen Partnern (USA, EU) seit längerem aufmerksam. Angesichts der immer noch zunehmenden globalen Verflechtung ist die Notwendigkeit internationaler Zusammenarbeit und damit verbunden eine punktuelle «Durchbrechung» der auf dem Souveränitätsgedanken basierenden Prinzipien seitens der Schweiz auch im Justizbereich unbestritten. Beispiele für eine solche Durchbrechung sind mitunter ganz generell die Anerkennung der Rechtsprechung des EGMR sowie die Zulassung der Zustellung von bestimmten Beweiserhebungen und Dokumenten abseits des Rechtshilfeweges oder andere staatsvertragliche Verpflichtungen. Internationale Abkommen wie die Budapest-Konvention sowie die liberale Ausnahmebewilligungspraxis[78] schränken den Anwendungsbereich von Artikel 271 StGB bereits heute ein. Gerade im Amts- und Rechtshilfeverkehr ist folglich eine Tendenz hin zum Abbau souveränitätsrechtlicher Hindernisse festzustellen.[79] Diese Tendenz dürfte insbesondere auch im Bereich e-Evidence und anderweitiger (digitaler) Kooperationsformen in Strafsachen, wie sie z.B. im noch nicht in Kraft getretenen zweiten Zusatzprotokoll der Budapest-Konvention anvisiert sind, weiterhin zunehmen.

Während ein **grundsätzliches Konfliktpotenzial** zwischen dem Territorialitätsprinzip und extraterritorialen Anordnungsmöglichkeiten besteht, ist ein tendenzieller, punktueller Abbau von Rechtshilfeschranken keineswegs auszuschliessen. Untersuchungen im Bereich des Kindes- und Jugendschutzes im Internet[80] oder die angestrebte Regulierung von Kommunikationsplattformen sind weitere Regelungsgegenstände, die im Hinblick auf Aufdeckungsanordnungen und mögliche Souveränitätskonflikte zu berücksichtigen sein werden.

Im Bericht des Bundesrates «Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmissbrauch via Live-Streaming» wird die Schwierigkeit thematisiert, elektronische Beweismittel zu sichern und grenzüberschreitend Zugang zu diesen zu erlangen. Die bestehenden Verfahren zum grenzüberschreitenden Zugriff auf Daten sind gemäss

---

76 Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE n° 224).

77 BGE 143 IV 270, S. 287 f. E. 7.10 m.H. Allerdings kann die Würdigung, inwiefern solche Datenerhebungen von einem ausländischen Staat hingegen als Eingriff in ihre Souveränität beurteilt würden, von derjenigen des Bundesgerichts abweichen.

78 BSK StGB-HUSMANN, Art. 271 Rz. 78 ff.

79 BSK StGB-HUSMANN, Art. 271 Rz 9 m.V.a. GAUTHEY/MARKUS, ZSR 2015, 361.

80 Damit werden z.B. die Untersuchungen im Zusammenhang mit dem Bericht zum Postulat 19.4016 Yvonne Feri vom 12. September 2019: «Sexuelle Gewalt an Kindern im Internet. Was macht das Bundesamt für Polizei?» oder zum Postulat 19.4105 Fabio Regazzi (N) vom 24. September 2019: «Die Täter vor dem Live-Streaming eines Kindsmissbrauchs stoppen, und der Kinderprostitution im Internet wirksame Grenzen setzten» gemeint.

den Schlussfolgerungen des Berichts nicht mehr zeitgemäss. Der Bericht zeigt auf, dass auch Handlungsbedarf besteht, um aus den verschiedenen Lösungsmöglichkeiten die optimale zu bestimmen. Wichtig sei zudem, die Analyse zum e-Evidence-Paket der EU zur Kenntnis zu nehmen, vorab hinsichtlich möglicher Kollisionen mit Schweizer Recht.[81] Die e-Evidence-Gesetzgebung der EU wird am 28. Juli 2026 in Kraft treten. Das Bundesamt für Justiz hat im Jahr 2023 einen Bericht zur e-Evidence-Vorlage der EU verfasst, in dem es einerseits den Inhalt der Vorlage analysiert, andererseits die Auswirkungen auf die Schweiz sowie die Unterschiede zum US-CLOUD Act beleuchtet.

2. Problematik der Erhebung von Einwohnerdaten

Ob Überwachungsanordnungen der EU, welche sich auf Personen in der Schweiz auswirken, rechtmässig sind, ist ebenso eine offene Rechtsfrage. Heute weisen zahlreiche Sachverhalte - und damit auch Strafverfahren - regelmässig extraterritoriale Komponenten auf. Praktisch bedeutet dies, dass unter Einhaltung konkreter (Straf-)Verfahrensgarantien gewisse Zugriffsmöglichkeiten auf Daten bereits bestehen.

Das geltende schweizerische Recht sieht vor, dass Verbindungsdaten (wie auch Inhaltsdaten) unter bestimmten Voraussetzungen durch Echtzeitüberwachung erhoben werden können, wobei sich eine strafprozessuale Überwachung auf den Deliktskatalog gemäss Artikel 3 BÜPF i.V.m. Artikel 269 StPO beziehen muss. Artikel 30 und 33 der Budapest-Konvention verlangen, dass die gemäss einer Überwachungsanordnung nach BÜPF zugänglichen Verkehrsdaten bei der internationalen Zusammenarbeit unter Umständen auch den zuständigen ausländischen Behörden zugänglich gemacht werden sollen.

Durch Überwachungsanordnungen erlangte Verbindungsdaten (wie auch Inhaltsdaten) müssen aber grundsätzlich via Rechtshilfeersuchen beantragt werden (Art. 18*a* und 18*b* IRSG). Nach Artikel 33 der Budapest-Konvention muss jede Vertragspartei für eine andere Vertragspartei Verkehrsdaten in Echtzeit in Zusammenhang mit bestimmten Kommunikationen, die mittels eines Computersystems übermittelt werden, erheben und ist verpflichtet, in diesem Bereich zusammenzuarbeiten. Dabei ist – wie es in Artikel 34 der Budapest-Konvention ersichtlich ist – die Verpflichtung zur Rechtshilfe bei der Erhebung *von Inhaltsdaten* sehr restriktiv ausgestaltet, weil das Abfangen dieser Daten stark in die Privatsphäre eingreift. Diese Form der Rechtshilfe wird nur gewährt, soweit die anwendbaren Verträge und innerstaatlichen Rechtsvorschriften dies gestatten. Gemäss Artikel 18*b* IRSG dürfen vor Abschluss eines Verfahrens nur Verkehrsdaten an das Ausland übermittelt werden, aber keine Inhaltsdaten, und dies auch nur unter Beachtung der folgenden Voraussetzungen.

Gemäss Artikel 18b IRSG dürfen elektronische Verkehrsdaten vor Abschluss eines Rechtshilfeverfahrens an die ersuchende Behörde weitergegeben werden, wenn die vorläufigen Massnahmen zeigen, dass sich der Ursprung der Kommunikation, die Gegenstand des Ersuchens ist, in einem anderen Staat befindet (Absatz 1 Buchstabe a) oder diese Daten von der Vollzugsbehörde aufgrund der Anordnung einer bewilligten Echtzeitüberwachung gem. Art. 269-281 StPO erhoben werden (Absatz 1 Buchstabe b). Da eine solche Vorabübermittlung grundsätzlich von den im Rechtshilfesystem etablierten Grundsätzen abweicht, sind zu Gunsten der betroffenen Person dreierlei Schutzmassnahmen vorgesehen:

- Die Überwachungsmassnahme bedarf der Genehmigung des zuständigen Zwangsmassnahmengerichts nach Artikel 272 StPO (Art. 18*b* Abs. 1 Bst. b IRSG);
- die übermittelten Daten dürfen vor Abschluss des Rechtshilfeverfahrens nicht als Beweismittel verwendet werden, sodass die Möglichkeit besteht, die übermittelten Informationen aus den ausländischen Akten entfernen zu lassen, wenn eine Beschwerde gutgeheissen

[81] Bericht des Bundesrates in Erfüllung der Postulate 19.4016 Feri Yvonne vom 14. September 2019 und 19.4105 Regazzi Fabio vom 24. September 2019, « Massnahmen zur Bekämpfung von sexueller Gewalt an Kindern im Internet und Kindsmissbrauch via Live-Streaming, vom 8. Dezember 2023, S. 32.

wurde (Art. 18*b* Abs. 2 IRSG); und

- diese Übermittlung unterliegt der unverzüglichen Kontrolle des Bundesamts für Justiz (vgl. Art. 18b Abs. 3 IRSG).

Dieser Verfahrensablauf stellt sicher, dass die Einhaltung der Gesetze überprüft und dass bei den schweizerischen ebenso wie bei den ausländischen Behörden interveniert werden kann. Sobald es die Situation erlaubt, in jedem Fall jedoch spätestens vor Abschluss der Strafuntersuchung oder der Einstellung des Verfahrens, muss die betroffene Person über die erfolgte Übermittlung benachrichtigt werden und kann nicht nur gegen die Schlussverfügung, sondern auch gegen die Überwachungsverfügung Beschwerde führen. Bei Gutheissung der Beschwerde muss die ausländische Behörde die Informationen aus ihren Akten entfernen und dies den Schweizer Behörden bescheinigen. Bis die betroffene Person ihre Rechte geltend machen konnte, dürfen die sie betreffenden Informationen nicht als Beweismittel, sondern lediglich zu Ermittlungszwecken verwendet werden.

Angesichts etablierter, innerstaatlicher Strukturen, die eine durch Überwachung angeordnete Datenerhebung sowie Datenweitergabe ans Ausland nur unter restriktiven Voraussetzungen (und jeweils nur via Rechtshilfe) zulassen, sind diese von der EU vorgeschlagenen Massnahmen zum jetzigen Zeitpunkt mit Zurückhaltung zu betrachten. Dies umso mehr, als die damalige Vorsteherin des EJPD gemeinsam mit vier europäischen Kolleginnen und Kollegen im Mai 2023 ihre Bedenken gegenüber den Plänen der EU deponierte und es heute um immer noch laufende Rechtsetzungsarbeiten der EU handelt.

G. Verwertbarkeit der durch eine Aufdeckungsanordnung gewonnenen Beweismittel in einem schweizerischen Strafverfahren

Es stellt sich die Frage, ob die durch eine Aufdeckungsanordnung gewonnenen Beweismittel in einem Strafverfahren in der Schweiz verwertbar sind. Dies ist grundsätzlich zu bejahen.

Des preuves obtenues par des autorités étrangères peuvent être utilisées dans une procédure pénale en Suisse pour autant qu'elles aient été obtenues dans le cadre d'une procédure d'entraide judiciaire en matière internationale. Avec les États de l'UE, la Suisse coopère sur la base de la Convention européenne d'entraide judiciaire (RS 0.351.1) et de son Deuxième Protocole additionnel (RS 0.351.12). Si la Suisse obtient des preuves qui ont été obtenues sur la base d'une injonction de détection par les autorités européennes, pour autant qu'elles soient transmises à la Suisse par le biais d'une procédure d'entraide judiciaire en matière pénale, ces preuves seront exploitables dans la procédure suisse. Ainsi, si, sur la base d'une injonction de détection, les autorités françaises par exemple obtiennent des preuves qui pourraient être utiles à une procédure suisse, elles peuvent en informer les autorités suisses. Si les autorités suisses en sont informées ou en ont connaissance d'une autre manière, elles pourront présenter une demande d'entraide judiciaire en matière pénale à la France afin de les obtenir et de les utiliser dans une procédure pénale suisse.

Les procédures d'entraide judiciaire en matière pénale reposent sur une confiance entre États. La Suisse considérera que les preuves transmises par une autorité européenne ont été obtenues de manière conforme au droit de l'État duquel provient cette autorité. Il n'est pas pertinent de savoir si les preuves ont été obtenues en application du droit national de l'État en question ou en application du droit européen. La seule condition, pour que les preuves soient exploitables dans une procédure pénale suisse, est qu'elles aient été obtenues en respect des normes applicables à l'entraide judiciaire en matière pénale.

V. Würdigung und Ausblick

Die Schweiz hat verschiedene Massnahmen getroffen und ist daran, verschiedene weitere Massnahmen zu schaffen und umzusetzen, um den Schutz von Kindern und Jugendlichen im Internet sicherzustellen. Ein gewisser Handlungsbedarf wurde in den in Kapitel III.A genannten Postulatsberichten identifiziert.

Eine dem Erlass von Aufdeckungsanordnungen vergleichbare Massnahme kennt die Schweiz nicht. Es besteht gegenwärtig auch keine Absicht, eine solche Massnahme einzuführen. Dennoch können Schweizer Dienste, die in der EU ihre Dienstleistungen anbieten, sowie Internetnutzende in der Schweiz von den im CSA-Verordnungsvorschlag vorgesehenen Massnahmen betroffen sein. Aufgrund der in der EU geführten Diskussionen lassen sich die Auswirkungen auf die Schweiz zum jetzigen Zeitpunkt noch nicht abschliessend beurteilen.

Aktuell ist davon auszugehen, dass die Vereinbarkeit von Aufdeckungsanordnungen von EU-Mitgliedstaaten mit der geltenden Schweizerischen Rechtsordnung fraglich ist. Ein Konflikt mit Artikel 271 StGB kann nicht ausgeschlossen werden.

Sollte der CSA-Verordnungsvorschlag durch die EU verabschiedet werden, wäre diese Frage vertieft zu klären.