



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und
Öffentlichkeitsbeauftragter
EDÖB

Der Beauftragte

CH-3003 Bern

POST CH AG

EDÖB; EDÖB-A-AAB03401/1

An die Kommission für Rechtsfragen
des Nationalrats

Parlamentsdienste
Parlamentsgebäude
3003 Bern

Ihr Zeichen:

Unser Zeichen: EDÖB-A-AAB03401/1

Sachbearbeiter/in: Petru Emanuel Zlatescu

Bern, 4. April 2023

Ordnungsantrag vom 10.01.23 betreffend «Chat-Kontrolle»

Vorschlag für eine Verordnung des Europäischen Parlaments und Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vom 11. Mai 2022

Sehr geehrte Frau Präsidentin

Mit E-Mail vom 13. Januar 2023 haben Sie den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) um die Beantwortung mehrerer Fragen betreffend den Verordnungsentwurf der EU-Kommission zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern («Chatkontrolle») gebeten.

A. Einleitende Bemerkungen zum Verordnungsentwurf der EU

1. Stand der Gesetzgebungsarbeiten

Beim Verordnungsentwurf handelt es sich um einen Legislativvorschlag der Europäischen Union (EU). Die vorliegenden Darlegungen des Beauftragten stützen sich auf die im Rahmen des Legislativprozesses publizierten Materialien der EU-Kommission, des Europäischen Datenschutzausschusses (EDSA) und des Europäischen Datenschutzbeauftragten (EDSB). Ferner ist zu betonen, dass sich das Legislativverfahren in dieser Sache in einem frühen Stadium befindet, viele Punkte offenlässt und (grundlegende) Änderungen des Entwurfs noch vorgenommen werden können.

Feldeggweg 1
3003 Bern
Tel. +41 58 462 48 58, Fax +41 58 465 99 96
www.edoeb.admin.ch



EDÖB-A-AAB03401/1

2. Zweck, Umfang, Behörden und Verfahren

a) Zweck und Umfang

Der Entwurf unterwirft die Anbieter von Hosting-Diensten und Anbieter interpersoneller Kommunikationsdienste spezifischen Pflichten, die private Kommunikation ihrer Kundinnen und Kunden zu überwachen, bezüglich

- der Aufdeckung, Meldung, Sperrung und Entfernung von bekannten und neuen Darstellungen von sexuellem Kindesmissbrauch im Internet;
- sowie der Kontaktaufnahme mit Kindern (Grooming).

b) Behörden

Zum Vollzug der geplanten Massnahmen gegen Kindesmissbrauch sieht der Entwurf die Schaffung neuer Behörden vor. Auf Stufe der EU sollen ein Zentrum für die Verhütung und Bekämpfung sexuellen Kindesmissbrauchs mit Sitz in Den Haag und in den Mitgliedstaaten sog. Koordinierungsbehörden geschaffen werden, welchen gegenüber den Anbietern besondere Aufsichts- und Untersuchungsbefugnisse zukommen. Jede Koordinierungsbehörde überwacht die Einhaltung der Pflichten durch die der Verordnung unterstellten Anbieter ihres Zuständigkeitsgebiets, indem sie u.a. das Internet überwacht und Beschwerden des Publikums, namentlich auch von Kindern, entgegennimmt. Stellt eine Koordinationsbehörde fest, dass ein Anbieter Pflichten nach der Verordnung verletzt hat, kann sie Sanktionen bis zu 6% der Jahreseinnahmen verhängen.

c) Verfahren zur Durchführung von Überwachungen

Telekomunternehmen, die Hosting-Dienste erbringen, oder Anbieter interpersoneller Kommunikationsdienste wie Betreiber von Gratisplattformen werden in der Verordnung zu umfassenden Analysen der Kindesmissbrauchs-Risiken und geeigneter Massnahmen zu deren Minderung verpflichtet. Diese Analysen haben sie der zuständigen Koordinierungsbehörde in Berichtsform vorzulegen.

Die Koordinationsbehörde am Niederlassungsstandort ist befugt, bei der örtlichen Justizbehörde des Mitgliedstaates oder einer von Letzterem bezeichneten unabhängigen Verwaltungsbehörde den Erlass einer sog. Aufdeckungsanordnung zu beantragen, die einen bestimmten Dienstanbieter verpflichtet, konkrete Überwachungsmassnahmen durchzuführen. Nach Vorkonsultation des verpflichteten Anbieters, des EU-Zentrums und - im Falle der Überwachung betreffend Grooming - der zuständigen Datenschutzbehörde durch die Koordinationsbehörde entscheidet die zuständige Behörde über die Durchführung der Überwachung. Überwachungen betreffend die Verbreitung von Darstellungen sexuellen Missbrauchs dürfen 24 Monate und solche betreffend Grooming 12 Monate nicht überschreiten.

Gegen die Aufdeckungsanordnung steht den Dienstanbietern der Rechtsweg offen. Sie müssen ihre Nutzerinnen und Nutzer über die Anordnung der Aufdeckungsanordnung informieren. Letztere können die Anordnung ebenfalls gerichtlich anfechten.

d) Meldepflicht

Erhält ein Anbieter Kenntnis von Informationen, die auf einen potenziellen sexuellen Kindesmissbrauch im Internet über seine Dienste hindeuten, meldet er diese unverzüglich dem EU-Zentrum. Die Meldungen erfolgen über ein von diesem betriebenes System und umfassen:

- alle Inhaltsdaten über Kindesmissbrauch im Internet, einschliesslich Bilder und Videos;
- Texte und Sprachnachrichten resp. Transkriptionen von Gesprächen, die als Kontaktaufnahmen zu Kindern (Grooming) identifiziert wurden.

Das EU-Zentrum prüft und bearbeitet die Meldungen der Anbieter. Alle Meldungen, die nicht offensichtlich unbegründet sind, leitet das Zentrum an Europol und die zuständigen Strafverfolgungsbehörden der Mitgliedstaaten weiter. Im Falle der Weiterleitung der Meldung teilt das Zentrum dem Anbieter mit, dass der betreffende Nutzer nicht informiert werden darf.

3. Kritik des EDSA und des EDSB

In ihrer gemeinsamen Stellungnahme vom 28. Juli 2022 äussern sich der EDSA und der EDSB kritisch zu Vorlage, ohne diese jedoch als Ganzes abzulehnen. Die beiden Datenschutzorgane bemängeln, dass:

- die Vorlage zu generell gehalten und teilweise unklar formuliert sei und den Behörden zu grosse Ermessensspielräume lasse, was Raum für Missbräuche schaffe;
- die Tauglichkeit und Effizienz der Überwachungsmassnahmen unzureichend belegt seien;
- damit gerechnet werden müsse, dass die zur Entdeckung von relevanten Informationen eingesetzten Technologien zu inakzeptabel hohen Fehlerraten führen würden;
- die Massnahmen zur Aufdeckung von Grooming und die Überwachung von Sprachkommunikation zu streichen seien;
- die im Entwurf vorhandenen Hinweise, wonach die unterstellten Provider die Verschlüsselung von Online-Kommunikation brechen oder verbieten müssten, unverhältnismässig seien;
- der vorgesehene Datenaustausch zwischen dem EU-Zentrum und Interpol im Rahmen einer Einzelfall-bezogenen Übermittlung von Informationen abzuwickeln sei.

4. Einschätzung des EDÖB

Der Beauftragte hat sich nicht zu Projekten der EU zu äussern. Er kann indessen die Aussagen des EDSA und des EDSB gut nachvollziehen, wonach sich der lange Rechtstext insbesondere mit Blick auf zentrale Fragen wie die Bearbeitung von Personendaten im Zusammenhang mit Grooming oder der Verschlüsselung von Daten als wenig bestimmt erweist.

Mit der gegen den Kindesmissbrauch im Internet gerichteten Vorlage soll in der EU ein komplexes und umfassendes institutionelles Netzwerk zur automatisierten Überwachung privater Kommunikation geschaffen werden, das nach Einschätzung des Beauftragten in seiner Funktionsweise jenem gegen die Geldwäscherei ähnlich ist. Wie die Finanzwirtschaft würde mit der geplanten Verordnung auch die Telekommunikationsbranche zu einer staatlichen Erfüllungsgehilfin, indem sie private Kommunikationsdaten ihrer Kundinnen und Kunden inkl. Chatnachrichten und Fotos aufgrund automatisierter Prozesse ohne deren Wissen an eine zentrale Meldestelle weitergeben müsste, die nach einer Triage Teile dieser Informationen an die Strafverfolgungsbehörden weiterreicht.

Der Beauftragte rechnet im Falle der Realisierung der Vorlage damit, dass es nur eine Frage der Zeit wäre, bis das kostspielige institutionelle Netzwerk der EU gegen den sexuellen Missbrauch von Kindern alsbald auch gegen andere Straftaten und Kriminalitätsphänomene zum Einsatz gelangen würde. Dies zum einen, weil eine solche Ausweitung schon bei der Geldwäschereibekämpfung zu beobachten ist, indem die Verwendungszwecke dieses System mit erweiterten Zielsetzungen wie etwa fiskalischen ergänzt und die Kataloge der strafbaren Vortaten entsprechend erweitert werden. Und zum andern, weil jede automatische Massendurchsuchung privater Kommunikation zwangsläufig zu Zufallsfunden führt, deren Verwertung das Strafprozessrecht ab einer gewissen Schwere zulässt.

B. Beantwortung der Fragen der Kommission

1. Umfasst der aktuelle Gesetzesentwurf der EU-Kommission eine mögliche Verpflichtung von Anbietern, ihre Nachrichtenkanäle dauernd und ohne Anfangsverdacht automatisiert zu überwachen?

Mittels Aufdeckungsanordnung verpflichten die Koordinationsbehörden 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.

II. Umfasst der aktuelle Gesetzesentwurf der EU-Kommission eine Verpflichtung, von dieser automatisierten Überwachung aufgegriffene Inhalte an ein EU-Zentrum weiterzuleiten? Ist dabei ein Rechtsweg vorgesehen? Was geschieht mit diesen Meldungen und den Inhalten?

Jeder der Verordnung unterstellte Dienstanbieter ist verpflichtet, die betroffenen Inhalte an das EU-Zentrum zu melden. Erachtet das EU-Zentrum eine Meldung als nicht offensichtlich unbegründet, leitet es diese an Europol und an die zuständige nationale Strafverfolgungsbehörde weiter.

Kommt es zu keiner Weiterleitung, werden die betroffenen Nutzer nachträglich über die Meldung informiert, was spätestens drei Monate nach deren Erstattung der Fall sein muss. Inwiefern die Meldung an das EU-Zentrum selbst Anfechtungsobjekt einer Beschwerde sein kann, ist für uns aus dem Verordnungsentwurf nicht ersichtlich geworden.

Kommt es zu einer Weiterleitung, werden Europol und die Strafverfolgungsbehörden in aller Regel eine Geheimhaltungsanordnung erlassen, sodass die betroffenen Nutzer erst im Rahmen des Strafverfahrens informiert werden, um ihre Rechte geltend machen zu können.

Zu den Rechtsbehelfen gegen die Aufdeckungsanordnungen s. vorne A.2.c.) *in fine*.

III. Inwiefern wäre die Schweiz, resp. Einwohnerinnen und Einwohner sowie Anbieterinnen von solchen Diensten vom Gesetz betroffen?

Es muss davon ausgegangen werden, dass die Verordnung extraterritoriale Auswirkungen entfalten soll.

Der Entwurf sieht vor, dass Anbieter einschlägiger Dienste, die ihre Hauptniederlassung nicht in der EU haben, eine Rechtsvertretung in der EU benennen müssen, die für die Entgegennahme, Einhaltung und Durchsetzung von Beschlüssen im Zusammenhang mit der Verordnung erforderlich sind. Dies gilt ausdrücklich auch für Aufdeckungsanordnungen.

Weiter ist davon auszugehen, dass Einwohnerinnen und Einwohner der Schweiz von Überwachungsmaßnahmen betroffen sein werden, wenn sie Dienste eines auch in der EU ansässigen Anbieters in Anspruch nehmen. Inwieweit dies auch für Individualkommunikation ohne Auslandsbezug der Fall sein wird, vermögen wir aus dem Verordnungstext nicht abzuleiten.

Sollten aufgrund der EU-Verordnung beschaffte Informationen seitens Interpol an das fedpol weitergeleitet werden, müssen Einwohnerinnen und Einwohner der Schweiz aufgrund der beidseitigen Strafbarkeit sexueller Missbräuche an Kindern nach Einschätzung des EDÖB indessen in der Schweiz mit einer strafrechtlichen Verfolgung und Verwertung der Informationen rechnen.

IV. Welche Auswirkungen hat eine Meldung von automatisch filtrierte Inhalte an ein EU-Zentrum auf die Beweislast?

Die nach dem Verordnungsentwurf im Rahmen von Aufdeckungsanordnungen automatisch ausgesonderten und an das EU-Zentrum weitergeleiteten Inhalte werden von Letzterem an die Strafverfolgungsbehörden weitergeleitet, wenn sie nicht offensichtlich unbegründet sind. Dies hat zur Folge, dass die von einer Meldung betroffenen Kundinnen und Kunden aufgrund wenig erhärteter Informationen zu Beschuldigten in einem Strafverfahren werden können.

Dieser Umstand ändert indessen nichts an der Unschuldsvermutung zugunsten der Beschuldigten im strafprozessualen Verfahren. Hingegen steht die automatisierte und verdachtslose Aussonderung belastender Informationen durch private Anbieter in einem Spannungsverhältnis zum Recht ihrer Kundinnen und Kunden, sich in einem allfälligen Strafverfahren nicht selbst belasten zu müssen. Allerdings wird dieses Spannungsverhältnis dadurch gemildert, dass die von einer Aufdeckungsanordnung betroffene Anbieter ihre Kundinnen und Kunden diese Massnahme vor Eintreten deren Rechtskraft ankündigen müssen.

V. Ist der aktuelle Gesetzesentwurf der EU-Kommission mit unserem Datenschutzverständnis, unseren Gesetzen und Grundrechten vereinbar?

Zunächst ist festzuhalten, dass der Gesetzesentwurf der Europäischen Kommission vom Europäischen Parlament und vom Rat nun auf seine Vereinbarkeit mit der Rechtsordnung der Europäischen Union

hin geprüft wird. Ob die geplante Verordnung nach Berücksichtigung der Kritik der Datenschutzorgane der EU in ihrer definitiven Ausgestaltung einer allfälligen Überprüfung durch den Europäischen Gerichtshof standhalten wird, muss sich zeigen.

Als Leiter der Bundesaufsichtsbehörde zum Schutz der Privatsphäre und informationellen Selbstbestimmung der Schweizer Bevölkerung wendet sich der Beauftragte grundsätzlich dagegen, dass private Unternehmen die private Kommunikation der Gesamtheit ihrer Kundinnen und Kunden systematisch und verdachtsunabhängig überwachen.

Der Beauftragte verkennt nicht, dass die Aufdeckung und Verfolgung schwerer Straftaten wie des Terrorismus oder des sexuellen Missbrauchs von Kindern gewichtige öffentliche Interessen darstellen, zu deren Durchsetzung sich die Überwachung privater Individualkommunikation sehr wohl als nötig, geeignet und datenschutzkonform erweisen kann. Angesichts des grundrechtlichen Gehalts des Rechts auf Privatsphäre und informationelle Selbstbestimmung setzt die Datenschutzkonformität entsprechender Massnahmen nach der Überzeugung des Beauftragten indessen voraus, dass diese auf einer formell-gesetzlichen Grundlage beruhen, welche ihre Durchführung von einer richterlichen Genehmigung im Einzelfall abhängig macht (wie dies auch das Nachrichtendienstgesetz des Bundes hinsichtlich der behördlichen Überwachung der Individualkommunikation von Personen zu Zwecken der Aufdeckung terroristischer Aktivitäten tut).

Gerne werde ich meine Antworten im Rahmen der geplanten Anhörung näher erläutern.

Mit freundlichen Grüssen


Adrian Lobsiger