Providers Are Watching Us

Paulina Jo Pesch 2020-09-27T13:52:21

Die Europäische Kommission hat am 10. September 2020 einen Verordnungsentwurf vorgelegt, der es ermöglichen soll, den sexuellen Missbrauch von Kindern im Netz effektiv zu bekämpfen. Zusammen mit der bereits angekündigten Folgeregelung zeichnet sich in den Plänen der Kommission jedoch ein fundamentaler Angriff auf den europäischen Datenschutz ab. Sie ermöglichen eine weitreichende Überwachung von Nutzer:innen durch die Provider und eine potenziell ausufernde Speicherung von Daten. Die geplanten Maßnahmen werden so die Vertraulichkeit digitaler Kommunikation aushöhlen, indem sie private Verschlüsselungsmaßnahmen beschränken.

Hintergrund und Pläne

Der Verordnungsentwurf vom 10. September sieht vorübergehende Abweichungen von der EU-Privacy-Richtlinie vor. Konkret sollen bestimmte Provider Technologien einsetzen können, die Material über Kindesmissbrauch sowie Kindesmissbrauch erkennen sollen. Erklärter Hintergrund des Entwurfs ist, dass diese Provider mit der ab dem 21. Dezember 2020 anwendbaren EU-Richtlinie über elektronische Kommunikation (EECC) dem Anwendungsbereich der ePrivacy-Richtlinie (die europäische Datenschutzrichtlinie für elektronische Kommunikation) unterfallen werden, die keine entsprechende Rechtsgrundlage enthält. Somit müssten der Kommission zufolge Provider die Nutzung von Erkennungstechnologien einstellen, soweit es an Regelungen im nationalen Recht fehlt. Lediglich temporär soll die Verordnung deshalb wirken, weil die Kommission sie zeitnah durch neue Rechtsvorschriften ersetzen will, die Provider sogar dazu verpflichten, Erkennungsmaßnahmen einzusetzen und erkannte Fälle an Strafverfolgungsbehörden zu melden. Die Kommission hat angekündigt, diese Rechtsvorschriften noch bis zum zweiten Quartal 2021 vorzuschlagen.

Maßnahmen hoher Eingriffsintensität

Der Entwurf enthält eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Provider nummernunabhängiger elektronischer Kommunikationsdienste. Hierunter fallen etwa Anbieter von E-Mail-, Messenger- und Videotelefonie-Diensten. Artikel 3 Absatz 1 des Entwurfs sieht vor, dass Art. 5 Abs. 1 und Art. 6 der ePrivacy-Richtlinie, die den Schutz der Kommunikations- und Verkehrsdaten der Nutzer:innen regeln, keine Anwendung auf bestimmte Verarbeitungen personenbezogener und anderer Daten durch solche Provider finden. Diese Ausnahmeregelung soll Verarbeitungsvorgänge betrefffen, die unbedingt notwendig für die Nutzung von Technologien sind, die nur den Zwecken dienen, Material über Kindesmissbrauch zu entfernen und Kindesmissbrauch zu erkennen sowie den Strafverfolgungsbehörden zu melden. Zusätzlich müssen die in den Buchstaben a–e der Vorschrift niedergelegten Voraussetzungen sämtlich erfüllt sein, damit die Ausnahmeregelung greift.

Die Maßnahmen, die der Vorschrift unterfallen, und ihre Eingriffsintensität klingen im Verordnungsentwurf nur vage an. In ihren Ausführungen zur Verhältnismäßigkeit verweist die Kommission – angesichts der geplanten, weitreichenderen Folgeregelung einigermaßen rabulistisch – auf den vorübergehenden Charakter der Ausnahmeregelung. Es gehe lediglich darum, dass die Provider die bereits üblichen „best practices“ fortführen können. Die Kommission impliziert ohne

jede Begründung durchgängig, dass der bisherige Einsatz automatisierter Erkennungsmaßnahmen – nach Maßgabe der noch allein anwendbaren DSGVO – als rechtskonform zu bewerten sei. Die Ausnahmeregelung sei außerdem auf das „unbedingt notwendige“ Maß begrenzt und der Entwurf sehe Maßnahmen vor, die den Datenschutz gewährleisten. Dies wird dem Regelungsgehalt des Verordnungsentwurfs nicht gerecht.

Der Verordnungsentwurf legalisiert eine weitreichende Überwachung durch Provider. Erfasst sind potenziell sämtliche Kommunikationsinhalte (Text, Bilder, Tonaufnahmen und Videos) und Verkehrsdaten aller Nutzer:innen der betreffenden Dienste, die auf Fälle begangenen und drohenden Kindesmissbrauch hin durchleuchtet werden können.

Zu den gezielteren Erkennungsmaßnahmen gehören solche zur Erkennung bereits bekannten Materials über Kindesmissbrauch, wie etwa Microsofts PhotoDNA, das etwa Twitter oder Facebook seit Jahren nutzen, oder entsprechende Technologien von Google. Solchen Maßnahmen ist zuzugestehen, dass die manuelle Prüfung aller Inhalte unmöglich und bloße „Notice und Takedown“-Verfahren bekanntermaßen gerade bei Material über Kindesmissbrauch ineffizient ist.

Einsatz Wahrscheinlichkeits-basierter Methoden

Der Verordnungsentwurf erfasst darüber hinaus problematischere probabilistische Maßnahmen. Mit solchen lassen sich automatisiert Fälle aufspüren, bei denen eine gewisse Wahrscheinlichkeit für Missbrauch besteht. Ein Beispiel ist Googles Bedspred Detector, der auf Grundlage bekannter Bildaufnahmen Opfer oder Täter:innen in neuen Bildaufnahmen erkennen soll. Da weder bekannt ist, wie die Wahrscheinlichkeit objektiv und verlässlich ermittelt werden kann noch konkrete Anforderungen an die Güte der Methoden gestellt werden, öffnet dies eine Tür für Eingriffe von praktisch unbegrenzter Streubreite.

Zu den probabilistischen Maßnahmen, die der Entwurf erfasst, zählen aber auch solche zur Erkennung nur anhand abstrakter Schlüsselindikatoren, etwa bestimmter Wörter. Dabei geht es insbesondere um Fälle, in denen Erwachsene Kinder online in Missbrauchsabsicht mit Geschenken oder Vorteilen ködern, Kinder bedrohen oder pornographisches Material an Kinder gelangen lassen (Artikel 2 Absatz 2 Buchstabe des Verordnungsentwurfs). Gemäß Artikel 3 Absatz 1 Buchstabe c des Verordnungsentwurfs sollen Provider die Daten anhand „relevanter Schlüsselindikatoren“ überprüfen, um solche Vorgänge zu erkennen. Erwägungsgrund 11 schließt das systematische Filtern und Durchsuchen von Kommunikation aus, die Text enthält. Es solle nur spezifische Kommunikation überprüft werden, für die es konkrete Verdachtselemente gibt. Es liegt nahe, dass konkrete Verdachtselemente sich niederschwellig aus den besagten relevanten Schlüsselindikatoren ergeben sollen.

Unzureichende Vorgaben insbesondere zu Transparenz und Speicherdauer

Die Anwendung probabilistischer Maßnahmen ist nicht zwingend mit dem Datenschutz unvereinbar. Dem wahrscheinlichkeitsbasierten Charakter solcher Maßnahmen ist aber besonders Rechnung zu tragen. Hier überzeugt der Verordnungsentwurf nicht, auch wenn er auf das Risiko falscher Positiver eingeht. Dass die automatisiert ermittelten Ergebnisse von Menschen überprüft werden (Artikel 3 Absatz 1 Buchstabe c und Erwägungsgrund 11 des Verordnungsentwurfs), ist hier das Mindeste. Klare Vorgaben zur Relevanz von Schlüsselindikatoren fehlen. Das in Artikel 3 Absatz 1

Buchstabe c genannte Beispiel des Altersunterschieds offenbart insoweit ein weites Verständnis der Kommission. Das gibt Eltern auch jenseits des Jugendschutzes Anlass, den elektronischen Versand von Bildaufnahmen der Familie sorgfältig zu überdenken.

Unzureichend sind auch die Transparenzvorgaben. Artikel 3 Absatz 1 Buchstabe e fordert einen jährlichen Bericht der Provider, der Art und Umfang der verarbeiteten Daten, Anzahl der identifizierten Fälle, Anzahl und Anteil falscher Positiver für die jeweiligen eingesetzten Technologien, Maßnahmen zur Verringerung der Fehlerquoten, Speicherdauer und angewandte Schutzmaßnahmen enthalten soll. Hier fehlt es einerseits an der Vorgabe, die eingesetzten Technologien, d.h. ihre Funktionsweise im Einzelnen transparent zu machen. Zwar könnte ihrer vollen Offenlegung entgegengehalten werden, dass diese die Umgehung erleichtern würde. Wünschenswert wäre aber eine unabhängige Überprüfung der eingesetzten Verfahren.

Höchst problematisch ist auch, dass der Verordnungsentwurf in lediglich vorgibt, die Anzahl falscher Positiver müsse soweit wie möglich begrenzt werden (Artikel 3 Absatz 1 Buchstabe b). Überspitzt formuliert bedeutet dies, dass eine Technologie, die 99 % falsche Positive auswirft, eingesetzt werden dürfte, solange eine bessere Technologie nicht verfügbar ist. Das ist wiederum im Zusammenhang zu sehen mit den höchstflexiblen Vorgaben des Verordnungsentwurfs zur Speicherdauer. Artikel 3 Absatz 1 Buchstabe d bestimmt, dass die Verarbeitung „unbedingt notwendig“ sein muss für die Zwecke der Verordnung. Absatz 2 konkretisiert, die Speicherung sei zulässig, soweit sie für Meldungen an die Strafverfolgungsbehörden nötig ist, und um verhältnismäßige Anfragen der Strafverfolgungsbehörden zu beantworten. Hier können sich uferlose Speicherfristen ergeben. Im Falle automatisiert erkannter Verdachtsfälle soll die Speicherdauer zunächst von der notwendigen Zeit für die Überprüfung durch einen Menschen bestimmt werden – und kann somit je nach Anteil falscher Positiver und Gesamtzahl der Treffer sowie von den Providern eingesetzter Ressourcen stark variieren. In den von den Providern verifizierten Fällen hängt die weitere Speicherdauer dann von der Reaktionszeit und Ermittlungsgeschwindigkeit der Strafverfolgungsbehörden ab. Auf dieser Grundlage können sich schnell Speicherfristen von über einem Jahr ergeben. Wer sich mit internationalen Cybercrime-Fällen befasst hat, weiß, dass diese Schätzung noch zurückhaltend ist.

Angesichts der besonderen Sensibilität der Daten – ein auch falscher Verdacht von Kindesmissbrauch ist geeignet, das öffentliche Ansehen einer Person zu zerstören und sie erheblich zu gefährden – hätte es enger Vorgaben zur Speicherdauer und darüber hinaus insbesondere klarerer Vorgaben zu technischen und organisatorischen Maßnahmen bedurft.

Im Zusammenhang mit Wahrscheinlichkeits-basierten Verfahren, etwa zur Risikobewertung, wird der Begriff der Notwendigkeit nahezu pervertiert. Dies gilt insbesondere, weil die Verlässlichkeit der Verfahren regelmäßig steigt, wenn besonder viele Daten – ggfs. auch solche aus dritten Quellen – genutzt werden. Zumindest lässt sich in diese Richtung leicht argumentieren, solange es an harten Vorgaben für die Verfahren fehlt. Dies gilt nicht nur im Bereich der Erkennung geschehenen und drohenden Kindesmissbrauchs, sondern etwa ebenso für die Bewertung von Betrugsrisiken durch Zahlungsdienstleister gemäß den technischen Regulierungsstandards der Delegiertenverordnung (EU) 2018/389 oder das Clustering vermutlich derselben Person gehörender Cryptocoin-Adressen zu Strafverfolgungszwecken. Solange es für Risikobewertungen an eng begrenzten Regeln fehlt, droht bei jeder gesetzlichen Erlaubnis oder sogar Verpflichtung, in dem Umfang Daten zu verarbeiten, der zur Risikobewertung notwendig ist, eine Aushöhlung der datenschutzrechtlichen Vorgaben. Bei deren Auslegung lässt sich aus der Gestattung oder Verpflichtung zur Risikobewertung eine Rechtmäßigkeit von umfangreichen Datenverarbeitungen ableiten. Statt einer leerformelartigen Begrenzung auf das Notwendige und Verhältnismäßige bedarf es einer klaren, verhältnismäßigen Regelung zur

Zuverlässigkeit sowie Relevanz und deren Nachweis, Transparenz und Umfang der Datenverarbeitung, an der es im Verordnungsentwurf fehlt. Das höhlt nicht nur den Datenschutz aus, sondern verfehlt auch das erklärte Ziel der Kommission, die Rechtssicherheit zugunsten von Strafverfolgern und Providern zu erhöhen.

Die nie endenden „Crypto Wars“

Äußerst kritisch ist schließlich zu sehen, dass sämtliche Erkennungsmaßnahmen nicht vereinbar sind mit einer wirksamen Ende-zu-Ende-Verschlüsselung, bei der die Provider keinen Zugriff die auf Endgeräte der Nutzer:innen haben. Die Kommission hat explizit ausgeführt, nötig seien Lösungsvorschläge, wie Provider Kindesmissbrauch in Ende-zu-Ende verschlüsselter Kommunikation aufdecken und melden könnten. Damit setzt sich die „unendliche Geschichte“ der sogenannten Crypto Wars fort, also der Debatte darum, ob der Staat private, starke Verschlüsselung unterbinden darf. Sollten die Provider Hintertüren in die Verschlüsselung einbauen, birgt dies erhebliche Sicherheitsrisiken. Wenn es Sicherheitslücken oder Hintertüren gibt, können auch dritte Angreifer diese ausnutzen. Wie gefährlich nicht geschlossene Sicherheitslücken sind, hat sich etwa im Falle der von der NSA entdeckten Lücke EternalBlue eindrucksvoll gezeigt.

Mit ihrem Angriff auf die private Verschlüsselung gibt die Kommission zugunsten von Maßnahmen zweifelhafter Effektivität Nutzer:innen und deren personenbezogene Daten dem Zugriff von Kriminellen und Geheimdiensten preis. Dabei können Kriminelle zumindest beim Austausch von Material über Kindesmissbrauch die regulierten Provider ohne Weiteres umgehen, indem sie zum Beispiel Darknet-Plattformen nutzen. Zudem steht zu befürchten, dass der Einsatz automatisierter Erkennungstechnologien mittel- bis langfristig nicht nur gesetzlich angeordnet werden soll, um Kindesmissbrauch zu bekämpfen, sondern auch, um andere Straftaten zu verhindern und zu verfolgen.

Danksagung der Autorin: Herzlicher Dank für wertvolle Anmerkungen gebührt Prof. Dr. Rainer Böhme.
