Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte

VB verfassungsblog.de/vielen-dank-ihre-post-ist-unbedenklich/

Erik Tuchtfeld
25 May 2022

„Vielen Dank, Ihre Post ist unbedenklich“

Vor zwei Wochen hat die Kommission ihren Entwurf für eine „Verordnung zur Festlegung von Vorschriften (sic!) für die Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern“ vorgestellt. Die damit verbundene Einführung der Überprüfung sämtlicher digital verschickter Nachrichten (diskutiert unter dem Schlagwort „Chatkontrolle“) brachte unter anderen den Kryptographie-Professor Matthew Green zur Bewertung des Vorhabens als „the most sophisticated mass surveillance machinery ever deployed outside of China and the USSR“. Das evident grundrechtswidrige Vorhaben dürfte das größte staatliche Überwachungsvorhaben in Europa seit dem Ende des Kalten Krieges sein.

Der Entwurf der Kommission

Der aktuelle Vorschlag tritt die Nachfolge des im Sommer vergangenen Jahres in Rekordzeit verabschiedeten Verordnung 2021/1232 an. Nachdem der Europäische Kodex für die elektronische Kommunikation (EKEK) – wohl aus Versehen – auch die digitale Kommunikation über Messenger und E-Mail unter den umfassenden Schutz der Vertraulichkeit der Kommunikation stellte (vgl. Erwägungsgründe 2, 9, 23 VO 2021/1232), fiel den Betreibern großer unverschlüsselter Kommunikationsdienste wie Facebook Messenger auf, dass dies auch das bisher übliche (serverseitige) Scannen der Kommunikation auf Abbildungen von Kindesmissbrauch verbieten würde. Daraufhin wurde durch Verordnung 2021/1232 der Vertraulichkeitsschutz erneut gelockert und diese Maßnahmen kurzfristig wieder zugelassen. Der politisch großen Einigkeit standen schon damals erhebliche rechtliche Zweifel gegenüber. Auch wenn es hierbei nicht um eine *Anordnung* von Überprüfungsmechanismen, sondern nur um die *Erlaubnis* solcher Maßnahmen ging, hielt beispielsweise die ehemalige deutsche EuGH-Richterin Colneric das Vorhaben für grundrechtswidrig.

Was gestern ein Dürfen war, soll nun zum Müssen werden: Art. 10 Abs. 1 des aktuellen Entwurfs der Kommission sieht vor, dass sowohl Hosting-Anbieter (also bspw. Webseitenhoster, soziale Plattformen und ähnliches) wie auch interpersonelle

Kommunikationsdienste (also Messenger und E-Mail-Anbieter) zukünftig „detection orders“ erfüllen müssen. Kommt es zu einer solchen Anweisung, müssen sie Software installieren und einsetzen, die bekannte und bisher unbekannte Abbildungen von Kindesmissbrauch sowie sogenanntes „Grooming“ erkennen soll. „Grooming“ beschreibt dabei die Kontaktaufnahme von Erwachsenen gegenüber Kindern für sexuelle Zwecke (Art. 2 lit. o des Entwurfs i.V.m. Art. 6 der Richtlinie zur Bekämpfung des sexuellen Missbrauchs). Hierfür darf der Anbieter entweder eigene Software oder Softwareentwicklungen eines neu zu schaffenden, in Den Haag angesiedelten, EU-Zentrums gegen Kindesmissbrauch einsetzen (Art. 10 Abs. 2; 40 bis 42). Diese „detection orders“ werden auf Antrag einer (zu schaffenden) Koordinierungsstelle (Art. 25 bis 32) von einem Gericht oder einer unabhängigen Verwaltungsbehörde erlassen, sofern ein erhebliches Risiko besteht, dass ein Dienst für Online-Kindesmissbrauch genutzt wird (Art. 7).

Da es nicht darum geht, ob ein Dienst zu einem erheblichen Maße für Kindesmissbrauch verwendet wird, sondern ob ein erhebliches Risiko (unabhängig vom Umfang) einer solchen Nutzung besteht, dürfte nahezu jedes gängige, allgemein verfügbare digitale Kommunikationsmittel hiervon erfasst werden. Bei Anbietern unverschlüsselter (bzw. nur transport-verschlüsselter) Kommunikationsdienste – wie es beispielsweise regelmäßig bei E-Mails der Fall ist, aber auch beim Facebook-Messenger, Twitter-Direktnachrichten, Instagram-Nachrichten, etc. – dürfte dies dazu führen, dass serverseitig Algorithmen eingesetzt werden, um Abbildungen von Kindesmissbrauch und Grooming-Nachrichten zu erkennen. Sobald verdächtige Nachrichten (automatisiert) erkannt werden, werden sie zunächst an das bereits genannte EU-Zentrum ausgeleitet (Art. 12) und dann von diesem, sofern sich der Verdacht (ob durch automatisierte oder manuelle Verfahren bleibt offen) bestätigt, an Europol oder nationale Sicherheitsbehörden weitergeleitet (Art. 48).

Spannend wird es bei Anbietern Ende-zu-Ende-verschlüsselter Kommunikation (wie Signal, Threema oder WhatsApp). Diese trifft die gleiche Verpflichtung, sie haben aber schon technisch (eigentlich) keine Möglichkeit, die Inhalte der Kommunikation zu durchsuchen. Die einzige Möglichkeit hierfür wird sein, Inhalte bereits vor der Verschlüsselung zu prüfen, also in der jeweiligen App selbst einen Mechanismus einzubauen, der die Nachricht überprüft, bevor sie versendet (und damit verschlüsselt) wird. So kann die Kommission in Ihrem Entwurf auch ohne Weiteres Ende-zu-Ende-Verschlüsselung als „wichtiges Werkzeug zur Sicherstellung der Sicherheit und Vertraulichkeit der Kommunikation der Nutzer, inklusive der von Kindern“ bezeichnen (Erwägungsgrund 26). Denn diese Verschlüsselung wird nicht verboten, sie wird schlicht obsolet, in dem jede Messaging-App zur Wanze wird, die schon vor der Verschlüsselung aktiv ist.

Im Vergleich zur analogen Kommunikation entspricht die serverseitige Überprüfung dem Postboten, der jeden Brief und jedes Paket öffnet und einen Blick auf seinen Inhalt wirft, die Überprüfung auf Geräteseite dagegen dem Polizeibeamten, der so lange nicht warten möchte und schon beim Schreiben einen Blick über die Schulter des Absenders wirft.

Auf andere kritische Aspekte des Kommissionsentwurfs, wie Netzsperren (Art. 16 bis 18) oder Verifizierungspflichten (Art. 4 Abs. 3, Art. 6 Abs. 1 lit. c) sei an dieser Stelle aus Platzgründen nur kurz hingewiesen, ohne sie ausführlich zu thematisieren. Sie bieten jeweils mehr als genug Anlass für eigenständige Beiträge.

Das Wesen des Kommunikationsgeheimnisses

Das Recht auf vertrauliche Kommunikation wird in der Europäischen Union insbesondere durch Art. 7 (Recht auf Privatsphäre) und Art. 8 (Recht auf Datenschutz) der Grundrechte-Charta gewährleistet. Vor dem Hintergrund des umfassenden Screenings jeglicher digitaler Kommunikation dürften darüber hinaus aber auch in erheblichem Maße *chilling effects* für die Informations- und Meinungsfreiheit (Art. 11) zu befürchten sein. Über den privaten Bereich hinaus sind dabei insbesondere auch die Auswirkungen auf Berufsgeheimnisträger:innen wie Journalist:innen, Rechtsanwält:innen und Ärzt:innen, deren besonders geschützte Kommunikation mit ihren Informant:innen/Mandant:innen/Patient:innen durchleuchtet wird, zu beachten (*La Quadrature du Net*, Rn. 118).

Die Rechtsprechung des EuGH zur Vorratsdatenspeicherung, in der es also nur um die Verarbeitung von Metadaten (bspw. Angaben zum Zeitpunkt der Kommunikation und den Beteiligten) ging, macht die offenkundige Unvereinbarkeit des aktuellen Vorhabens mit den genannten Grundrechten deutlich. So müssen sich Eingriffe in die Privatsphäre „auf das absolut Notwendige beschränken“ (st. Rechtsprechung, vgl. *La Quadrature du Net*, Rn. 130). Darüber hinaus muss jeder Eingriff den nach Art. 52 Abs. 1 S. 1 GrCh absolut geschützten Wesensgehalt des in Art. 7 GrCh verankerten Rechts auf Privatsphäre achten.

Was ist der Wesensgehalt, der Kern dieses Rechts auf „Achtung der Kommunikation“? Jedenfalls doch, dass nicht jede Kommunikation – sei es automatisiert, sei es manuell – auf bestimmte Faktoren hin überprüft wird, sondern dass im Grundsatz privat bleibt, was privat gedacht ist (zur Unterscheidung zwischen privater und öffentlicher Kommunikation siehe auch hier). Zwar gibt es keinen Grundsatz ohne Ausnahmen: So berührt *anlassbezogene* Telekommunikationsüberwachung, die *im Einzelfall* sämtliche Kommunikation erfasst, nicht den Wesensgehalt des Rechts auf Vertraulichkeit der Kommunikation (beachte aber auch hier die in Deutschland verfassungsrechtlich erforderliche Ausnahme für Kommunikation, die dem Kernbereich privater Lebensgestaltung zuzuordnen ist, § 100d StPO).

Eine allgemeine Überwachung sämtlicher Kommunikation kann von der Intensität auf der Seite der Erhebung jedoch kaum mehr übertroffen werden (die einzige Einschränkung ist der digitale Transportweg, analoge Post soll bisher nicht überprüft werden), sondern nur noch in Bezug auf die Charakteristika, nach denen gesucht wird (man denke an die Möglichkeit der Suche nach terroristischen Inhalten o.ä.). Dementsprechend hat auch der EuGH eine Verletzung des Wesensgehalts von Art. 7 GrCh bei der auf Metadaten gerichteten Vorratsdatenspeicherung nur deshalb abgelehnt, weil „die Richtlinie […] die Kenntnisnahme

des Inhalts elektronischer Kommunikation als solchen nicht gestattet“ (*Digital Rights*, Rn. 39). Im Umkehrschluss dürfte das Vorhaben der Kommission, das sich gerade auf die Inhalte elektronischer Kommunikation bezieht, den Wesensgehalt von Art. 7 GrCh berühren und damit von vornherein rechtswidrig sein.

Keine Maschine ist fehlerfrei

Die Rechtswidrigkeit des Entwurfs wäre also auch schon dann zu bejahen, wenn man von einer perfekten Technologie ausginge, die tatsächlich und ausschließlich nur strafbare Inhalte identifizieren würde. Die Kommission selbst geht aber davon aus, dass rund 12% der zukünftigen Meldungen *false positives* sind, also keine strafbaren Inhalte betreffen würden (Fn. 32 des Entwurfs). Da jeden Tag in der EU Milliarden von Nachrichten versendet werden, dürfte eine 12%ige Fehlerrate dazu führen, dass täglich Tausende von Nachrichten ohne jeden sachlichen Grund an öffentliche Stellen ausgeleitet werden. Unter Berücksichtigung der Art von Inhalten, nach denen die Technologie sucht, dürfte dies primär intime Chat-Nachrichten betreffen, die einvernehmlich ausgetauscht werden. Es besteht also zukünftig die reale Gefahr, dass private Fotos, Videos und Textnachrichten auf den Schreibtischen von Behördenmitarbeiter:innen landen.

Die Pflicht zum Schutz der Kinder

Selbstverständlich sind der Kommission sowohl die einschlägige Rechtsprechung wie auch die tatsächlichen Probleme bekannt. Sie beruft sich überraschenderweise sogar selbst – wenn auch höchst selektiv – auf die Rechtsprechung zur Vorratsdatenspeicherung, wenn sie unterstreicht, dass aus Art. 7 und 8 der Grundrechte-Charta auch Schutzpflichten für die Europäische Union gegenüber den von Missbrauch betroffenen Kindern erwachsen (Fn. 27 des Entwurfs mit Verweis auf Rn. 126 von *La Quadrature du Net*). Gerade die Existenz dieser Schutzpflichten macht den Entwurf aber zum Skandal: Kinder haben einen Anspruch auf staatlichen Schutz. Gerade das hat der EuGH auch in *La Quadrature du Net* anerkannt und *trotzdem* die Regelungen zur anlasslosen Vorratsdatenspeicherung als unverhältnismäßig eingestuft. Es gibt keinen Anhaltspunkt dafür, dass er nun zu einem anderen Ergebnis käme. Damit hat die Kommission einen Vorschlag erstellt, der viel Zeit, Geld und Aufmerksamkeit auf sich ziehen wird, nur damit er – falls er sich politisch durchsetzt – am Ende vor Gericht für nichtig erklärt wird.

Für den dringend notwendigen verbesserten Schutz von Kindern ist damit nichts gewonnen. Dabei wäre viel zu tun: Aktuell wirken Sicherheitsbehörden beispielsweise in Teilen nicht auf die Löschung bekannter Abbildungen von Kindesmissbrauch hin, weil ihnen hierfür die Ressourcen fehlen – eine flagrante Verletzung der grundrechtlichen Schutzpflicht gegenüber den Betroffenen. Schon allein die Sichtung des vorhandenen Materials stellt die Polizei vor

erhebliche Kapazitätsprobleme. Wenn bereits hierfür die Mittel fehlen, so lässt dies für die noch deutlich aufwändigere Ermittlung der Täter:innen, die den betroffenen Kindern unmittelbare Gewalt antun, nur Düsteres vermuten.

Die Kommission sollte gemeinsam mit den Mitgliedsstaaten einen effektiven, rechtskonformen Maßnahmenplan zur Bekämpfung des Kindesmissbrauchs erarbeiten. Mehr personelle Ressourcen für die Sicherheitsbehörden, verbesserte Anzeigemöglichkeiten innerhalb der Dienste, bessere Medien- und Sexualaufklärung für Kinder und ein Ausbau von Beratungs- und Anlaufstellen für Betroffene sollten dazugehören. Dystopische Totalüberwachung dagegen nicht.

MAX PLANCK LAW

SUGGESTED CITATION Tuchtfeld, Erik: *„Vielen Dank, Ihre Post ist unbedenklich“: Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte, VerfBlog,* 2022/5/25, https://verfassungsblog.de/vielen-dank-ihre-post-ist-unbedenklich/, DOI: 10.17176/20220525-182426-0.