Scannen privater Kommunikation in der EU

Prinzipien von EDRi für Ausnahmen von der Datenschutzrichtlinie für elektronische Kommunikation zum Zweck der Entdeckung von online verbreiteten Darstellungen des sexuellen Missbrauchs von Kindern (CSAM)

Übersetzung: Digitale Gesellschaft und Digitalcourage 09.02.2022

Zusammenfassung:

Die automatische Durchsuchung der privaten Kommunikation eines jeden Menschen zu jeder Zeit stellt einen unverhältnismäßigen Eingriff in den Kern des Grundrechts auf Privatsphäre dar. Sie kann eine Form der undemokratischen Massenüberwachung darstellen und schwerwiegende und ungerechtfertigte Auswirkungen auch auf viele andere Grundrechte und Freiheiten haben.

EDRi will sicherstellen, dass jeder EU-Vorschlag zur Aufdeckung von Online-Material über sexuellen Kindesmissbrauch (CSAM – vom englischen „child sexual abuse material“) mit den Grundrechtsverpflichtungen der EU in Einklang steht, insbesondere dass die Maßnahmen rechtmäßig und objektiv notwendig und verhältnismäßig zu ihrem erklärten Ziel sind. Die Überwachung oder das Abfangen privater Kommunikation oder ihrer Metadaten zur Aufdeckung, Untersuchung oder Verfolgung von CSAM darf daher nur auf tatsächlich Verdächtige beschränkt werden, gegen die ein begründeter Verdacht besteht. Sie muss ordnungsgemäß gerechtfertigt und speziell angeordnet sein und den nationalen und den EU-Vorschriften für polizeiliche Maßnahmen, ordnungsgemäße Verfahren, den Grundsätzen guter Verwaltung und den Grundrechtsgarantien entsprechen. Wir schlagen zehn voneinander untrennbare Prinzipien vor, die sicherstellen sollen, dass die wichtigen Bemühungen zur Ermittlung und Verfolgung derjenigen, die CSAM verbreiten, in einer Weise erfolgen können, die demokratisch und mit den europäischen Werten vereinbar ist. Nur so können die Opfer am ehesten Gerechtigkeit erfahren. Dazu gehört, dass die Mitgliedstaaten den zahlreichen bestehenden Empfehlungen zur Bekämpfung von CSAM nachkommen.

Inhalt

Politischer Hintergrund

Im Juli 2021 einigte sich der Rat der Europäischen Union mit dem Europäischen Parlament auf die Verabschiedung eines neuen Gesetzes, das eine vorübergehende Ausnahme von bestimmten Teilen der ePrivacy-Richtlinie von 2002 vorsieht.

Die Datenschutzrichtlinie für elektronische Kommunikation (2002) ist das einzige Instrument der EU, das ausdrücklich das Recht eines jeden auf Privatspäre und die Vertraulichkeit der Kommunikation schützt, wie es in Artikel 7 der Charta der Grundrechte der EU verankert ist. Im Jahr 2018 wurde mit der Neufassung des Europäischen Kodex für die elektronische Kommunikation (EECC) die Definition eines „elektronischen Kommunikationsdienstes“ erweitert. Diese Ausweitung bedeutet, dass ab Dezember 2020 verschiedene Vorschriften der Datenschutzrichtlinie für elektronische Kommunikation nun für eine breitere Palette von Online-Diensten gelten.

Dies war Anlass für die Europäische Kommission, eine befristete Ausnahmeregelung von der Datenschutzrichtlinie für elektronische Kommunikation vorzuschlagen, um das laufende freiwillige Scannen privater Kommunikation durch Diensteanbieter.innen zu legalisieren. Die Ausnahmeregelung wird im August 2024 auslaufen und die Europäische Kommission beabsichtigt, sie durch ein langfristiges Gesetz zu ersetzen. Ein Vorschlag der Kommission wird voraussichtlich im März 2022 vorgelegt.

Erörterung des einschlägigen EU- und internationalen Rechts

Das Recht auf den Schutz der Privatsphäre in der Kommunikation (Artikel 7 EU-Grundrechtecharta) stellt sicher, dass jede.r ohne unangemessene Eingriffe Gesundheits- und Rechtsberatung in Anspruch nehmen, sich Freund.innen und Familienangehörigen anvertrauen und online Unterstützungsnetzwerke aufbauen kann. Es schützt den Nachrichtenverkehr von Journalist.innen und Menschenrechtler.innen und sichert deren vertrauliche Quellen, um Korruption aufzudecken und sich für einen sozialen Wandel einzusetzen. Auch darüber hinaus ist die Privatsphäre eine zentrale Grundlage für die Wahrnehmung fast aller anderen Grundrechte. So hat etwa die Hohe Kommissarin der Vereinten Nationen (UN) für Menschenrechte, Michelle Bachelet, erklärt:[1]

> „Das Recht auf Privatsphäre spielt eine zentrale Rolle für das Machtgleichgewicht zwischen Staat und Individuum und ist ein Grundrecht für eine demokratische Gesellschaft.“

Deshalb muss jede Einschränkung des Rechts auf Privatsphäre auf einem Gesetz beruhen, einem legitimen Ziel in einer demokratischen Gesellschaft dienen und für dieses Ziel notwendig und verhältnismäßig sein.

Die Privatsphäre von Kindern:

Das Recht auf Privatsphäre ist für junge Menschen vielleicht sogar noch wichtiger, da dessen Verletzung tiefgreifende Auswirkungen auf ihre Persönlichkeitsentwicklung haben kann. Wie

1 https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E

die Vereinten Nationen in ihrer „Allgemeinen Bemerkung Nr. 25 zu den Rechten von Kindern in Bezug auf das digitale Umfeld“ aus dem Jahr 2021 anerkennen, die in Absprache mit 709 jungen Menschen entwickelt wurde: „Privatsphäre ist für die Handlungsfähigkeit, Würde und Sicherheit von Kindern und für die Ausübung ihrer Rechte von entscheidender Bedeutung“ (¶ 67).[2] Das UNICEF-Toolkit 2018 zur Online-Privatsphäre von Kindern ergänzt:[3]

„Die Kommunikationsprivatsphäre von Kindern ist bedroht, wenn ihre Posts, Chats, Nachrichten oder Anrufe von Regierungen oder anderen Akteuren abgefangen werden.“

Die Allgemeine Bemerkung Nr. 25 der Vereinten Nationen enthält ebenfalls mehrere Empfehlungen zur Privatsphäre von Kindern, die für das Scannen privater Online-Kommunikation von großer Bedeutung sind:

> „Jegliche digitale Überwachung von Kindern sowie die damit verbundene automatisierte Verarbeitung personenbezogener Daten sollte das Recht des Kindes auf Privatsphäre achten und nicht routinemäßig, wahllos oder ohne das Wissen des Kindes bzw. im Fall sehr kleiner Kinder, ohne das Wissen der Eltern oder Betreuenden erfolgen. In kommerziellen Umgebungen oder Bildungs- und Betreuungseinrichtungen sollte eine solche Überwachung nur stattfinden dürfen, wenn das betroffene Kind berechtigt ist, dieser zu widersprechen. Dabei sollte stets das am wenigsten in die Privatsphäre eingreifende zweckdienliche Mittel gewählt werden.“ (¶ 75)
>
> „Technologien, die Online-Aktivitäten zu Sicherheitszwecken überwachen, wie etwa Nachverfolgungsgeräte und -dienste, können, wenn sie nicht sorgfältig eingesetzt werden, ein Kind daran hindern, eine Beratungsstelle anzusprechen oder nach sensiblen Informationen zu suchen.“ (¶ 76);
>
> „Von entscheidender Bedeutung kann der Schutz der Privatsphäre eines Kindes im digitalen Umfeld sein, wenn Eltern oder Betreuende selbst eine Bedrohung für die Sicherheit des Kindes darstellen oder um dessen Betreuung streiten.“ (¶ 77)

Gerichtshof der Europäischen Union (EuGH):

In mehreren Fällen hat der EuGH bestätigt, dass der allgemeine Zugriff auf den Inhalt der elektronischen Kommunikation durch Behörden den Kern des Rechts auf Privatsphäre verletzt. Etwa in den Urteilen zu Digital Rights Ireland Ltd (C-293/12) (2014) und Maximilian Schrems (C-362/1) (2015). Dies wird in unserem kommenden Papier über die vorgeschlagene langfristige Ausnahmeregelung ausführlicher untersucht werden.

Die Datenschutzgrundverordnung (DSGVO):

Datenschutz durch Technik und „Privacy by design“ bedeutet, dass wir alle in der Lage sein sollten, unser Recht auf Privatsphäre in vollem Umfang zu genießen, solange es keinen legitimen Grund für eine Einschränkung dieses Rechts gibt. Das automatische Scannen der privaten Kommunikation eines jeden Menschen stellt diesen Grundsatz jedoch auf den Kopf. Jeder Einzelne von uns wird so behandelt, als stünde er im Verdacht, CSAM online anzusehen oder zu verbreiten, und wird auf dieser Grundlage ausspioniert. Es ist zu betonen, dass die

2 https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

3 https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

befristete ePrivacy-Ausnahmeregelung (2021) keine eigenständige rechtliche Grundlage bietet, auch nicht für das freiwillige Scannen privater Kommunikation. Die Ausnahmeregelung nimmt diese Scanning-Praktiken zwar von den Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation aus, die DSGVO gilt jedoch weiterhin. Das Europäische Parlament aber hat bereits festgestellt, dass solche Scanning-Praktiken nach der DSGVO rechtswidrig sein können.[4]

Die zehn Prinzipien

Maßnahmen zur Aufdeckung, Untersuchung oder Verfolgung von Online-CSAM müssen immer mit den nationalen und EU-weiten Verpflichtungen in Bezug auf die Grundrechte vereinbar sein. Wir sind der Meinung, dass zumindest die zehn folgenden Prinzipien kumulativ erfüllt werden müssen, um sicherzustellen, dass die Grundsätze der Notwendigkeit und Verhältnismäßigkeit in der kommenden CSAM-Gesetzgebung objektiv erfüllt werden:

1. **Keine Massenüberwachung:** Das allgemeine, automatische Scannen der privaten Kommunikation aller Menschen zu jeder Zeit ist ein grundlegend unverhältnismäßiger Eingriff in das Recht auf Privatsphäre. Ob zur Entdeckung von CSAM oder zu anderen Zwecken, solche Praktiken sind in einer demokratischen Gesellschaft niemals zu rechtfertigen. Dementsprechend dürfen Diensteanbieter.innen nicht dazu verpflichtet werden, die private Kommunikation generell und automatisch zu scannen;
2. **Eingriffe müssen gezielt und auf Grundlage eines individuellen Verdachts stattfinden:** Jede Überwachung privater Kommunikation darf nur auf die Person oder Personen abzielen, gegen die ermittelt wird (nicht auf andere Nutzer.innen des Dienstes), und zwar auf der Grundlage eines spezifischen, begründeten und individuellen Verdachts (z. B. kann die Überwachung aller Nutzer.innen eines bestimmten Dienstes nicht als gezielt angesehen werden). Nur der individuelle Verdacht gegen eine Person kann Grundlage für eine Überwachung sein. Der Verdacht darf nicht das Ergebnis einer allgemeinen Überwachung sein;
3. **Eingriffe müssen rechtmäßig und auf gesetzlicher Grundlage erfolgen:** Jede Untersuchung privater Kommunikation muss eine spezifische Rechtsgrundlage haben, die öffentlich zugänglich, klar, bestimmt, abschließend und allgemein sein muss. Außerdem muss sie den nationalen und den EU-Vorschriften über rechtsstaatliche Verfahren, ordentliche Verwaltungspraxis, Strafverfolgung, Rechenschaftspflicht, Transparenz, Nichtdiskriminierung usw. entsprechen;
4. **Eingriffe müssen individuell angeordnet sein:** Jede Untersuchung privater Kommunikation muss spezifisch und individuell von einem Richter angeordnet werden. Die Polizei darf nicht ohne richterliche Anordnung die Wohnung einer Verdachtsperson betreten oder Telefongespräche abhören. Dieselben Grundsätze gelten für den privaten

4 https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-temporary-derogation-from-the-e-privacy-directive-for-ott-services

Online-Bereich. Eine richterliche Anordnung muss eingeholt werden, bevor die Kommunikation einer Person abgehört wird, und nicht rückwirkend;

5. **Maßnahmen dürfen nur so wenig wie nötig in die Privatsphäre eingreifen und müssen sich auf die Erkennung von CSAM beschränken:** Jede Untersuchung privater Kommunikation muss gewährleisten, dass der Eingriff in das Recht auf Privatsphäre so gering wie möglich ist. Sie muss sich auf die Aufdeckung von CSAM beschränken und sicherstellen, dass Diskriminierung verhindert und das Risiko falsch positiver Ergebnisse minimiert wird. Um dies zu gewährleisten, sollten die nationalen Datenschutzbehörden und der Europäische Datenschutzausschuss (EDPB) verbindliche Leitlinien für die Zulässigkeit bestimmter Technologien bereitstellen, die zur Aufdeckung von CSAM bereits eingesetzt werden und die künftig eingesetzt werden sollen;
6. **Unabhängige Aufsicht und Überprüfung der Technologie und ihres Einsatzes:** Es muss eine strenge Aufsicht über bestehende und künftige Technologien zur Aufdeckung von Online-CSAM durch nationale Datenschutzbehörden geben, einschließlich unabhängiger Audits und der Durchsetzung von Melde- und Dokumentationspflichten für Strafverfolgungsbehörden, um die Wirksamkeit der Maßnahmen nachzuweisen und eine Kontrolle zu ermöglichen (z. B. in Bezug auf Verurteilungen, falsch-positive Meldungen, absolute vs. wiederholte Meldungen und die Dienste, bei denen CSAM aufgedeckt werden); die ordnungsgemäße Durchführung von Datenschutz-Folgenabschätzungen für alle verwendeten Technologien/Methoden und Transparenz;
7. **Kontrolle durch unabhängige Sicherheitsforschung und Zivilgesellschaft muss gewährleistet sein:** Unabhängige Sicherheitsforscher.innen und die Zivilgesellschaft müssen Zugang zu den technischen Details aller vorgeschlagenen Werkzeuge oder Technologien haben, um beabsichtigte oder unbeabsichtigte Risiken zu bewerten. Maßnahmen, die Geräte unsicher und anfällig für böswillige Akteur.innen machen, wie die automatisierte Analyse von Kommunikationsinhalten auf dem Gerät selbst (CSS – vom englischen Client Side Scanning), sollten nicht zugelassen werden;
8. **Maßnahmen müssen Verschlüsselung wahren:** Die Verfügbarkeit und Verwendung von Verschlüsselung ist für den Schutz unserer digitalen Infrastruktur und Kommunikation unerlässlich. Alle Maßnahmen zur Bekämpfung von CSAM müssen daher Verschlüsselung als wichtige Sicherheitsmaßnahme respektieren und dürfen ihre Entwicklung, Verfügbarkeit oder Verwendung nicht in einer Weise untergraben, die sich auf alle Nutzer.innen des Kommunikationsdienstes auswirkt. Methoden wie Client Side Scanning (CSS) untergraben das Prinzip der Ende-zu-Ende-Verschlüsselung (E2E), indem sie Mittel zur Umgehung kryptographischer Systeme einführen, die irgendwann unweigerlich von böswilligen Akteur.innen ausgenutzt werden;
9. **In die Bewältigung komplexer sozialer Probleme investieren:** Das gravierende Problem des sexuellen Missbrauchs von Kindern ist nicht nur eine Frage der Online-Verbreitung. Vor allem sollten die Antworten der EU und der Mitgliedstaaten auf dieses schwerwiegende Problem in Prävention, Bildung, Unterstützung der Opfer, sozialen Diensten, sozialstaatlichen Maßnahmen und anderen Methoden zur Bekämpfung der Grundursache dieser Probleme bestehen und in diese investieren. Technologische Lösungen sind kein Allheilmittel für komplexe gesellschaftliche Probleme. Darüber hinaus

werden in dem Bericht des Europäischen Parlaments von 2017 über die Umsetzung der „Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern“ durch die Mitgliedstaaten und in der Mitteilung der Europäischen Kommission von 2020 für eine wirksamere Bekämpfung des Kindesmissbrauchs eine Reihe wichtiger Initiativen genannt, die von den Mitgliedstaaten noch umgesetzt werden müssen und für die Abhilfe geschaffen werden sollte, bevor neue technische Lösungen oder Rechtsvorschriften vorgeschlagen werden;

10. **Alle Interessengruppen einbeziehen:** Es ist unerlässlich, alle relevanten Interessengruppen zusammenzubringen, damit produktive Diskussionen über die Bekämpfung von CSAM im Internet geführt werden. Wenn es um Risiken für die Privatsphäre und den Datenschutz geht, müssen Gruppen, die sich für Grundrechte im Digitalen einsetzen – einschließlich derjenigen, die speziell die Rechte junger Menschen vertreten –, gebührendes Gewicht erhalten.

Entscheidend ist, dass der Prozess, durch den diese Prinzipien in Gesetze umgesetzt werden, den Anforderungen an ein demokratisches Gesetzgebungsverfahren entsprechen und die Mitsprache des Parlaments gewährleistet wird. Anders als bei den Verhandlungen über die befristete Ausnahmeregelung müssen die Mitglieder des Europäischen Parlaments (MdEP) ausreichend Zeit und Unterstützung erhalten, um ihre zentrale Rolle bei der Prüfung von Gesetzesentwürfen wahrnehmen und die Vorschläge der Exekutive der EU tatsächlich kontrollieren zu können.

Die oben genannten Prinzipien werden eine Bewertung der Notwendigkeit und Verhältnismäßigkeit jeder vorgeschlagenen Maßnahme zur Bekämpfung von Online-CSAM unterstützen, die angesichts der weitreichenden Auswirkungen auf das Recht auf Privatsphäre und Vertraulichkeit der Kommunikation von der Kommission nachgewiesen werden muss, um die Rechtmäßigkeit und Zulässigkeit jeder Abweichung von der Datenschutzrichtlinie für elektronische Kommunikation sicherzustellen.

Weitere Informationen

Für weitere Informationen wenden Sie sich an:

Digitale Gesellschaft e.V.	tom.jennissen@digitalegesellschaft.de
Digitalcourage e.V.	presse@digitalcourage.de

über EDRi:	https://edri.org/about-us/who-we-are/
über die Digitale Gesellschaft:	https://digitalegesellschaft.de/uber-uns/
über Digitalcourage:	https://digitalcourage.de/ueber-uns