Europäische Kommission: Wahren Sie Privatsphäre, Sicherheit und Meinungsfreiheit indem Sie den neuen Gesetzentwurf zurückziehen

Mittwoch, 8. Juni 2022

Sehr geehrte EU-Kommissar.innen,

wenn Sie die Funktionsweise des Internets grundlegend untergraben, machen Sie es für alle weniger sicher.

Wir schreiben Ihnen als 73 zivilgesellschaftliche Organisationen und Gewerkschaften, die in den Bereichen Menschenrechte, Medienfreiheit, Technologie und Demokratie im digitalen Zeitalter tätig sind. Gemeinsam fordern wir Sie auf, die „Verordnung zur Festlegung von Vorschriften zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern" (CSA-Verordnung) zurückzuziehen und eine mit den europäischen Grundrechten vereinbare Alternative vorzulegen.

Es ist nicht möglich, privat und sicher zu kommunizieren und zugleich einen direkten Zugriff für Regierungen und Unternehmen einzurichten. Auch böswilligen Akteur.innen würden die Maßnahmen Tür und Tor öffnen. Eine sichere Internet-Infrastruktur, die freie Meinungsäußerung und Selbstbestimmung fördert, ist nicht möglich, wenn Internetnutzer.innen einer allgemeinen Überprüfung und Filterung unterzogen werden können und ihnen Anonymität verweigert wird.

Die vorgeschlagene CSA-Verordnung stuft Scanning- und Überwachungstechnologien – trotz gegenteiliger Expert.innenmeinungen – politisch als sicher ein. Sollte dieses Gesetz verabschiedet werden, wird das Internet in einen Raum verwandelt, **der die Privatsphäre, die Sicherheit und die freie Meinungsäußerung aller Menschen gefährdet**.[1] Dies gilt insbesondere für Kinder und Jugendliche, die mit dieser Verordnung eigentlich geschützt werden sollen.

Die vorgesehenen Vorschriften würden Anbieter.innen sozialer Medien für die von ihren Nutzer.innen geteilten privaten Nachrichten haftbar machen. Das würde Plattformen dazu zwingen, riskante und fehleranfällige Techniken anzuwenden, **um jederzeit Kontrolle darüber zu haben, was wir alle tippen und teilen**. In der Folgenabschätzung, die dem Verordnungsvorschlag beigefügt ist, werden Unternehmen angehalten, Client-

1 Der ehemalige UN-Sonderberichterstatter für das Recht auf freie Meinungsäußerung, David Kaye, betont: „Verschlüsselung und Anonymität ermöglichen es Einzelnen, ihr Recht auf Meinungsfreiheit und freie Meinungsäußerung im digitalen Zeitalter auszuüben."

Side-Scanning einzusetzen, um ihre Nutzer.innen zu überwachen, wohl wissend, dass die Diensteanbieter.innen das aus Sicherheitsgründen skeptisch sehen. Die Verordnung wäre ein noch nie dagewesener Angriff auf das Recht auf private Kommunikation und die Unschuldsvermutung.

Nicht nur Erwachsene sind auf Privatsphäre und Sicherheit angewiesen. Wie die Vereinten Nationen und UNICEF erklären, ist die Privatsphäre im Netz für die Entwicklung und Selbstverwirklichung junger Menschen von entscheidender Bedeutung. Sie sollten keiner Massenüberwachung ausgesetzt werden. Auch das britische Royal College of Psychiatrists weist darauf hin, dass es für Kinder schädlich ist, sie auszuspionieren und dass Maßnahmen, die auf Selbstbefähigung und Bildung basieren, sie im Netz wirkungsvoller schützen.

Die CSA-Verordnung wird in vielerlei Hinsicht schweren Schaden anrichten:

- **Eine private Nachricht über die eigene Missbrauchserfahrung**, die für einen vertrauenswürdigen Erwachsenen gedacht ist, könnte automatisch markiert, von den Mitarbeiter.innen eines Social-Media-Unternehmens geprüft und dann zur Untersuchung an die Strafverfolgungsbehörden weitergeleitet werden. Das geschähe gegen den Willen der Betroffenen und verletzt ihre Würde. Das könnte Opfer davon abhalten, sich Hilfe zu holen;
- **Whistleblower.innen** und Quellen, die anonym über Korruption in der Regierung berichten wollen, könnten sich nicht mehr auf Online-Kommunikationsdienste verlassen, da die Ende-zu-Ende-Verschlüsselung ausgehebelt wäre. Bemühungen, Machthaber.innen zur Rechenschaft zu ziehen, würden erheblich erschwert;
- Private intime **Fotos jung aussehender Erwachsener**, die diese rechtmäßig an ihre Partner.innen schicken, könnten von der KI fälschlich markiert werden, Mitarbeiter.innen sozialer Medien angezeigt werden und dann an Strafverfolgungsbehörden geleitet werden;
- Solche unvermeidlichen Falschmeldungen **würden Strafverfolgungsbehörden überlasten**, die bereits jetzt nicht über die Ressourcen verfügen, alle Fälle zu bearbeiten. Sie müssten ihre begrenzten Kapazitäten darauf verwenden, riesige Mengen rechtmäßiger Kommunikation zu sichten, anstatt gefundenes Missbrauchsmaterial zu löschen und Verdächtige und Täter.innen zu verfolgen;
- Bisher sichere Messengerdienste, zum Beispiel Signal, wären gezwungen, ihre Dienste technisch unsicher zu machen. Nutzer.innen hätten dann keine sichere Alternative mehr. Dies würde alle gefährden, die sich auf sichere Kommunikation verlassen: **Anwältinnen, Journalisten, Menschenrechtsverteidigerinnen, NGO-Mitarbeiter – einschließlich derer, die Opfern helfen –, Regierungsmitglieder** und viele andere. Wenn Dienste die

Nachrichten weiterhin verschlüsseln wollen, würden sie mit einer Geldstrafe in Höhe von sechs Prozent ihres weltweiten Umsatzes belegt oder gezwungen, sich aus dem EU-Markt zurückzuziehen;

- **Quellenschutz und die digitale Sicherheit von Journalist.innen** werden gefährdet, weil damit Ende-zu-Ende-Verschlüsselung abgeschafft würde. Außerdem wird die Pressefreiheit durch den "Chilling Effect" der Maßnahmen eingeschränkt;
- Sobald diese Technologie eingeführt wäre, könnten Regierungen auf der ganzen Welt Unternehmen gesetzlich dazu verpflichten, nach Beweisen für **politische Opposition zu suchen, nach Aktivist.innen, gewerkschaftlichen Zusammenschlüssen und auch nach Menschen, die abtreiben lassen, wo Abtreibung kriminalisiert ist** – also nach allem, was eine Regierung womöglich unterdrücken möchte;
- **Bereits entrechtete, verfolgte und marginalisierte Gruppen auf der ganzen Welt wären von diesen Bedrohungen besonders betroffen.**

In den vergangenen Jahren ist die EU zum Vorreiter für das Menschenrecht auf Privatsphäre und Datenschutz geworden und hat damit einen weltweiten Standard gesetzt. Doch mit der vorgeschlagenen CSA-Verordnung macht die Europäische Kommission eine Kehrtwende in Richtung Autoritarismus, Kontrolle und Zerstörung der Freiheit im Netz. Dies wäre ein gefährlicher Präzedenzfall für weltweite Massenüberwachung.

Zum Schutz der freien Meinungsäußerung, der Privatsphäre und der Sicherheit im Internet fordern wir, die unterzeichnenden 73 Organisationen, Sie als Mitglieder der Kommission auf, die Verordnung zurückzuziehen.

Wir fordern stattdessen zielgerichtete, rechtmäßige und technisch machbare Alternativen, um das schwerwiegende Problem des Missbrauchs von Kindern zu bekämpfen. Maßnahmen müssen der Selbstverpflichtung der EU "Digitalen Dekade" zu einem „sicheren und geschützten" digitalen Umfeld für alle entsprechen – das schließt Kinder und Jugendliche ausdrücklich ein.

Unterzeichnet,

1. Access Now – International
2. Alternatif Bilisim (AiA-Alternative Informatics Association) – International
3. APADOR-CH – Rumänien
4. ApTI Romania – Rumänien
5. ARTICLE 19 – International
6. Aspiration – USA
7. Attac Austria - Österreich
8. Aufstehn.at – Österreich
9. Austrian Chamber of Labour – Österreich
10. Big Brother Watch – Großbritannien
11. Bits of Freedom – Niederlande
12. Center for Civil and Human Rights (Poradňa) - Slowakei

13. Centre for Democracy & Technology – Europa
14. Chaos Computer Club – Deutschland
15. Centrum Cyfrowe – Europa
16. Citizen D / Državljan D – Slowenien
17. Civil Liberties Union for Europe – Europa
18. Committee to Protect Journalists – EU/International
19. COMMUNIA Association for the Public Domain – Europa
20. D64 – Zentrum für Digitalen Fortschritt – Deutschland
21. Dataskydd.net – Schweden
22. Defend Digital Me – Großbritannien
23. Deutsche Vereinigung für Datenschutz (DVD) – Germany
24. DFRI – Schweden
25. Digitalcourage – Deutschland
26. Digitale Gesellschaft – Deutschland
27. Digitale Gesellschaft / Digital Society – Schweiz
28. Digital Rights Ireland – Irland
29. European Digital Rights (EDRi) - Europa
30. Electronic Frontier Finland – Finnland
31. Elektronisk Forpost Norge (EFN) – Norwegen
32. Electronic Frontier Foundation (EFF) – International
33. The Electronic Privacy Information Center (EPIC) – International
34. epicenter.works for digital rights – Österreich
35. Equipo Decenio Afrodescendiente – Spanien
36. Internet Society Catalan Chapter (ISOC-CAT) – Europa
37. Eticas Foundation – International
38. European Center for Not-For-Profit Law (ECNL) – Europa
39. The European Federation of Journalists (EFJ) – Europa
40. Fitug e.V. – Deutschland
41. The Foundation for Information Policy Research (FIPR) – Großbritannien
42. Global Forum for Media Development – International
43. Hermes Center for Transparency and Digital Human Rights – Italien
44. Homo Digitalis – Griechenland
45. Human Rights House Zagreb – Kroatien
46. iNGO European Media Platform – Europa
47. International Press Institute (IPI) – International
48. Irish Council for Civil Liberties – Irland
49. IT-Pol – Dänemark
50. Iuridicum Remedium – Tschechien
51. La Quadrature du Net – Frankreich
52. Ligue des droits humains – Belgien
53. Lobby4kids – Kinderlobby – Österreich
54. Netherlands Helsinki Committee – TNiederlande
55. Nordic Privacy Center – Nordische Staaten
56. Norway Chapter of the Internet Society – Norwegen
57. Norwegian Unix User Group – Norwegen
58. Österreichischer Rechtsanwaltskammertag – Österreich
59. Open Rights Group – Großbritannien
60. quintessenz - Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter – Österreich

61. Panoptykon Foundation – Polen
62. Peace Institute – Slowenien
63. Presseclub Concordia – Österreich
64. Privacy First – Niederlande
65. Privacy International – International
66. Ranking Digital Rights – International
67. Statewatch EU – Europa
68. Vrijschrift.org – Niederlande
69. Whistleblower-Netzwerk – Deutschland
70. Wikimedia – International
71. Women's Link Worldwide – Europa
72. Worker Info Exchange – International
73. Xnet – Spanien