www.jusletter-it.eu

Simon Schlauri

Fernmeldeüberwachung: Chatkontrolle durch die Hintertür?

Beitragsart: TechLawNews by Ronzani Schlauri Attorneys
Region: EU
Rechtsgebiete: Telekommunikationsrecht

Zitiervorschlag: Simon Schlauri, Fernmeldeüberwachung: Chatkontrolle durch die Hintertür?, in: Jusletter IT 31. Mai 2022

Inhaltsübersicht

Umstrittener Vorschlag für Chatkontrolle in der EU

[1] Am 5. Mai 2022 veröffentlichte die EU-Kommission einen Entwurf für eine Verordnung zur Bekämpfung von Kindesmissbrauch: Anbieterinnen von Kurznachrichtendiensten wie Threema, Signal oder iMessage sollen durch die neuen Regeln unter anderem verpflichtet werden, Fotos und Videos von Kindesmissbrauch in ihren Nachrichten ausfindig zu machen und gegen sogenanntes Grooming[1] vorzugehen. Der Vorstoss stiess weitherum auf heftige Kritik.[2] Dies insbesondere, weil er dazu führt, dass die bisher in solchen Diensten meist genutzte Ende-zu-Ende-Verschlüsselung aufgeweicht werden müsste, was faktisch die Tür zur Massenüberwachung aufstiesse und einen schweren Eingriff in die Grundrechte darstellte.[3]

Revision der Ausführungsverordnungen zum BÜPF

[2] In der Schweiz ist derzeit eine Revision der Ausführungsverordnungen zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) im Gang. Bis zum 23. Mai 2022 lief die entsprechende Vernehmlassungsfrist.[4]

[3] Im Zusammenhang mit dieser Revision sorgte die Einführung einer Entschlüsselungspflicht (Art. 50 Abs. 7 E-VÜPF) für Aufsehen. Die Norm lautet:

> «*Jede FDA*[5] *und jede AAKD*[6] *mit weitergehenden Pflichten gemäss Artikel 22 oder 52*[7] *entfernt die von ihr oder für sie angebrachten Verschlüsselungen. Sie erfasst und entschlüsselt dafür den Fernmeldeverkehr der überwachten Person an geeigneten Punkten, damit die Überwachungsdaten ohne die vorgenannten Verschlüsselungen geliefert werden.*»

1 Als Grooming bezeichnet man die gezielte Manipulation Minderjähriger mit dem Ziel, das Opfer in eine Falle zu locken, um Straftaten, insbesondere solche gegen die sexuelle Integrität, zu begehen.

2 Vgl. etwa Heise Newsticker vom 11. Mai 2022, Chatkontrolle: EU-Kommission bringt Verordnung für Kinderporno-Scans auf den Weg, tinyurl.com/mrybk2f5.

3 Einen schwerwiegenden Eingriff sieht etwa auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB; zit. bei D. Schurter, Oberster Schweizer Datenschützer spricht sich gegen Aufweichung der Verschlüsselung aus, in: watson, 20. Mai 2022, tinyurl.com/yc3vnvd7.

4 tinyurl.com/jvzmhwc8.

5 Anbieterin von Fernmeldediensten wie Telefonie, SMS oder Internetzugang.

6 Anbieterin abgeleiteter Kommunikationsdienste (d.h. von Diensten, die *über* das Internet vermittelt werden und nicht selber Internetzugangsdienste sind).

7 AAKD, die bestimmte Schwellenwerte erreichen (beispielsweise 100 Auskunftsanfragen pro Jahr), können vom Dienst ÜPF «upgegradet» werden, mit dem Ergebnis, dass sie vergleichbare Überwachungspflichten wie herkömmliche Anbieterinnen von Fernmeldediensten zu erfüllen haben.

[4] Kritisch sind dabei zwei verschiedene Aspekte:

a. Handelt es sich bei Ende-zu-Ende-Verschlüsselung um «*von* der Anbieterin oder *für* die Anbieterin» angebrachte Verschlüsselung?
b. Könnte der in einer Kommunikations-App integrierte Verschlüsselungsmechanismus als «geeigneter Punkt für die Entschlüsselung» verstanden werden?

[5] Im Rahmen des Vernehmlassungsverfahrens erkundigte sich der Schreibende beim Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF), der die Vernehmlassung im Auftrag des Bundesrates durchführte, ob die entsprechenden Formulierungen zu einer Pflicht führen würden, eine «Backdoor» in Kommunikationssoftware einzuführen.

[6] Der Dienst ÜPF verneinte diese Frage ausdrücklich. Er schrieb:

> *«Beim neuen Art. 50 Abs. 7 E-VÜPF handelt es sich nicht um eine Pflicht zur Einrichtung einer «Backdoor» in der von der Betreiberin angebotenen Software. Insbesondere nicht betroffen ist daher die End-to-End Verschlüsselung in der von Ihnen geschilderten Situation, wo der Kunde eine Verschlüsselung auf seinem Endgerät mittels Kommunikationssoftware, die von der Betreiberin angeboten wird, auf Inhalten anbringt, die an andere Kunden gerichtet sind.»*

Rechtliche Aspekte

[7] In der Tat ist keine andere Auslegung der gesetzlichen Grundlage des BÜPF denkbar: Art. 26 Abs. 2 Bst. c sieht seit jeher vor, dass Anbieterinnen von Fernmeldediensten *von ihnen* angebrachte Verschlüsselungen entfernen müssen. Dabei geht es um Verschlüsselungen, welche die Anbieterinnen selber anbringen, um die Kommunikationswege abzusichern oder Verschlüsselungstechnik zur Absicherung von gespeicherten Daten. Im Gegensatz dazu wird eine Ende-zu-Ende-Verschlüsselung vom Nutzer selber angebracht, und nicht von der Anbieterin.

[8] Die Ende-zu-Ende-Verschlüsselung hat gerade das Ziel, dass auch die Anbieterin selber die übermittelten Daten nicht sehen kann und dient dem Datenschutz: Der Grundsatz der Datenminimierung (ein Teilaspekt des datenschutzrechtlichen Verhältnismässigkeitsgrundsatzes von Art. 4 Abs. 2 DSG) besagt nämlich, dass nur jene Daten bearbeitet werden dürfen, die für die Bearbeitung auch notwendig sind. Und für die Übermittlung von Daten muss eine Anbieterin keinen Zugriff auf die übermittelten Daten haben, sodass sich eine Pflicht für die Anbieterinnen, eine Ende-zu-Ende-Verschlüsselung m.E. sogar aus dem Datenschutzgesetz ergibt. Zudem werden Daten oftmals sogar «peer-to-peer», d.h. direkt zwischen den Endgeräten und ohne Umweg über die Server der Anbieterin, übermittelt.

[9] Die übermittelte Information wird in aller Regel mit «Public-Key-Kryptografie» verschlüsselt. Dazu nutzt die Software auf dem Endgerät des Absenders einen öffentlich verfügbaren Verschlüsselungsschlüssel («public key») des Empfängers, dessen Gegenstück (Entschlüsselungsschlüssel, «private key») nur der Empfänger kennt. Die Verschlüsselung erfolgt dabei für die Nutzer transparent in der jeweiligen App. D. h. der Nutzer bekommt die Details der Verschlüsselung gar nicht mit; sie läuft im Hintergrund ab.

[10] Eine Auslegung der neuen VÜPF in einer Weise, die eine derartige Pflicht für Anbieterinnen abgeleiteter Dienste zur Einrichtung einer «Backdoor» einschliessen würde, ist damit von der gesetzlichen Grundlage des BÜPF nicht gedeckt und verstiesse zudem gegen das Datenschutzgesetz.

Schlussfolgerungen

[11] Nachdem das Bundesgericht sich in Überwachungssachen bereits mehrfach nonchalant – oder auch aus technischem Unverstand – über die gesetzlichen Grundlagen des BÜPF hinweggesetzt und teils sogar freihändig erhebliche neue Überwachungspflichten einführt hat,[8] ist die in der Vernehmlassung geäusserte Forderung, man solle die Unklarheit doch bitte im erläuternden Bericht oder dem Verordnungstext klarstellen, auf jeden Fall zu unterstützen. Nicht dass der Dienst ÜPF oder gar die Gerichte noch auf die Idee kommen, die in der EU aufs Schärfste kritisierte Chatkontrolle in der Schweiz durch die Hintertür einer Verordnung einzuführen.

8 Etwa indem es eine Entschädigung von drei Franken für 40 Minuten Arbeit einer Fernmeldeanbieterin als «angemessen» im Sinne von Art. 38 BÜPF taxierte (Urteil 2C_650/2020 vom 27. Juli 2021), oder, besonders irritierend, indem es einen Anbieter eines Internet-Diskussionsforums unter den Begriff «Internetanbieter» des alten BÜPF subsumierte, obwohl der französische Gesetzeswortlaut, «fournisseurs d'accès Internet», eine solche Interpretation diametral ausschloss (Urteil 6B_766/2009 vom 8. Januar 2010).