

Anfrage

**der Abgeordneten Douglas Hoyos-Trauttmansdorff, Dr. Nikolaus Scherak, MA,
Kolleginnen und Kollegen**

an die Bundesministerin für Digitalisierung und Wirtschaftsstandort

betreffend Regulation gegen sichere Verschlüsselung auf EU-Ebene

Seit einigen Monaten wird auf EU-Ebene die Einführung von Maßnahmen gegen die missbräuchliche Verwendung verschlüsselter Messenger-Dienste für illegale Aktivitäten diskutiert. EU-Innenkommissarin Ylva Johansson kündigte im Juli 2020 an, dass Serviceanbieter dazu verpflichtet werden sollen, ihre Plattformen aktiv nach illegalen Inhalten zu durchsuchen. Das gelte auch für verschlüsselte Nachrichten (<https://fm4.orf.at/stories/3006235/>). Der für digitale Dienste zuständige EU-Binnenmarktkommissar Thierry Breton bestätigte im August 2020, dass die EU Maßnahmen setzen wird, um Anbieter Ende-zu-Ende (end-to-end, E2E) verschlüsselter Chat-Services in die Pflicht zu nehmen (<https://fm4.orf.at/stories/3006235/>).

In einem Anfang September 2020 bekannt gewordenen 30-seitigen Arbeitspapier der Europäischen Kommission werden verschiedene technische Möglichkeiten zur Durchsuchung von E2E-verschlüsselter Kommunikation nach illegalen Inhalten detailliert dargelegt. Darin wird auch festgehalten, dass E2E-verschlüsselte Nachrichten von Dritten nicht durchsucht werden können, sowie andere technische Möglichkeiten der Verschlüsselung präsentiert.

Am 10. September 2020 legte die EU-Kommission schließlich einen Vorschlag für eine neue Verordnung vor, in der vorgesehen ist, dass zum Aufspüren gewisser illegaler Inhalte auch verschlüsselte Kommunikation durchsucht werden können soll (<https://ec.europa.eu/digital-single-market/en/news/interim-regulation-processing-personal-and-other-data-purpose-combatting-child-sexual-abuse>). Dieser Vorschlag sieht die Einführung einer Ausnahme vom Schutz der Privatsphäre, der Vertraulichkeit von Kommunikation und der persönlichen Daten im Bereich der elektronischen Kommunikation vor.

Anfang November wurde bekannt, dass laut einem internen Dokument der deutschen Ratspräsidentschaft an die Delegationen der Mitgliedsstaaten der Terroranschlag in Wien im EU-Ministerrat dazu benützt werde, um ein Verbot sicherer Verschlüsselung für Services wie WhatsApp, Signal und viele andere im Schnellsiedeverfahren durchzusetzen (<https://fm4.orf.at/stories/3008930/>). Eine Resolution des Ministerrats sei laut Dokument - da wird um allfällige letzte Einwände gebeten - nicht nur fast fertig ausformuliert. Sie sei im Rat offenbar auch bereits fertig abgestimmt. Am 19. November soll sie dann in der Ratsarbeitsgruppe zur Kooperation im nationalen Sicherheitsbereich (COSI) verabschiedet werden, am 25. ist die Vorlage im Rat der ständigen Vertreter der EU-Mitgliedsstaaten (COREPER) geplant. Dort hat der Ratsresolution bereits den Status eines I-Items, damit kann er ohne weitere Diskussion heuer noch verabschiedet werden. In einer für Anfang Dezember geplanten virtuellen Sitzung des Rats der Innen- und Justizminister soll die Resolution dann offiziell werden.

Durch die vorgeschlagenen Maßnahmen könnten Anbieter von Messenger-Diensten dazu gezwungen werden, die Sicherheit ihrer Services zugunsten von Überwachbarkeit aufzugeben. Es besteht die Befürchtung, dass das Vorhaben darauf hinaus läuft, dass E2E-verschlüsselte Services wie WhatsApp, Signal oder Wire so nicht mehr angeboten werden könnten, was das Ende sicherer digitaler Kommunikation bedeuten

würde. Expert_innen befürchten daher durch eine Aufhebung von E2E-Verschlüsselung massive Einschnitte in die Sicherheit der Nutzer_innen, sowohl aus technischer, als auch aus demokratischer Sicht.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Wie hat Österreich zur in der Begründung näher beschriebenen Thematik der Einschränkung von E2E-Verschlüsselung auf EU-Ebene bisher abgestimmt?
2. Wie wird Österreich bei künftigen Abstimmungen zu dieser Thematik auf EU-Ebene abstimmen?
3. Mit welcher Begründung spricht man sich für eine Einschränkung der E2E-Verschlüsselung aus?
 - a. Sind Ihrem Ministerium die technischen Sicherheitsprobleme, die allen User_innen durch eine Einschränkung der E2E-Verschlüsselung entstehen, bekannt?
 - i. Wenn ja, mit welcher Begründung wird das Inkaufnehmen dieser Sicherheitsprobleme für alle User_innen gerechtfertigt?

N. Scherndl
(SCHERNDL)



