Rat der Europäischen Union

Brüssel, den 6. November 2020
(OR. en)

**12143/1/20**
**ÜBF 1**

**LIMITE**

**JAI 851**
**COSI 156**
**CATS 73**
**ENFOPOL 256**
**COPEN 287**
**DATAPROTECT 106**
**CYBER 198**
**IXIM 107**

**VERMERK**

| | |
|---|---|
| Von: | Ratspräsidentschaft |
| An: | Delegationen |
| Thema: | Entwurf für einen Beschluss des Rates zur Verschlüsselung - Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung |

Die Delegationen erhalten beiliegend die überarbeitete Fassung[1] des Entwurfs für einen Beschluss des Rates zur Verschlüsselung. Er gibt die von den Mitgliedsstaaten vor und während der am 3. November 2020 abgehaltenen informellen VTC Sitzung der JHA Counsellors (Verschlüsselung) vorgebrachten Anmerkungen wieder.

Sofern die Delegationen keine weiteren Sachvorträge mit entsprechend ausformulierten Vorschlägen bis 12. November 2020, 12 Uhr an paul.gaitzsch@diplo.de, COSI.DE2020@bmi.bund.de und cosi@consilium.europa.eu eingereicht haben, legt die Ratspräsidentschaft diesen überarbeiteten Text COSI (VTC) am 19. November 2020 zur Zustimmung vor im Hinblick darauf, dass er am 25. November 2020 COREPER (I-item) vorgelegt und schließlich vom Rat in einem schriftlichen Verfahren angenommen wird.

Bitte beachten Sie, dass das Dokumentenformat an einen „Beschluss des Rates“ angepasst wurde, so dass der Text zur Annahme in einem schriftlichen Verfahren durch den Rat angenommen werden könnte, wenn es in einem VTC-Format abläuft.

[1] Änderungen zur vorherigen Fassung sind **fett unterstrichen** und ~~durchgestrichen~~ markiert.

**ANLAGE**

**Entwurf für einen Beschluss des Rats zur Verschlüsselung**
**Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung**

1. Präambel: Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung

Die Europäische Union befürwortet die Entwicklung, Umsetzung und Nutzung einer starken Verschlüsselung in vollem Umfang. Bei der Verschlüsselung handelt es sich um eine Maßnahme zum Schutz der Grundrechte und digitalen Sicherheit von Regierungen, Industrie und der Gesellschaft. Gleichzeitig muss die Europäische Union sicherstellen, dass die für **die Bereiche Sicherheit und Strafgerichtsbarkeit zuständigen Behörden und Stellen, wie beispielsweise** Vollstreckungs- und Justizbehörden, in der Lage sind, die ihnen rechtmäßig übertragenen Befugnisse online und offline auszuüben.

Nach den Schlussfolgerungen des Europäischen Rates vom 1. + 2. Oktober 2020 (EUCO 13/20) *wird die EU ihre Werkzeuge und regulatorischen Befugnisse zur Schaffung von weltweiten Regeln und Standards einsetzen.* Man hat sich darauf verständigt, finanzielle Mittel aus der Aufbau- und Resilienzfazilität auf die Erreichung von Zielen zu verwenden. Hierzu zählen beispielsweise *die Stärkung Europas, sich vor Bedrohungen aus dem Netz zu schützen, ein sicheres Kommunikationsumfeld, insbesondere durch Quantenverschlüsselung, zu schaffen und den Zugriff auf Daten für juristische und gesetzesvollziehende Zwecke zu gewährleisten.*

2. Derzeitige Nutzung / Verschlüsselungsstatus

In der heutigen Welt kommt die Verschlüsselungstechnologie in allen Bereichen des öffentlichen und privaten Lebens mehr und mehr zum Einsatz. Sie stellt eine Maßnahme zum Schutz der Regierungen, **kritischen Infrastrukturen,** Zivilgesellschaft, Bürger und Industrie durch Sicherung der Privatsphäre, **Vertraulichkeit** und **Datenintegrität** von Kommunikation und personenbezogenen Daten dar: Es ist erkennbar, dass alle Beteiligten von der Hochleistungsverschlüsselungstechnologie profitieren. Verschlüsselung wurde von den Datenschutzbehörden der EU als wichtiges Werkzeug zum Schutz von personenbezogenen Daten ausgemacht, die in Länder außerhalb der EU übermittelt werden, **vorausgesetzt jedoch, ein im wesentlichen vergleichbares Schutzniveau** liegt vor, was nach Ansicht des Gerichtshofes eine gesetzliche Anforderung an die Datenübertragungen[2] ist. Nicht nur, dass elektronische Geräte und Anwendungen immer häufiger so programmiert sind, dass sie standardmäßig die gespeicherten Nutzerdaten verschlüsseln, sondern es sind auch immer mehr Kommunikationskanäle durch eine Ende-zu-Ende-Verschlüsselung (E2E) gesichert. Dies wird positiv durch eine zunehmende Reaktion der Kommunikations- und App-Unternehmen verstärkt, wo Instant Messanger-Apps und andere Online-Plattformen mehrheitlich ebenfalls die Ende-zu-Ende Verschlüsselung implementiert haben.

[2] Urteil vom 16. Juli 2020 im Verfahren C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

3. Herausforderungen bei der Gewährleistung der öffentlichen **Sicherheit**

„Digitales Leben“ und Cyberspace sind nicht nur Chance, sondern auch enorme Herausforderung: Mit der Digitalisierung der modernen Gesellschaften gehen gewisse Verletzlichkeiten und das Potential für eine **Ausbeutung für kriminelle Zwecke** einher. Daher können Straftäter die für legale Zwecke entwickelten frei erhältliche Standardverschlüsselungslösungen in ihre *modi operandi* [3] integrieren.

Gleichzeitig ist der Gesetzesvollzug zunehmend abhängig vom Zugriff auf elektronische Beweismittel bei der wirksamen Bekämpfung von Terrorismus, organisierter Kriminalität, sexuellem Missbrauch von Kindern (vor allem die digitalen Seiten) sowie einer Vielzahl cyberfähiger Straftaten. **Für die zuständigen Behörden ist der Zugriff auf elektronische Beweismittel nicht nur entscheidend für den Erfolg ihrer Ermittlungen und damit für die Überführung der Straftäter, sondern auch für den Schutz und die Sicherheit der Opfer.**

Es gibt aber Einzelfälle, in denen die Verschlüsselung die Analyse des Inhalts von Kommunikationen im Rahmen des Zugriffs auf elektronische Beweismittel extrem erschwert **oder nahezu unmöglich macht, trotz der Tatsache, dass der Zugriff auf solche Daten rechtmäßig wäre.** Ungeachtet des technologischen Umfelds der Gegenwart gilt es daher, den **für die Bereiche Sicherheit und Strafgerichtsbarkeit zuständigen** Behörden ihre Befugnisse zu bewahren, durch rechtmäßigen Zugriff ihren gesetzlich vorgeschriebenen Aufgaben nachzukommen. Derartige Gesetze zur Durchsetzung von Befugnissen haben stets das ordnungsgemäße Verfahren und sonstige Garantien vollumfänglich zu beachten und andere Freiheiten und Rechte, insbesondere das Recht auf Schutz der Privatsphäre und Kommunikation sowie das Recht auf Schutz personenbezogener Daten.

4. Schaffung eines **besseren** Ausgleichs

Das Prinzip der Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung ist vollständig beizubehalten. Die Europäische Union spricht sich weiterhin für eine starke Verschlüsselung aus. Verschlüsselung ist ein Anker des Vertrauens in der Digitalisierung und **beim Schutz der Grundrechte und** sollte gefördert und ausgebaut werden.

Der Schutz der Privatsphäre und der Sicherheit der Kommunikation durch Verschlüsselung und die gleichzeitige Aufrechterhaltung der Möglichkeit des legalen Zugriffs der für die Bereiche Sicherheit und Strafgerichtsbarkeit zuständigen Behörden auf die einschlägigen Daten zu berechtigten, klar festgelegten Zwecken bei der Bekämpfung schwerer Straftaten **und/oder organisierter** Kriminalität **und von Terrorismus,** die digitale Welt inbegriffen, sind außerordentlich wichtig. Bei jeder Maßnahme sind diese Interessen sorgfältig gegeneinander abzuwägen.

5. Verbindung mit Kräften der Technologie-Industrie

Die Europäische Union sucht im Sinne des Fortschritts den offenen Dialog mit der Technologieindustrie **während sie gleichzeitig Forschung und Hochschulen verbindet**, um die dauerhafte Implementierung und Nutzung der starken Verschlüsselungstechnologie sicherzustellen. Den **zuständigen** Behörden muss es möglich sein, auf rechtmäßige und

[3] iOCTA 2020, S. 25

zielgerichtete Art und Weise und unter vollumfänglicher Beachtung der Grundrechte und Datenschutzverordnungen auf Daten unter Wahrung der Cybersicherheit zuzugreifen. Technische Lösungen für den Zugriff auf verschlüsselten Daten müssen den Prinzipien Rechtmäßigkeit, **Transparenz**, Erforderlichkeit und Verhältnismäßigkeit entsprechen.

Da es nicht nur einen Weg zur Erreichung der gesetzten Ziele gibt, müssen Regierungen, Industrie, **Forschung und Hochschulen** zusammenarbeiten, um diese **strategische** Balance herbeizuführen.

6. Rechtlicher Rahmen

**Die Wirkungen aus den unterschiedlichen Rechtsverordnungen sind dringend zu überprüfen, um** ein **EU-weit einheitliches** Rechtsregelwerks **voranzubringen**, das **es den zuständigen Behörden ermöglichen würde, ihre operativen Aufgaben erfolgreich durchzuführen. Potentielle technische Lösungen haben die Behörden in die Lage zu versetzen, ihre investigativen Befugnisse nutzen zu können, die auf Verhältnismäßigkeit, Erforderlichkeit und juristische Aufsicht** nach den Gesetzen der einzelnen Staaten beruhen, während sie gleichzeitig die Grundrechte achten und die Vorteile der Verschlüsselung beibehalten. Potentielle Lösungen ~~können möglicherweise der Unterstützung der Service Provider bedürfen~~ sind **unter Mitwirkung der Telekommunikationsanbieter** auf transparente Art und Weise zu entwickeln. **Solche technischen Lösungen könnten es mitunter erforderlich machen**, dass die technischen und **operativen** Fähigkeiten sowie das **Fachwissen der zuständigen** Behörden verbessert werden müssen, um den Herausforderungen der Digitalisierung bei ihrer Arbeit weltweit **gerecht werden zu können**. ~~Dem Prinzip der Verhältnismäßigkeit entsprechend, sind solche Maßnahmen vorzuziehen.~~

~~Die Entwicklung von technischen Werkzeugen zur Unterstützung von Strafverfahren, gilt es ebenfalls zu prüfen. Solche technischen Werkzeuge sollten den in dieser Erklärung ausgeführten Prinzipien unterliegen.~~

7. Innovative investigative Fähigkeiten

Schlussendlich ist **die Verbesserung der Zusammenarbeit** auf EU-Ebene gleichrangig, die **abzielt auf:**

**1)** die Bündelung der Bemühungen aller Mitgliedsstaaten, EU-Institutionen und Organe;
**2)** die Festlegung und Ausarbeitung innovativer Ansätze **angesichts der neuen Technologien;**
**3)** **die Analyse angemessener technischer** und **operativer Lösungen; und**
**4)** **die Bereitstellung maßgeschneiderter erstklassiger Schulungen.**

Technische **und operative** Lösungen, die **in einem Rechtsrahmen verankert sind,** der auf den Prinzipien Rechtmäßigkeit, Erforderlichkeit und Verhältnismäßigkeit beruht, sollten in enger Absprache mit den Service Providern und den zuständigen Behörden entwickelt werden, wenngleich es keine einzige vorgeschriebene technische Lösung gibt, mit Hilfe derer der Zugriff auf verschlüsselte Daten möglich ist.