Rat der
Europäischen Union

Brüssel, den 24. November 2020
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

VERMERK

Absender:	Vorsitz
Empfänger:	Delegationen
Nr. Vordok.:	12863/20
Betr.:	Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung

Die Delegationen erhalten in der Anlage die Entschließung des Rates zur Verschlüsselung.

ANLAGE

Entschließung des Rates zur Verschlüsselung
Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung

1. Präambel: Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung

Die Europäische Union unterstützt uneingeschränkt die Entwicklung, Umsetzung und Nutzung starker Verschlüsselung. Die Europäische Union unterstreicht, dass die uneingeschränkte Wahrung der Grundrechte und der Menschenrechte sowie der Rechtsstaatlichkeit bei allen Maßnahmen im Zusammenhang mit dieser Entschließung – sowohl online als auch offline – gewährleistet werden muss. Verschlüsselung ist ein notwendiges Mittel zum Schutz der Grundrechte und der digitalen Sicherheit von Regierungen, Industrie und Gesellschaft. Gleichzeitig muss die Europäische Union sicherstellen, dass die zuständigen Behörden im Bereich Sicherheit und Strafjustiz, z. B. Strafverfolgungs- und Justizbehörden, ihre gesetzlichen Befugnisse ausüben können und somit sowohl online als auch offline unsere Gesellschaften und Bürgerinnen und Bürger schützen können.

Gemäß den Schlussfolgerungen des Europäischen Rates vom 1./2. Oktober 2020 (EUCO 13/20), *wird die EU ihre Instrumente und Regelungsbefugnisse nutzen, um zur Gestaltung globaler Regeln und Standards beizutragen*. Es wurde vereinbart, dass die Mittel im Rahmen der Aufbau- und Resilienzfazilität verwendet werden, um Ziele zu erreichen wie etwa die *Verbesserung der Fähigkeit der EU, sich vor Cyberbedrohungen zu schützen, für ein sicheres Kommunikationsumfeld zu sorgen – insbesondere durch Quantenverschlüsselung – und den Zugang zu Daten für Gerichts- und Strafverfolgungszwecke sicherzustellen*.

2. Derzeitiger Einsatz/Stand der Verschlüsselung

In der Welt von heute werden Verschlüsselungstechnologien zunehmend in allen Bereichen des öffentlichen und privaten Lebens eingesetzt. Sie tragen dazu bei, Einzelpersonen, die Zivilgesellschaft, kritische Infrastrukturen, die Medien sowie die Journalistinnen und Journalisten, die Industrie und die Regierungen zu schützen, indem sie die Privatsphäre, Vertraulichkeit, Datenintegrität und Verfügbarkeit von Kommunikationsdaten und personenbezogenen Daten sicherstellen: Ganz offensichtlich kommen Verschlüsselungstechnologien allen Seiten zugute. Die EU-Behörden für Datenschutz und Cybersicherheit erkennen die Verschlüsselung als wichtiges Instrument an, das beispielsweise zum Schutz personenbezogener Daten beiträgt, die zwar in Gebiete außerhalb der EU übertragen werden, jedoch dem Erfordernis eines im Wesentlichen gleichwertigen Schutzniveaus unterliegen, was nach Auffassung des Gerichtshofs eine rechtliche Anforderung für Datenübermittlungen darstellt[1]. Es werden nicht nur elektronische Geräte und Anwendungen zunehmend so programmiert, dass sie gespeicherte Nutzerdaten standardmäßig verschlüsseln, sondern auch immer mehr Kommunikationskanäle und Datenspeicherdienste werden durch Ende-zu-Ende-Verschlüsselung (End-to-End/E2E) gesichert. Dies spiegelt sich positiv in einer stärkeren Reaktion der Kommunikations- und Anwendungsbranche wider, in der die meisten Nachrichtenanwendungen (Messaging Apps) und andere Online-Plattformen auch Ende-zu-Ende-Verschlüsselung eingeführt haben.

3. Herausforderungen bei der Gewährleistung der Sicherheit

Der „digitale Alltag“ und der Cyberraum bieten nicht nur große Chancen, sondern bewirken auch große Herausforderungen: Die Digitalisierung moderner Gesellschaften bringt gewisse Schwachstellen und das Potenzial einer Ausbeutung für kriminelle Zwecke mit sich. So können Kriminelle leicht zugängliche, herkömmliche Verschlüsselungslösungen, die für rechtmäßige Zwecke konzipiert sind, für ihre Vorgehensweisen nutzen.[2]

Gleichzeitig hängt die Strafverfolgung zunehmend vom Zugang zu elektronischen Beweismitteln ab, um Terrorismus, organisierte Kriminalität, sexuellen Missbrauch von Kindern (insbesondere dessen Online-Aspekte) sowie eine Vielzahl anderer Cyberstraftaten und durch den Cyberraum ermöglichter Straftaten wirksam zu bekämpfen. Für die zuständigen Behörden kann der Zugang zu elektronischen Beweismitteln von wesentlicher Bedeutung sein, nicht nur um erfolgreiche Ermittlungen durchzuführen und damit Kriminelle vor Gericht zu bringen, sondern auch um die Opfer zu schützen und zur Gewährleistung der Sicherheit beizutragen.

---

[1] Urteil des Gerichtshofs vom 16. Juli 2020 in der Rechtssache C-311/18, Data Protection Commissioner gegen Facebook Ireland Limited und Maximillian Schrems (ECLI:EU:C:2020:559:).

[2] IOCTA 2020, S. 25.

Es gibt jedoch Fälle, in denen die Verschlüsselung den Zugang zu Kommunikationsinhalten und deren Analyse im Rahmen des Zugangs zu elektronischen Beweismitteln äußerst schwierig oder praktisch unmöglich macht, obwohl der Zugang zu diesen Daten rechtmäßig wäre. Unabhängig vom derzeitigen technologischen Umfeld ist es daher unerlässlich, die Befugnisse der zuständigen Behörden im Bereich Sicherheit und Strafjustiz durch rechtmäßigen Zugang zu wahren, damit sie ihre Aufgaben wie gesetzlich vorgeschrieben und zulässig wahrnehmen können. Solche Gesetze, in denen die Durchsetzungsbefugnisse vorgesehen sind, müssen stets im vollen Einklang mit einem ordnungsgemäßen Verfahren und anderen Garantien sowie den Grundrechten stehen, insbesondere dem Recht auf Achtung des Privatlebens und der Kommunikation und dem Recht auf den Schutz personenbezogener Daten.

4. Herstellung des richtigen Gleichgewichts

Der Grundsatz „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ muss in vollem Umfang gewahrt werden. Die Europäische Union unterstützt weiterhin eine starke Verschlüsselung. Verschlüsselung ist ein Stützpfeiler des Vertrauens in die Digitalisierung und in den Schutz der Grundrechte und sollte gefördert und weiterentwickelt werden.

Es ist äußerst wichtig, die Privatsphäre und die Sicherheit der Kommunikation durch Verschlüsselung zu schützen und gleichzeitig für die zuständigen Behörden im Bereich Sicherheit und Strafjustiz die Möglichkeit aufrechtzuerhalten, über einen rechtmäßigen Zugang zu Daten für legitime und klar definierte Zwecke im Rahmen der Bekämpfung schwerer und/oder organisierter Kriminalität und Terrorismus – auch in der digitalen Welt – zu verfügen, und die Rechtsstaatlichkeit zu wahren. Bei allen Maßnahmen müssen diese Interessen sorgfältig gegen die Grundsätze der Notwendigkeit, Verhältnismäßigkeit und Subsidiarität abgewogen werden.

5. Bündelung der Kräfte mit der Technologiebranche

Die Europäische Union ist bestrebt, in einen aktiven Dialog mit der Technologiebranche einzutreten und dabei Forschung und Wissenschaft einzubeziehen, um die weitere Umsetzung und den Einsatz starker Verschlüsselungstechnologien sicherzustellen. Die zuständigen Behörden müssen unter uneingeschränkter Achtung der Grundrechte und der einschlägigen Datenschutzgesetze rechtmäßig und gezielt auf Daten zugreifen können und gleichzeitig die Cybersicherheit wahren. Technische Lösungen für den Zugang zu verschlüsselten Daten müssen den Grundsätzen der Rechtmäßigkeit, Transparenz, Notwendigkeit und Verhältnismäßigkeit – einschließlich des Schutzes personenbezogener Daten durch Technikgestaltung und Voreinstellungen – entsprechen.

Da es keine Patentlösung gibt, um die gesteckten Ziele zu erreichen, müssen Regierungen, Industrie, Forschung und Wissenschaft transparent zusammenarbeiten, um dieses Gleichgewicht strategisch herzustellen.

6. Regelungsrahmen

Die Notwendigkeit, EU-weit einen Regelungsrahmen zu entwickeln, der es den zuständigen Behörden ermöglichen würde, ihre operativen Aufgaben wirksam zu erfüllen und gleichzeitig die Privatsphäre, die Grundrechte und die Sicherheit der Kommunikation zu schützen, könnte weiter bewertet werden.

Potenzielle technische Lösungen müssen es den Behörden ermöglichen, ihre Untersuchungsbefugnisse auszuüben, die nach ihrem innerstaatlichen Recht der Verhältnismäßigkeit, Notwendigkeit und gerichtlichen Kontrolle unterliegen, wobei die gemeinsamen europäischen Werte und die Grundrechte zu achten und die Vorteile der Verschlüsselung zu wahren sind. Mögliche Lösungen sollten in transparenter Weise und in Zusammenarbeit mit den nationalen und internationalen Anbietern von Kommunikationsdiensten und anderen einschlägigen Interessenträgern entwickelt werden. Solche technischen Lösungen und Normen – sowie die rasche Entwicklung der Technologie im Allgemeinen – würden es auch erfordern, dass die technischen und operativen Kompetenzen und Fachkenntnisse der zuständigen Behörden kontinuierlich verbessert werden, um die Herausforderungen der Digitalisierung bei ihrer Arbeit auf globaler Ebene anzugehen.

7. Innovative Ermittlungskapazitäten

Es ist von größter Bedeutung, die Koordinierung auf EU-Ebene zu verbessern um

1. die Bemühungen aller Mitgliedstaaten und der Organe und Einrichtungen der EU zu bündeln,

2. innovative Konzepte im Hinblick auf neue Technologien zu bestimmen und festzulegen,

3. geeignete technische und operative Lösungen zu analysieren und

4. maßgeschneiderte und hochwertige Schulungen bereitzustellen.

In enger Abstimmung mit den Diensteanbietern, anderen einschlägigen Interessenträgern und allen einschlägigen zuständigen Behörden sollten technische und operative Lösungen, die in einem auf den Grundsätzen der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit beruhenden Regelungsrahmen verankert sind, entwickelt werden; es sollte jedoch keine einheitliche vorgeschriebene technische Lösung für den Zugang zu verschlüsselten Daten geben.