Anfrage zur schriftlichen Beantwortung E-004790/2021
an die Kommission
Artikel 138 der Geschäftsordnung
Patrick Breyer (Verts/ALE)

Betrifft: Verwendung unsicherer Verschlüsselungsstandards in strafrechtlichen Angelegenheiten und Strafsachen

1. Welche Verschlüsselungs- und Hash-Algorithmen und welche Schlüssellängen werden derzeit verwendet, um die Vertraulichkeit und Integrität dieser Daten bei ihrer Übermittlung zu schützen, wenn öffentliche Stellen der EU wie Europol DNS-Daten, Fingerabdrücke und andere biometrische Daten (wie Daten zur Gesichtserkennung) austauschen?

2. Gemäß dem Beschluss 2008/616/JI des Rates ist in Bezug auf den Austausch von DNS-Daten vorgesehen, dass die „Verschlüsselungsalgorithmen AES (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bit und RSA (Rivest–Shamir–Adleman) mit einer Schlüssellänge von 1 024 Bit“ sowie der „Hash-Algorithmus SHA-1“ verwendet werden. Allerdings ist der Hash-Algorithmus SHA-1 im Jahr 2017 entschlüsselt worden, und die 1 024-Bit-RSA-Verschlüsselung ist anfällig für Brute-Force-Angriffe (d.h. das Ausprobieren aller möglichen Codes) mithilfe besonders leistungsfähiger moderner Rechner. Wann werden die in diesem Beschluss festgelegten Rechtsvorschriften aktualisiert, um sicherzustellen, dass der kryptografische Schutz bei der grenzüberschreitenden Datenübermittlung auf der Grundlage aktueller technischer Leitlinien erfolgt?

3. Besteht bei einer grenzüberschreitenden Zusammenarbeit in strafrechtlichen Angelegenheiten und Strafsachen generell die Verpflichtung, beim Austausch personenbezogener Daten Verschlüsselungsmechanismen zum Schutz der Vertraulichkeit und Integrität der Daten zu verwenden? Wenn ja, wo und auf der Grundlage welcher technischen Empfehlungen sind die entsprechenden Schutzniveaus festgelegt?