Europeiska unionens råd

Bryssel 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

NOT

från:	Ordförandeskapet
till:	Delegationerna
Föreg. dok. nr:	12863/20
Ärende:	Rådets resolution om kryptering – Säkerhet genom kryptering och säkerhet trots kryptering

För delegationerna bifogas rådets resolution om kryptering.

BILAGA

Rådets resolution om kryptering
Säkerhet genom kryptering och säkerhet trots kryptering

1. Ingress: Säkerhet genom kryptering och säkerhet trots kryptering

Europeiska unionen stöder till fullo utvecklingen, genomförandet och användningen av stark kryptering. Europeiska unionen understryker behovet av att säkerställa att de grundläggande och mänskliga rättigheterna samt rättsstatsprincipen respekteras fullt ut i alla åtgärder beträffande denna resolution, såväl online som offline. Kryptering är ett nödvändigt sätt att skydda grundläggande rättigheter och den digitala säkerheten för stater, näringslivet och samhället. Samtidigt måste Europeiska unionen säkerställa att behöriga myndigheter på området säkerhet och straffrätt, t.ex. brottsbekämpande och rättsliga myndigheter, kan utöva sina lagliga befogenheter, både online och offline, och skydda vårt samhälle och medborgarna.

Enligt Europeiska rådets slutsatser av den 1–2 oktober 2020 (EUCO 13/20) ”kommer EU att utnyttja sina verktyg och sin regleringsmakt för att bidra till att utforma globala regler och standarder”. Man enades om att medel från faciliteten för återhämtning och resiliens skulle användas för att bidra till mål som t.ex. ”stärkande av EU:s förmåga att skydda sig mot cyberhot, tillhandahålla en säker kommunikationsmiljö, särskilt genom kvantkryptering, och säkerställa tillgång till uppgifter för rättsliga och brottsbekämpande ändamål”.

2. Nuvarande användning av/situation för kryptering

I dagens värld används krypteringsteknik i allt högre grad inom alla områden i det offentliga såväl som privata rummet. Det är ett sätt att skydda enskilda personer, det civila samhället, kritisk infrastruktur, medier och journalister, näringslivet och stater genom att säkerställa integritet, konfidentialitet, dataintegritet och tillgång till kommunikation och personuppgifter. Det är uppenbart att alla parter tjänar på krypteringstekniken. EU:s dataskyddsmyndigheter och it-säkerhetsmyndigheter har fastställt att kryptering är ett viktigt verktyg som exempelvis bidrar till att skydda personuppgifter som överförs till länder utanför EU men som omfattas av kravet på en väsentligen likvärdig skyddsnivå, vilket enligt domstolen är ett rättsligt krav för överföringar av uppgifter[1]. Inte bara programmeras elektronisk utrustning och applikationer i allt högre utsträckning till att automatiskt kryptera lagrade användardata, utan allt fler kommunikationskanaler och datalagringstjänster säkras också genom totalsträckskryptering (E2E). Detta återspeglas uttryckligen i ett ständigt ökande gensvar från kommunikations- och applikationsbranschen, där de allra flesta snabbmeddelandeapparna och andra onlineplattformar också har infört totalsträckskryptering.

3. Utmaningar när det gäller att garantera säkerheten

Det digitala livet och cyberrymden innebär inte enbart stora möjligheter utan också betydande utmaningar: digitaliseringen av moderna samhällen medför vissa sårbarheter och kan utnyttjas för kriminella ändamål. Brottslingar kan således använda sig av lättillgängliga, standardiserade krypteringslösningar utformade för legitima ändamål i sina metoder[2].

Samtidigt är brottsbekämpningen i allt högre grad beroende av tillgången till elektroniska bevis för att effektivt bekämpa terrorism, organiserad brottslighet, sexuella övergrepp mot barn (särskilt online-aspekterna av dessa) samt en rad andra former av it-brott och brottslighet som möjliggörs av informationsteknik. För behöriga myndigheter kan tillgång till elektroniska bevis vara av avgörande betydelse, inte bara för att genomföra framgångsrika utredningar och därigenom ställa brottslingar inför rätta, utan även för att skydda brottsoffer och bidra till att garantera säkerheten.

---

1 Dom av den 16 juli 2020 i mål C-311/18 – Data Protection Commissioner mot Facebook Ireland Limited och Maximillian Schrems, ECLI:EU:C:2020:559.

2 Iocta 2020, s. 25.

Det finns dock fall där kryptering gör tillgången till och analysen av kommunikationsinnehåll inom ramen för tillgång till elektroniska bevis ytterst utmanande eller rentav praktiskt omöjlig, trots att tillgången till sådana uppgifter egentligen är laglig. Oberoende av dagens tekniska miljö är det därför viktigt att bevara de behöriga myndigheternas befogenheter på området säkerhet och straffrätt genom laglig tillgång, som gör att de kan utföra sina uppgifter i enlighet med vad som föreskrivs och är tillåtet enligt lag. Sådana lagar som föreskriver brottsbekämpande befogenheter måste alltid fullt ut respektera vederbörliga förfaranden och andra skyddsåtgärder samt grundläggande rättigheter, särskilt rätten till respekt för privatlivet och kommunikation och rätten till skydd av personuppgifter.

4. Att finna rätt balans

Principen om säkerhet genom kryptering och säkerhet trots kryptering måste upprätthållas i sin helhet. Europeiska unionen fortsätter att stödja stark kryptering. Kryptering kan stärka människors förtroende för digitaliseringen och för skyddet av de grundläggande rättigheterna, och bör främjas och utvecklas.

Det är ytterst viktigt att skydda integriteten och säkerheten i kommunikation genom kryptering, samtidigt som man bevarar möjligheten för behöriga myndigheter på området säkerhet och straffrätt att lagligen få tillgång till relevanta uppgifter för berättigade, tydligt definierade ändamål i kampen mot grov och/eller organiserad brottslighet och terrorism, även i den digitala världen, och upprätthåller rättsstatsprincipen. I alla de åtgärder som vidtas måste man noga väga dessa intressen mot principerna om nödvändighet, proportionalitet och subsidiaritet.

5. Samarbete med tekniksektorn

På längre sikt strävar Europeiska unionen efter att föra en aktiv dialog med tekniksektorn och samtidigt involvera forskare och den akademiska världen, för att säkerställa fortsatt tillämpning och användning av stark krypteringsteknik. Behöriga myndigheter måste kunna få tillgång till uppgifter på ett lagligt och målinriktat sätt, med full respekt för grundläggande rättigheter och relevant dataskyddslagstiftning, samtidigt som it-säkerheten upprätthålls. Tekniska lösningar för att få tillgång till krypterade uppgifter måste följa principerna om laglighet, öppenhet, nödvändighet och proportionalitet, inbegripet skydd av personuppgifter, genom utformning och standardinställningar.

Eftersom det finns fler än ett sätt att uppnå de fastställda målen måste stater, näringslivet, forskare och den akademiska världen samarbeta på ett transparent sätt för att strategiskt skapa denna balans.

6. Regelverk

Behovet av att utveckla ett regelverk för hela EU som skulle göra det möjligt för behöriga myndigheter att utföra sina operativa uppgifter på ett effektivt sätt och samtidigt skydda integriteten, de grundläggande rättigheterna och kommunikationssäkerheten kan utredas ytterligare.

Potentiella tekniska lösningar måste göra det möjligt för myndigheterna att använda sådana utredningsbefogenheter som är föremål för proportionalitet, nödvändighet och rättslig tillsyn enligt deras nationella lagstiftning, samtidigt som man respekterar gemensamma europeiska värderingar, värnar de grundläggande rättigheterna och bevarar fördelarna med kryptering. Möjliga lösningar bör utvecklas på ett transparent sätt i samarbete med nationella och internationella leverantörer av kommunikationstjänster och andra berörda aktörer. Sådana tekniska lösningar och standarder – och den snabba tekniska utvecklingen i allmänhet – kräver också en kontinuerlig förbättring av de behöriga myndigheternas tekniska och operativa kompetens och expertis, för att på ett effektivt sätt bemöta de utmaningar som digitaliseringen innebär i deras arbete globalt.

7. Innovativ utredningskapacitet

Slutligen är det av yttersta vikt att förbättra samordningen på EU-nivå i syfte att

1) kombinera alla medlemsstaters, EU-institutioners och EU-organs insatser,

2) definiera och fastställa innovativa metoder med hänsyn till ny teknik,

3) analysera lämpliga tekniska och operativa lösningar, och

4) tillhandahålla skräddarsydd högkvalitativ utbildning.

Tekniska och operativa lösningar som är förankrade i ett regelverk som bygger på principerna om laglighet, nödvändighet och proportionalitet bör utvecklas i nära samråd med tjänsteleverantörer, andra berörda aktörer och samtliga relevanta behöriga myndigheter, även om det inte bör finnas någon fastställd universell teknisk lösning för att ge tillgång till krypterade uppgifter.