



Rådet for
Den Europæiske Union

Bruxelles, 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

NOTE

fra:	formandskabet
til:	delegationerne

Tidl. dok. nr.:	12863/20
-----------------	----------

Vedr.:	Rådets resolution om kryptering - Sikkerhed ved hjælp af kryptering og på trods heraf
--------	--

Vedlagt følger til delegationerne Rådets resolution om kryptering.

**Rådets resolution om kryptering
Sikkerhed ved hjælp af kryptering og på trods heraf**

1. Præambel: - Sikkerhed ved hjælp af kryptering og på trods heraf

Den Europæiske Union støtter fuldt ud udviklingen, gennemførelsen og anvendelsen af solid kryptering. Den Europæiske Union understreger behovet for at sikre fuld respekt for de grundlæggende rettigheder, menneskerettighederne og retsstatsprincippet i forbindelse med alle foranstaltninger i henhold til denne resolution, både online og offline. Kryptering er et nødvendigt middel til beskyttelse af de grundlæggende rettigheder og den digitale sikkerhed for regeringer, industri og samfund. Samtidig skal Den Europæiske Union sikre, at de kompetente myndigheder vedrørende sikkerhed og strafferet, f.eks. retshåndhævende og judicielle myndigheder, kan udøve deres retmæssige beføjelser, både online og offline, og dermed beskytte vores samfund og borgerne.

Ifølge Det Europæiske Råds konklusioner af 1.-2. oktober 2020 (EUCO 13/20) *vil EU udnytte sine værktøjer og reguleringsmæssige beføjelser til at bidrage til udformningen af globale regler og standarder. Der var enighed om, at midlerne under genopretnings- og resiliensfaciliteten skulle anvendes til at fremme mål såsom at styrke EU's evne til at beskytte sig selv mod cybertrusler, sørge for et sikkert kommunikationsmiljø, navnlig gennem kvantekryptering, og sikre adgang til data til judicielle og retshåndhævende formål.*

2. Nuværende anvendelse/status over kryptering

På verdensplan anvendes krypteringsteknologi i dag i stigende grad på alle områder i såvel det offentlige som det private rum. Den kan bruges til at beskytte de enkelte borgere, civilsamfundet, kritiske infrastrukturer, medierne og journalisterne, industrien og regeringerne ved at sikre kommunikationens og personoplysningernes hemmelighed, fortrolighed, dataintegritet og tilgængelighed: det er tydeligt, at krypteringsteknologien er til gavn for alle. Kryptering er blevet identificeret af EU's databeskyttelses- og cybersikkerhedsmyndigheder som et vigtigt redskab, der f.eks. bidrager til beskyttelsen af personoplysninger, der overføres til ikke-EU-lande, men er underlagt kravet om et i det væsentlige tilsvarende beskyttelsesniveau, hvilket ifølge Domstolen er et lovkrav for dataoverførsler¹. Ikke kun elektroniske enheder og applikationer bliver i stigende grad programmeret til automatisk at kryptere lagrede brugerdata, men stadig flere kommunikationskanaler og datalagringstjenester sikres også ved hjælp af end-to-end-kryptering (E2E). Dette afspejles positivt i et stadig større modsvar fra kommunikations- og applikationssektoren, hvor der i størstedelen af instant messaging-apps og andre onlineplatforme også er implementeret end-to-end-kryptering.

3. Udfordringer med hensyn til at garantere sikkerheden

"Det digitale liv" og cyberspace frembyder ikke blot enorme muligheder, men også betydelige udfordringer: digitaliseringen af det moderne samfund medfører visse sårbarheder og muligheden for at blive udnyttet til kriminelle formål. De kriminelle kan således i deres *modus operandi* udnytte let tilgængelige, standardiserede krypteringsløsninger udviklet til lovlige formål².

Samtidig er retshåndhævelse i stigende grad afhængig af adgangen til elektronisk bevismateriale for effektivt at bekæmpe terrorisme, organiseret kriminalitet, seksuelt misbrug af børn (navnlig onlineaspekterne heraf) samt en række andre former for cyberkriminalitet og cyberbaserede forbrydelser. For de kompetente myndigheder kan adgang til elektronisk bevismateriale være afgørende, ikke blot med henblik på at foretage en vellykket efterforskning og dermed retsforfølge de kriminelle, men også for at beskytte ofrene og bidrage til at garantere sikkerheden.

¹ Dom af 16. juli 2020 i sag C-311/18, Data Protection Commissioner mod Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

² IOCTA 2020, s. 25.

Der er imidlertid situationer, hvor kryptering gør adgangen til og analysen af kommunikationsindhold i forbindelse med adgang til elektroniske beviser ekstremt udfordrende eller praktisk umulig, selv om adgangen til sådanne data reelt er lovlig. Uafhængigt af dagens teknologiske klima er det derfor vigtigt, at de kompetente myndigheder bevarer deres sikkerheds- og strafferetlige beføjelser, så de lovligt kan udføre deres opgaver som foreskrevet og godkendt ved lov. Sådanne love, der giver håndhævelsesbeføjelser, skal altid fuldt ud respektere en retfærdig procedure og andre garantier samt de grundlæggende rettigheder, navnlig retten til respekt for privatliv og kommunikation og retten til beskyttelse af personoplysninger.

4. Opnåelse af den rette balance

Princippet om sikkerhed gennem kryptering og på trods heraf skal opretholdes i sin helhed. Den Europæiske Union støtter fortsat stærk kryptering. Kryptering er et tillidsskabende element i digitaliseringen og beskyttelsen af de grundlæggende rettigheder og bør fremmes og udvikles.

Det er yderst vigtigt at beskytte privatlivets fred og kommunikationssikkerheden ved hjælp af kryptering og samtidig fastholde de kompetente sikkerheds- og strafferetlige myndigheders mulighed for lovligt at få adgang til relevante data til legitime, klart definerede formål i forbindelse med bekæmpelse af grov og/eller organiseret kriminalitet og terrorisme, herunder i den digitale verden, og opretholde retsstatsprincippet. Alle de foranstaltninger, der træffes, skal afveje disse interesser omhyggeligt i forhold til principperne om nødvendighed, proportionalitet og nærhed.

5. Samarbejde med den teknologiske industri

På længere sigt bestræber Den Europæiske Union sig på at føre en aktiv debat med teknologiindustrien og samtidig inddrage forskningsverdenen og den akademiske verden for at sikre fortsat gennemførelse og anvendelse af en stærk krypteringsteknologi. De kompetente myndigheder skal kunne få adgang til data på lovlig og målrettet vis under fuld overholdelse af de grundlæggende rettigheder og de relevante databeskyttelseslove, samtidig med at cybersikkerheden opretholdes. Tekniske løsninger, der giver adgang til krypterede data, skal overholde principperne om lovlighed, gennemsigtighed, nødvendighed og proportionalitet, herunder beskyttelse af personoplysninger gennem design og standardindstillinger.

Da der ikke findes nogen enkelt måde at nå de fastsatte mål på, er myndighederne, industrien, forskerne og den akademiske verden nødt til at samarbejde på en transparent måde for strategisk at skabe denne balance.

6. Lovgivningsmæssig ramme

Behovet for at udvikle et regelsæt i hele EU, så de kompetente myndigheder kan udføre deres operationelle opgaver effektivt og samtidig beskytte privatlivets fred, de grundlæggende rettigheder og kommunikationssikkerheden, kan vurderes yderligere.

Med de potentielle tekniske løsninger skal myndighederne kunne udøve deres undersøgelsesbeføjelser, som er underlagt proportionalitet, nødvendighed og retsligt tilsyn i henhold til deres nationale lovgivning, og samtidig respektere Europas fælles værdier og opretholde de grundlæggende rettigheder samt bevare fordelene ved kryptering. Mulige løsninger bør udvikles på en transparent måde i samarbejde med nationale og internationale udbydere af kommunikationstjenester og andre relevante interessenter. Sådanne tekniske løsninger og standarder – og den hurtige teknologiske udvikling generelt – vil også kræve løbende forbedring af de kompetente myndigheders tekniske og operationelle kompetencer og ekspertise til effektivt at tackle digitaliseringens udfordringer i deres arbejde på globalt plan.

7. Innovativ efterforskningskapacitet

Endelig er det afgørende at forbedre koordineringen på EU-plan med henblik på:

- 1) at kombinere indsatsen fra alle medlemsstater samt EU's institutioner og organer
- 2) at definere og etablere innovative tilgange med henblik på nye teknologier
- 3) at analysere passende tekniske og operationelle løsninger samt
- 4) at tilbyde skræddersyet uddannelse af høj kvalitet.

Tekniske og operationelle løsninger, der er forankret i en lovgivningsmæssig ramme på grundlag af principperne om lovlighed, nødvendighed og proportionalitet, bør udvikles i tæt samråd med tjenesteudbydere, andre relevante interessenter og alle relevante kompetente myndigheder, selv om der ikke bør være en enkelt foreskrevet teknisk løsning for at give adgang til krypterede data.