Euroopan unionin
neuvosto

Bryssel, 24. marraskuuta 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

ILMOITUS

Lähettäjä:	Puheenjohtajavaltio
Vastaanottaja:	Valtuuskunnat
Ed. asiak. nro:	12863/20
Asia:	Neuvoston päätöslauselma salauksesta – Turvallisuus salauksen avulla ja salauksesta huolimatta

Valtuuskunnille toimitetaan oheisena neuvoston päätöslauselma salauksesta.

Neuvoston päätöslauselma salauksesta
Turvallisuus salauksen avulla ja salauksesta huolimatta

1. Johdanto: Turvallisuus salauksen avulla ja salauksesta huolimatta

Euroopan unioni antaa täyden tukensa vahvan salauksen kehittämiselle, käyttöönotolle ja hyödyntämiselle. Euroopan unioni korostaa tarvetta varmistaa perusoikeuksien, ihmisoikeuksien ja oikeusvaltioperiaatteen täysimääräinen kunnioittaminen kaikissa tähän päätöslauselmaan liittyvissä toimissa sekä verkossa että sen ulkopuolella. Salaus on tarpeellinen keino, jolla suojellaan perusoikeuksia sekä hallitusten, elinkeinoelämän ja yhteiskunnan digitaalista turvallisuutta. Samalla Euroopan unionin on varmistettava, että turvallisuuden ja rikosoikeuden alan toimivaltaiset viranomaiset, kuten lainvalvonta- ja oikeusviranomaiset, voivat käyttää laillisia valtuuksiaan sekä verkossa että sen ulkopuolella suojellessaan yhteiskuntiamme ja kansalaisiamme.

Eurooppa-neuvoston 1. ja 2. lokakuuta 2020 antamien päätelmien (EUCO 13/20) mukaan *EU aikoo vahvistaa välineitään ja säädösvaltaansa helpottaakseen globaalien sääntöjen ja normien muokkaamista.* Tuolloin sovittiin, että elpymis- ja palautumistukivälineen varoja käytettäisiin muun muassa sellaisten tavoitteiden edistämiseen, joilla *parannetaan EU:n kykyä suojautua kyberuhkilta, tarjota suojattu viestintäympäristö, erityisesti kvanttisalauksen avulla, ja varmistaa tietojen saatavuus oikeudellisia ja lainvalvontatarkoituksia varten.*

2. Salauksen tämänhetkinen käyttö/tila

Salausteknologiaa käytetään nykyään yhä enemmän kaikilla julkisen ja yksityisen elämän aloilla. Se on keino, jolla suojellaan ihmisiä, kansalaisyhteiskuntaa, kriittisiä infrastruktuureja, mediaa ja toimittajia, teollisuutta ja hallituksia huolehtimalla viestinnän ja henkilötietojen yksityisyydestä, luottamuksellisuudesta sekä tietojen eheydestä ja saatavuudesta: on selvää, että kaikki osapuolet hyötyvät salausteknologiasta. EU:n tietosuoja- ja kyberturvallisuusviranomaiset ovat määritelleet salauksen tärkeäksi välineeksi, joka edistää esimerkiksi EU:n ulkopuolelle siirrettävien henkilötietojen suojaa mutta johon sovelletaan pääosiltaan vastaavan tasoisen suojan vaatimusta, joka unionin tuomioistuimen mukaan on tiedonsiirrolle asetettu lakisääteinen vaatimus[1]. Sen lisäksi, että elektroniset laitteet ja sovellukset ohjelmoidaan yhä enemmän jo oletusarvoisesti salaamaan tallennetut käyttäjätiedot, myös yhä useammat viestintäkanavat ja tiedontallennuspalvelut on suojattu päästä päähän -salauksella. Tämä näkyy myönteisesti viestintä- ja sovellusalalla, jossa suurin osa pikaviestintäsovelluksista ja muista verkkoalustoista on myös ottanut käyttöön päästä päähän -salauksen.

3. Turvallisuuden varmistamisen haasteet

"Digitaalinen elämä" ja kybertoimintaympäristö merkitsevät mittavia mahdollisuuksia, mutta myös huomattavia haasteita: modernien yhteiskuntien digitalisaatio tuo mukanaan tiettyjä haavoittuvuuksia ja mahdollisuuksia rikollisten tarkoitusperien mukaiseen hyväksikäyttöön. Rikolliset voivat näin ollen lisätä keinovalikoimaansa helposti saatavilla olevia käyttövalmiita salausratkaisuja, jotka on suunniteltu laillisia tarkoituksia varten[2].

Samaan aikaan lainvalvonta on yhä riippuvaisempaa sähköisen todistusaineiston saatavuudesta pyrkiessään torjumaan tehokkaasti terrorismia, järjestäytynyttä rikollisuutta, lasten seksuaalista hyväksikäyttöä (erityisesti sen verkkoon liittyvien näkökohtien osalta) sekä erilaisia muita kyberrikollisuuden muotoja ja kyberympäristöä hyväksi käyttäen tehtäviä rikoksia. Toimivaltaisten viranomaisten kannalta sähköisen todistusaineiston saatavuudella voi olla olennainen merkitys paitsi siksi, että tutkinta saadaan suoritettua onnistuneesti ja sen myötä rikolliset saatettua oikeuden eteen, myös siksi, että näin voidaan suojella uhreja ja auttaa varmistamaan turvallisuus.

---

[1] Tuomio 16.7.2020, asia C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

[2] Järjestäytynyttä verkkorikollisuutta koskeva uhka-arvio (iOCTA) 2020, s. 25.

Joissain tapauksissa viestinnän sisältöön pääsy ja sen analysointi sähköisen todistusaineiston saamiseksi saatavuuden puitteissa on salauksen vuoksi äärimmäisen haasteellista tai käytännössä mahdotonta huolimatta siitä, että pääsy tällaisiin tietoihin olisi laillista. Kulloisestakin teknologisesta ympäristöstä riippumatta on näin ollen välttämätöntä turvata turvallisuusalan ja rikosoikeuden toimivaltaisten viranomaisten valtuudet antamalla näille laillinen pääsy tietoihin, jotta ne voivat hoitaa tehtävänsä laissa säädetyllä ja sallitulla tavalla. Tällaisten lakien, joissa säädetään täytäntöönpanovaltuuksista, on aina noudatettava täysimääräisesti asianmukaista menettelyä ja muita takeita sekä perusoikeuksia, erityisesti oikeutta yksityiselämän ja viestinnän kunnioittamiseen ja oikeutta henkilötietojen suojaan.

4. Oikea tasapaino

Turvallisuus salauksen avulla ja turvallisuus salauksesta huolimatta -periaatteesta on pidettävä kiinni kokonaisuudessaan. Euroopan unioni antaa edelleen tukensa vahvalle salaukselle. Salaus on luottamuksen kulmakivi digitalisaatiossa ja perusoikeuksien suojelussa, ja sitä olisi edistettävä ja kehitettävä.

On erittäin tärkeää suojella viestinnän yksityisyyttä ja turvallisuutta salauksen avulla ja samalla säilyttää turvallisuuden ja rikosoikeuden alalla toimivaltaisten viranomaisten mahdollisuus päästä asiaankuuluviin tietoihin laillisia ja selkeästi määriteltyjä tarkoituksia varten vakavan ja/tai järjestäytyneen rikollisuuden ja terrorismin torjumiseksi, myös digitaalisessa maailmassa, ja vaalia oikeusvaltioperiaatetta. Kaikissa toteuttavissa toimissa on punnittava huolellisesti näitä etuja suhteessa tarpeellisuus-, suhteellisuus- ja toissijaisuusperiaatteisiin.

5. Voimien yhdistäminen teknologiateollisuuden kanssa

Euroopan unioni pyrkii jatkossa käymään teknologiateollisuuden kanssa aktiivista keskustelua, johon otetaan mukaan myös tutkijat ja tiedemaailma, jotta voidaan varmistaa vahvan salausteknologian jatkuva soveltaminen ja käyttö. Toimivaltaisten viranomaisten on voitava päästä tietoihin laillisesti ja kohdennetusti perusoikeuksia ja asiaankuuluvaa tietosuojalainsäädäntöä täysimääräisesti noudattaen, samalla kun pidetään yllä kyberturvallisuutta. Salattuihin tietoihin pääsyn mahdollistavien teknisten ratkaisujen on oltava laillisuus-, avoimuus-, tarpeellisuus- ja suhteellisuusperiaatteiden mukaisia, sisäänrakennetun ja oletusarvoisen henkilötietojen suojan periaate mukaan lukien.

Koska asetettujen tavoitteiden saavuttamiseen ei ole yhtä ainoaa tapaa, hallitusten, teollisuuden, tutkijoiden ja tiedemaailman on tehtävä avointa yhteistyötä noudattaen strategiaa, jolla tällaiseen tasapainoon voi päästä.

6. Sääntelykehys

Voitaisiin arvioida tarkemmin tarvetta kehittää EU:n laajuinen sääntelykehys, joka antaisi toimivaltaisille viranomaisille mahdollisuuden hoitaa operatiiviset tehtävänsä tehokkaasti samalla kun suojellaan yksityisyyttä, perusoikeuksia ja viestinnän turvallisuutta.

Mahdollisten teknisten ratkaisujen on annettava viranomaisille mahdollisuus käyttää tutkintavaltuuksiaan, joihin sovelletaan niiden kansallisen lainsäädännön mukaisia suhteellisuus- ja tarpeellisuusperiaatteita sekä oikeudellista valvontaa, samalla kun kunnioitetaan yhteisiä eurooppalaisia arvoja ja perusoikeuksia ja säilytetään salauksen edut. Mahdollisia ratkaisuja olisi kehitettävä avoimesti yhteistyössä kansallisten ja kansainvälisten viestintäpalvelujen tarjoajien ja muiden asiaankuuluvien sidosryhmien kanssa. Tällaiset tekniset ratkaisut ja standardit – ja teknologian nopea kehitys ylipäätänsä – edellyttäisivät myös toimivaltaisten viranomaisten teknisten ja operatiivisten taitojen ja asiantuntemuksen jatkuvaa parantamista, jotta nämä voivat vastata globaalin digitalisaation työlleen asettamiin haasteisiin.

7. Innovatiiviset tutkintavalmiudet

Kaiken kaikkiaan on erittäin tärkeää parantaa EU:n tason koordinointia, jonka tavoitteena on

1) yhdistää kaikkien jäsenvaltioiden sekä EU:n toimielinten ja elinten toimet,

2) määritellä ja ottaa käyttöön innovatiivisia lähestymistapoja uusia teknologioita silmällä pitäen,

3) analysoida tarkoituksenmukaisia teknisiä ja operatiivisia ratkaisuja ja

4) tarjota räätälöityä laadukasta koulutusta.

Laillisuus-, tarpeellisuus- ja suhteellisuusperiaatteisiin pohjautuvaan sääntelykehykseen perustuvia teknisiä ja operatiivisia ratkaisuja olisi kehitettävä kuullen tiiviisti palveluntarjoajia, muita asiaankuuluvia sidosryhmiä ja kaikkia asiaankuuluvia toimivaltaisia viranomaisia, vaikka ei olisikaan aiheellista säätää yhdestä yksittäisestä teknisestä ratkaisusta salattuihin tietoihin pääsyä varten.