Asia

OSA; Keskustelun avaus EU:n tasapainoisesta lähestymistavasta salaukseen sekä toimivaltaisten viranomaisten mahdollisuuksiin saada pääsy salattuun tietoon yksittäistapauksissa toimivaltuuksien puitteissa

Kokous

U/E/UTP-tunnus

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Neuvoston edellinen puheenjohtajamaa Saksa käynnisti EU:ssa keskustelut tasapainoisesta lähestymistavasta digitaalimaailman salaukseen sekä toimivaltaisten viranomaisten mahdollisuuksiin saada pääsy digitaalisesti salattuun tietoon. Saksa laati aiheesta neuvoston päätöslauselman (Council Resolution on Encryption (13084/1/20)) sekä asiakirjan toimenpiteistä päätöslauselman edistämiseksi (13550/20).

Näitä asiakirjoja käsiteltiin sisäisen turvallisuuden pysyvän komitean (COSI) kokouksessa 19.11.2020, ja niiden muodollinen hyväksyminen tapahtui neuvoston kirjallisessa menettelyssä 14.12.2020.

Asiakokonaisuus nostettiin esiin myös neuvoston päätelmissä sisäisestä turvallisuudesta ja eurooppalaisesta poliisikumppanuudesta (13083/1/20), jotka käsiteltiin joulukuun sisäministereiden videokokouksessa. Myös 13.11.2020 sisäministereiden videokokouksen yhteydessä hyväksytyssä sisäministereiden julistuksessa liittyen viimeaikaisiin terrori-iskuihin, neuvostoa kehotettiin harkitsemaan tätä asiakokonaisuutta.

Tämän kirjelmän tavoitteena on tiedottaa eduskuntaa asian käsittelyn vaiheesta ja määritellä valtioneuvoston lähtökohdat EU-tason jatkokeskustelua varten.

Suomen kanta

Valtioneuvosto huomioi avatun keskustelun EU:n tasapainoisesta lähestymistavasta liittyen salaukseen sekä toimivaltaisten viranomaisten mahdollisuuksiin saada pääsy salattuun tietoon toimivaltuuksien puitteissa. Valtioneuvosto pitää tärkeänä, että EU-tasolla kehitetään tasapainoinen ja teknologianeutraali lähestymistapa, joka samanaikaisesti huomioi tarpeen sekä turvata vahva salaus että viranomaisten laissa tarkkarajaisesti määritellyn mahdollisuuden yksittäistapauksissa päästä salattuihin tietoihin ja sähköiseen todistusaineistoon toimivaltuuksiensa puitteissa. Edellisen puheenjohtajamaa Saksan keskustelun pohjaksi laatimien asiakirjojen pohjalta keskustelua voi jatkaa tämän tasapainoisen lähestymistavan löytämiseksi.

Tulee keskustella menetelmistä, joilla vahva salaus pystytään säilyttämään, mutta samalla mahdollistetaan viranomaisille tietoturvallisesti tarkkarajainen ja oikeasuhtainen pääsy salattuun tietoon ja sähköiseen todistusaineistoon yksittäistapauksissa viranomaisten laissa määriteltyjen tehtävien hoitamiseksi eli rikosten ennalta estämiseksi, tutkimiseksi, rikosoikeudelliseen vastuuseen saattamiseksi, uhrien suojelemiseksi sekä kansallisen turvallisuuden suojaamiseksi.

On tärkeää selvittää laajassa yhteistyössä viranomaisten, yksityisen sektorin, tutkijoiden, kansalaisyhteiskunnan ja tietosuojasta vastaavien tahojen kanssa, miten tällaiset tekniset mahdollisuudet voidaan viranomaisille luoda. Laajassa yhteistyössä ja läpinäkyvästi etsityt EU-tason ratkaisut ovat tärkeitä, jotta voitaisiin löytää yhteisesti toimivia ratkaisuja, jotka eivät heikennä palveluntarjoajien sähköisten palvelujen kyberturvallisuutta eivätkä estä lainvalvontaviranomaisia estämästä ja tutkimasta vakavia rikoksia.

Lainsäätäjien aiemmin hyväksymiä lainvalvonta- ja oikeusviranomaisten toimivaltuuksia rikosten torjumiseksi ei voida joissain tapauksissa toteuttaa kuten aiemmin, koska teknologian kehitys on muuttanut viestinnän tapoja ja merkittävä osa viestinnästä tapahtuu teleyrityksistä riippumattomien toimijoiden alustoilla (ns. OTT-alustat).

Toimivaltaisten viranomaisten pääsy salattuun tietoon on rajattava esimerkiksi rikollisuuden vakavuuden perusteella. Lisäksi EU-tason ratkaisussa on varmistuttava kansallisten laillisuusvalvontaviranomaisten edellytyksistä valvoa viranomaisten toiminnan lainmukaisuutta.

Kaikkien esitettävien keinojen kohdalla tulee aktiivisesti arvioida suhdetta perusoikeuksiin, kuten yksityisyydensuojaan ja tietosuojaan. Kyse on erisuuntaisten perusteiden punninnasta ja viime kädessä kokonaisarviosta. Toisaalta perusoikeuksien, kuten viestinnän luottamuksellisuus, toteutuminen on turvattava, mutta samanaikaisesti viranomaisilla tulee olla riittävät, laissa tarkkarajaisesti määritellyt edellytykset torjua vakavaa rikollisuutta.

Digitaalisessa maailmassa salaus on keskeistä, sillä se turvaa toisaalta digitaalisia järjestelmiä ja toisaalta yksityisyyden suojaa ja henkilökohtaisia tietoja. Vahva salaus on merkityksellinen perusoikeuksien, kuten sananvapauden, yksityisyyden suojan ja tietosuojan, suojaamisessa.

Viranomaisten laissa määriteltyjen tehtävien tehokas hoitaminen myös digitaalimaailmassa edistää viranomaisten kykyä turvata perus- ja ihmisoikeuksien, kuten oikeuden elämään ja henkilökohtaiseen koskemattomuuteen ja omaisuuden suojan toteutumista. Digitaalisessa maailmassakin perus- ja ihmisoikeuksia on hyväksyttävää rajata vain täsmällisesti ja tarkkarajaisesti säädetyissä tilanteissa.

Valtioneuvosto korostaa tarvetta löytää tasapainoisia perus- ja ihmisoikeuksia kunnioittavia lähestymistapoja.

Asiasta ei ole komission esitystä. Jos tällainen komission esitys tulee, valtioneuvosto tarkastelee sitä huolellisesti ja muodostaa siihen kantansa sen jälkeen.

Pääasiallinen sisältö

Viestinnän yksityisyyden ja muiden perusoikeuksien suojaaminen salaamalla ja

toisaalta lainvalvontaviranomaisten tutkintavaltuuksien puolustaminen digitaalisessa maailmassa on noussut esiin EU:ssa.

1. Neuvoston edellisen puheenjohtajamaa Saksan laatimat asiakirjat

Neuvoston laajat päätelmät sisäisestä turvallisuudesta ja eurooppalaisesta poliisikumppanuudesta (13083/1/20) peräänkuuluttaa turvallisuusunionistrategiassa mainitun ja Euroopan neuvoston esiin nostaman tarpeen varmistaa lainvalvonta- ja oikeusviranomaisten laillinen pääsy sähköiseen todistusaineistoon nykypäivän alati muuttuvassa teknisessä ympäristössä.

Päätelmissä korostetaan, että vahva salaus on luottamuksen ankkuri digitalisaatiossa ja Euroopan unioni tukee täysin vahvan salauksen kehittämistä, toteuttamista ja käyttöä. Salaus on välttämätön keino suojella perusoikeuksia ja hallitusten, teollisuuden ja yhteiskunnan digitaalista turvallisuutta. Mutta samalla EU:n on varmistettava toimivaltaisten viranomaisten laillinen mahdollisuus päästä salattuihin tietoihin ja sähköiseen todistusaineistoon toimivaltansa puitteissa, sekä verkossa että sen ulkopuolella turvatakseen yhteiskuntiamme ja kansalaisiamme.

Päätelmissä viitataan neuvoston salausta koskevaan päätöslauselmaan (13084/1/20), jonka läpileikkaava teema on ”turvallisuus salauksen avulla ja salauksesta huolimatta”. Tällä tarkoitetaan sitä, että on löydettävä tasapaino sen välillä, että on edelleen turvattava sähköisen viestinnän yksityisyys ja turvallisuus vahvalla salauksella, mutta samalla on turvattava toimivaltaisten viranomaisten mahdollisuus käyttää laillisia valtuuksiaan päästä asiaankuuluviin tietoihin selkeästi määriteltyihin tarkoituksiin vakavan ja järjestäytyneen rikollisuuden ja terrorismin torjunnassa. EU korostaa tarvetta varmistaa perus- ja ihmisoikeuksien sekä oikeusvaltioperiaatteen täysimääräinen kunnioittaminen, niin fyysisessä kuin digitaalisessa maailmassa, kaikissa tähän päätöslauselmaan liittyvissä toimissa ja kaikkien toteutettujen toimien on tasapainotettava edellä mainitut intressit välttämättömyyden, suhteellisuuden ja toissijaisuuden periaatteiden kanssa.

Päätöslauselmassa korostetaan, että on selvää, että kaikki osapuolet hyötyvät tehokkaasta salausteknologiasta. EU pyrkii luomaan aktiivisen keskustelun teknologiateollisuuden kanssa ja tuomaan mukaan tutkimuksen ja korkeakoulut varmistaakseen vahvan salausteknologian jatkuvan kehityksen ja käytön.

"Digitaalinen elämä" ja kyberavaruus tarjoavat paitsi suuria mahdollisuuksia myös merkittäviä haasteita ja haavoittuvuuksia. Rikolliset voivat hyväksikäyttää yhteiskuntien digitalisaatiota, ja esimerkiksi sisällyttää omiin rikollisiin toimiinsa helposti saatavissa olevia, laillisiin tarkoituksiin suunniteltuja salausratkaisuja.

Samaan aikaan lainvalvontaviranomaiset ovat yhä riippuvaisempia sähköiseen todistusaineiston saatavuudesta torjuakseen tehokkaasti terrorismia, järjestäytynyttä rikollisuutta, erityisesti verkossa tapahtuvaa lasten seksuaalista hyväksikäyttöä sekä erilaista muuta tietotekniikka- ja tietoverkkorikollisuutta. Toimivaltaisille viranomaisille pääsy sähköiseen todistusaineistoon voi olla välttämätöntä paitsi tutkintojen suorittamiseksi ja siten rikollisten saattamiseksi oikeuden eteen, myös uhrien suojelemiseksi ja turvallisuuden takaamiseksi.

Päätöslauselmassa huomautetaan, että koska asetettujen tavoitteiden saavuttamiseksi ei ole yhtä tapaa, hallitusten, teollisuuden, tutkimuksen ja korkeakoulujen on toimittava yhdessä avoimesti tämän tasapainon luomiseksi. Teknisiä ratkaisuja salattujen tietojen lailliseen saatavuuteen on etsittävä läheisessä vuoropuhelussa toimivaltaisten

viranomaisten, teknologiateollisuuden, viestintäpalvelujen tarjoajien, korkeakoulujen ja muiden asiaankuuluvien sidosryhmien kanssa.

Päätöslauselman mukaan mahdollisten teknisten ratkaisujen, joiden avulla salattuihin tietoihin päästään, on noudatettava laillisuuden, läpinäkyvyyden, välttämättömyyden ja suhteellisuuden periaatteita sekä otettava huomioon henkilötietojen suojaaminen oletusarvoisesti. Teknisten ratkaisujen on annettava toimivaltaisille viranomaisille mahdollisuus käyttää tutkintavaltuuksiaan, joihin sovelletaan kansallisen lainsäädännön mukaista oikeasuhteisuutta, välttämättömyyttä ja oikeudellista valvontaa, kunnioittaen samalla yhteisiä eurooppalaisia arvoja ja perusoikeuksia, samalla säilyttäen salauksen edut.

Koordinointia EU:n tasolla tulee parantaa seuraavissa toimissa:
1) kaikkien jäsenvaltioiden sekä EU:n toimielinten toimien yhdistäminen;
2) innovatiivisten lähestymistapojen määritteleminen ja luominen uuteen tekniikkaan;
3) asianmukaisten teknisten ja operatiivisten ratkaisujen analysointi; ja
4) räätälöidyn korkealaatuisen koulutuksen tarjoaminen.

Turvallisuusunionistrategia

EU:n turvallisuusunionistrategian (COM (2020) 605 final) mukaisesti komissio aikoo selvittää toimenpiteitä, joilla parannetaan lainvalvontavalmiuksia digitaalisissa tutkintatoimissa. Komission tarkoituksena on varmistaa, että lainvalvontaviranomaisilla on käytössään asianmukainen välineistö, tekniikka ja osaaminen. Strategiassa todetaan, että salaus on olennaisen tärkeää digimaailmassa muun muassa turvaten sähköisiä maksutapahtumia sekä suojaten useita perusoikeuksia, kuten sananvapautta, yksityisyyden suojaa ja tietosuojaa.

Komissio aikoo kartoittaa lähestymistapaa digitaalimaailman salattuun tietoon liittyen. Komissio kannattaa lähestymistapaa, jossa tehokas salaus säilytetään viestinnän yksityisyyden ja turvallisuuden suojaamiseksi, mutta joka kuitenkin torjuu tehokkaasti rikollisuutta ja terrorismia. Suomen näkemykset turvallisuusunistrategiaan on annettu E-kirjeessä 119/2020 vp.

2. Seuraavat askeleet

Neuvoston edellinen puheenjohtajamaa Saksa loi asiakirjan ehdotetuista toimenpiteistä päätöslauselman edistämiseksi (13550/20). Tavoitteena on löytää koordinoitu ja johdonmukainen EU:n yhteinen kanta salaukseen ja siihen monimutkaiseen yhteiseen kysymykseen, jonka ”turvallisuus salauksen avulla ja salauksesta huolimatta”, asettaa.

Asiakirjassa peräänkuulutetaan yhteistyötä jäsenmaiden, komission ja muiden EU instituutioiden välillä teknisten ja operatiivisten ratkaisujen löytämiseksi, laillisuuden, välttämättömyyden ja suhteellisuuden periaatteiden pohjalta, läheisessä konsultaatiossa palveluntarjoajien ja relevanttien viranomaisten kanssa. Tavoitteena on luoda kestävä vuoropuhelu salauksesta jäsenvaltioiden, teknologiateollisuuden, kansalaisyhteiskunnan ja korkeakoulujen välillä. Europolin EU:n innovaatiokeskuksella ja kansallisilla tutkimus- ja kehitystiimeillä on tässä tärkeä rooli.

Lisäksi on tärkeää ylläpitää jatkuvaa tiedonvaihtoa kansainvälisen lausunnon ”E2E salaus ja yleinen turvallisuus” alullepanijamaiden (UK, USA, Australia, Uusi Seelanti, Kanada, Intia, Japani) ja muiden relevanttien kansainvälisten toimijoiden kanssa, jotta

voidaan huomioida kaikki intressit, kuten yksityisyyden suoja ja muut perusoikeudet huolellisesti.

Asiakirjassa tunnistetaan palveluntarjoajat ja sosiaalisen median foorumit tärkeiksi sidosryhmiksi ja ne otetaan mukaan keskusteluun teknisen asiantuntemuksen nostamiseksi seuraavalle tasolle ja vuoropuhelun edistämiseksi.

Asiakirjassa korostetaan asianmukaisten teknisten, toiminnallisten ja oikeudellisten ratkaisujen ja näkökohtien jatkuvan arvioinnin tärkeyttä, erityisesti salaustekniikoiden ja sovellusmenetelmien jatkuvan kehityksen vuoksi. Jäsenvaltioita ja EU:n toimielimiä kehotetaan osallistumaan aktiivisesti teknisiin standardointiprosesseihin, unohtamatta korkealaatuisten koulutusohjelmien tärkeyttä viranomaisten teknisen osaamisen takaamiseksi.

Lisäksi tulisi tarkastella eri sääntelykehysten vaikutuksia ja pyrkiä johdonmukaiseen EU-tason sääntelyyn, joka antaisi toimivaltaisille viranomaisille mahdollisuuden hoitaa operatiiviset tehtävänsä tehokkaasti.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

-

Käsittely Euroopan parlamentissa

-

Kansallinen valmistelu

Oikeus- ja sisäasiat jaosto 7, kirjallinen menettely 23.11-25.11.2020
EU-ministerivaliokunta 15.01.2021

Eduskuntakäsittely

-

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

-

Taloudelliset vaikutukset

-

Muut asian käsittelyyn vaikuttavat tekijät

Rikollisessa toiminnassa perinteiset fyysiset jäljet ovat siirtyneet ja siirtymässä pitkälti verkkoon ja rikolliset hyödyntävät salattuja tietojenvaihtomahdollisuuksia. Toimintaympäristö on muuttunut olennaisesti, kun kaikenlainen rikollisuus on siirtynyt verkkoon. Esimerkiksi verkon petosrikollisuuden ja tietomurtojen lisäksi myös perinteistä asekauppaa, huumekauppaa ja vaikkapa väärennettyjen matkustusasiakirjojen kauppaa käydään yhä useammin verkossa. Terrorismi ja esimerkiksi lasten seksuaalinen hyväksikäyttö ovat muita rikoslajeina, jossa rikolliset voivat salata henkilöllisyytensä ja

piilottaa viestinsä sisällön verkossa. Lainsäädännössä tällä hetkellä säädetyt tilanteet, joissa esimerkiksi telekuuntelun avulla lainvalvonta- ja oikeusviranomaiset voivat pyytää pääsyä tietoon palveluntarjoajalta eivät ole mahdollisia nykyisin käytettävissä olevien salausratkaisujen kohdalla.

Asiakirjat

-

Laatijan ja muiden käsittelijöiden yhteystiedot

Monna Airiainen SM/PO, p. 0295 488 360
Hannele Taavila SM/PO, p. 0295 488 568
Joni Korpinen OM, p. 0295 150 012
Marième Korhonen LVM, p. 0295 342 134
Kerttu Ruokolainen-Monte SUPO, p. 0295 484 788
Kimmo Ulkuniemi POHA, p. 0295 481 680
Päivi Pietarinen VNK/VNEUS, p. 0295 160 354

EUTORI-tunnus

Liitteet

Viite

Asiasanat
Hoitaa

Tiedoksi